Hype Cycle for Security in China, 2023

Published 13 October 2023 - ID G00798938 - 81 min read

By Analyst(s): Feng Gao, Anson Chen, Mia Yu, Angela Zhao

Initiatives: Digital Technology Leadership for CIOs in China; Infrastructure Security

Budget constraints, stringent regulation and ever-increasing digital exposure are challenging security investment in China's organizations. CIOs and their security and risk management leaders should use this Hype Cycle to prioritize security investment in this challenging environment.

Analysis

What You Need to Know

Organizations operating in China face multiple challenges in 2023. Budgets are constrained by slower-than-expected economic growth. Regulations and ever-increasing digital exposure are requiring more security investment. Organizations must balance these challenges and prioritize security investment.

Multiple trends are driving the development of security technology in China. They include threat exposure management, cybersecurity platform consolidation, zero trust adoption and identity-first security (see Top Cybersecurity Trends in China for 2024 and Beyond).

As using security tools from nonlocal vendors poses more challenges in terms of complying with regulations, local security vendors dominate China's security market.

CIOs and their security and risk management (SRM) leaders should study this Hype Cycle to gain a differentiated view of local innovations and prioritize their security investments in China.

The Hype Cycle

This Hype Cycle covers security innovations in China. Four additional innovations feature this year:

- Data security governance
- Exposure management

- Privacy in China
- Security service edge (SSE)

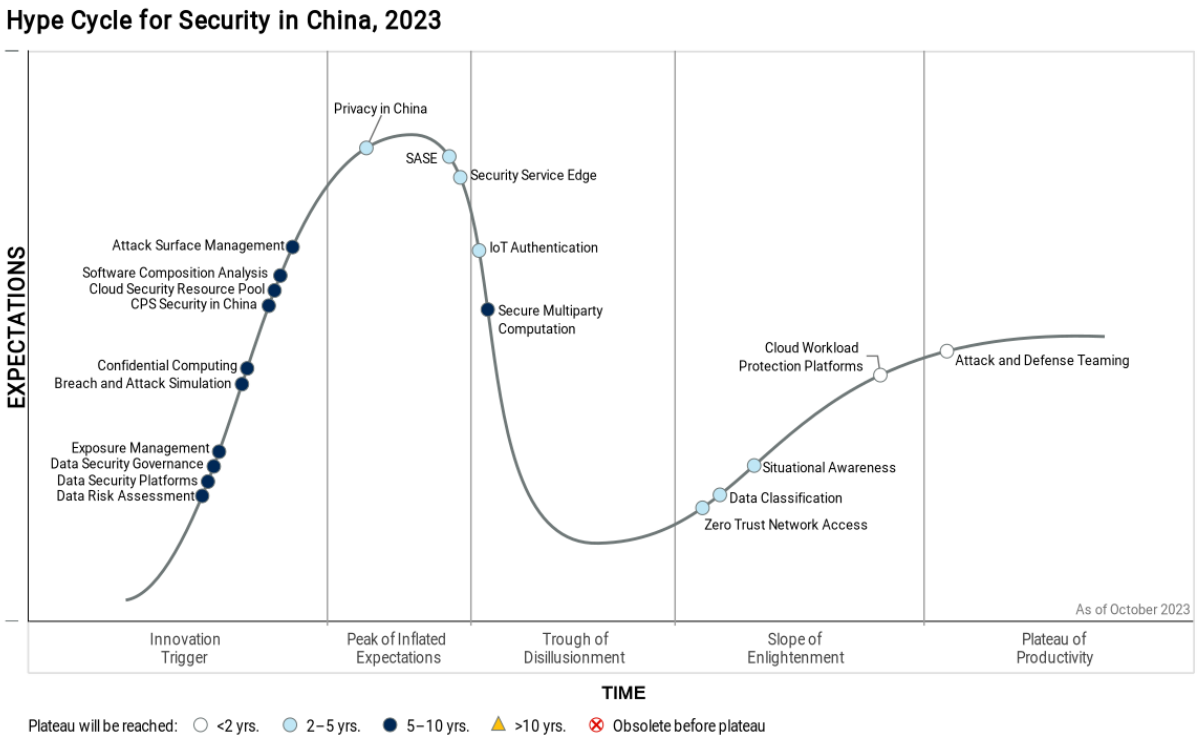
As last year, the Innovation Trigger is the most crowded part of the Hype Cycle. Data security governance and exposure management are additions here. Data security is the top security priority for organizations operating in China. Data security platforms and data risk assessment are also emerging. Exposure management is becoming more important to enable organizations to increase their visibility and prioritize risk reduction with an ever-increasing number of digital assets.

Security and privacy regulations are another hot topic in China. Privacy is at the Peak of Inflated Expectations following the introduction of China's Personal Information Protection Law (PIPL), which has increased awareness of the need to protect personal information. Confidential computing is climbing within the Innovation Trigger, while secure multiparty computation remains in the Trough of Disillusionment. Both innovations protect data during processing. China's national attack and defense drill is driving attack and defense teaming, which has entered the Plateau of Productivity.

As in the global market, cybersecurity platform consolidation is occurring in multiple ways in China. This is driven by budget constraints for clients operating in China. Data security platforms are aggregating different data protection requirements. The cloud security resource pool is a consolidated platform for cloud protection. Both SSE and secure access service edge (SASE) consolidate multiple edge access capabilities, but are descending from the peak as they attract less client interest than expected.

With more clients in China establishing zero trust strategies, adoption of zero trust network access (ZTNA) has increased. It has moved onto the Slope of Enlightenment. Internet of Things (IoT) authentication has quickly passed from the peak into the trough, and we now expect it to take only two to five years to reach the plateau.

Figure 1: Hype Cycle for Security in China, 2023



The Priority Matrix

The Priority Matrix illustrates the benefits of security technologies and services in China, as well as the number of years we expect it will take them to achieve mainstream adoption. The technologies featured are frequently asked about by SRM leaders and beneficial to organizations in China. Together, they cover a wide range of security topics, including application security, cloud security, data security, cyber risk, identity and access management, and security operations.

Attack and defense teaming is the only technology in this Hype Cycle that is currently on the plateau, which it has reached thanks to the national attack and defense drill. Cloud workload protection platforms will mature within two years, however, due to increasing cloud adoption.

Although data security attracts the most client interest, of the relevant technologies only data classification — for which vendor offerings and user adoption are both prevalent — is two to five years away from the plateau. Other data security innovations in this Hype Cycle are still five to 10 years away from the plateau. This is due to technological immaturity (secure multiparty computation, confidential computing, data security platforms) and users' lagging implementation of data security governance and data risk assessment.

Software composition analysis, exposure management, and breach and attack simulation are emerging as more clients in China become aware of their importance.

The trend for cybersecurity platform consolidation is driven by both demand and supply for reduced complexity and improved efficiency. Convergence of technologies and adoption of platforms such as data security platforms, SSE, SASE and the cloud security resource pool continue. This is improving clients' security posture.

Table 1: Priority Matrix for Security in China, 2023

(Enlarged table in Appendix)

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational		SASE Security Service Edge	Data Risk Assessment Data Security Governance Exposure Management Secure Multiparty Computation Software Composition Analysis	
High	Attack and Defense Teaming	Data Classification IoT Authentication Privacy in China	Breach and Attack Simulation CPS Security in China Data Security Platforms	
Moderate	Cloud Workload Protection Platforms	Situational Awareness Zero Trust Network Access	Attack Surface Management Cloud Security Resource Pool Confidential Computing	
Low				

Source: Gartner (October 2023)

Off the Hype Cycle

Bring your own identity in China no longer appears on the Hype Cycle because it has matured, with a high degree of market penetration. Social login and sign-up is a well-established and mainstream technology that provides people with digital identities managed by social digital consumer platforms in China, such as WeChat and Alipay.

On the Rise

Data Risk Assessment

Analysis By: Anson Chen

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Data risk assessment (DRA) is a process used to review whether data security and privacy controls are implemented effectively and satisfy an organization's risk appetite across all applicable security products and applications. These controls aim to mitigate business risks, such as noncompliance with regulations, infringements of privacy and data breaches.

Why This Is Important

China's continuing expansion of digital business initiatives and tightening regulatory oversight on data security governance (DSG) have made DRA a required part of assessing how business risks need to be mitigated. DRA analyzes gaps and inconsistencies in DSG policies stemming from controls applied by data security, privacy and identity management products. A DRA is fundamental to DSG's successful implementation and compliance with laws and sector-specific regulations.

Business Impact

A DRA provides insights to security and risk management (SRM) leaders on prioritizing data risks against the organization's risk appetite. It helps leaders design informed risk treatment strategies by identifying deviations in the implemented data security policies and assessing financial business impacts. Conducting DRA aids in fulfilling China's legal requirements in data processing and other sector-specific regulations (e.g., in finance, telecom, government and automotive).

Drivers

- China's national data economy initiatives and regulatory requirements drive public and private organizations to expand DRA's impact evaluation to national security and public interests (e.g., healthcare, transportation and utilities). This happens when important data, a large volume of personal information and cross-border data transfers are involved in the organization's business transaction activities.
- Backed by business leaders, DRA enhances business outcomes by addressing data risks that directly affect business risks, while identifying and evaluating data access needs for business users.
- The financial DRA (FinDRA) process enables business functions to make informed decisions regarding the data security budget. This is done by assessing the financial impact on the business and determining the optimal level of risk mitigation aligned with budgetary limitations and its impact on business outcomes.
- Every decision to mitigate a business-related data risk requires a DRA to establish how each risk might evolve. It also requires a data classification process that can identify data in structured and unstructured formats and leverage security, privacy and business metadata.
- The need to create a data map and undertake DRA analysis with data security posture management (DSPM) products enable the assessment of privileges provided to each user or machine account against the data in scope.
- The creation of a data risk register relies on executing the DRA process and implementing a data-centric security architecture (DCSA) approach. The register is designed to contain assessments of how gaps and inconsistencies in data security controls can lead to business risks.

Obstacles

- Diverse compliance requirements from different regulators demand that a DRA be characterized by different risk vectors. It includes full-scope data security risks, data outbound transfer risks, privacy and technical vulnerabilities. These risk vectors complicate the implementation of a DRA, and make manual DRA processes difficult to fulfill.
- Completing DRA processes requires expertise from different experts and an assessment of the effectiveness of deployed security controls, which is often difficult to acquire.

- Data processing activities evolve with changes in business processes. Point-in-time DRA will not suffice to identify data security risks promptly and sustainably.
- A DRA will succeed only if business leaders support the need for data security controls. However, most organizations in China struggle with insufficient engagement from business and without a successful engagement of stakeholders through a DSG.

User Recommendations

- Adopt process automation to streamline arbitration of DRA processes and generate report templates to address various DRA compliance requirements.
- Employ DSPs or DSPMs to enable DRA as part of routine data security operations.
- Leverage a Data Security Steering Committee (DSSC) to work with all stakeholders facilitating DRA, drawing on committee members' direct knowledge of and insights into business outcomes, business projects' requirements to process datasets and the impacts of business incidents.
- Identify data risks that are not mitigated — e.g., inadequate data residency controls and inconsistent data activity monitoring — and evaluate how these might create business risks and prioritize risk mitigation measures.
- Communicate DRA findings to central enterprise risk management (ERM) and DSSC through a DSG framework to gain business support for changes to staffing and budgets.

Gartner Recommended Reading

Security and Risk Management Leaders' Guide to Data Security in China

Prepare for the Security Assessment of Outbound Data Transfers From China

Innovation Insight: Data Security Posture Management

A Data Risk Assessment Is the Foundation of Data Security Governance

Use the Data Security Governance Framework to Balance Business Needs and Risks

Data Security Platforms

Analysis By: Anson Chen

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Data security platforms (DSPs) aggregate data protection requirements across data types, storage silos and ecosystems, starting with data discovery and classification. DSPs typically protect data by using policy-based authorization controls (e.g., database APIs, dynamic data masking, format-preserving encryption [(FPE] or tokenization). Select DSPs also undertake data activity monitoring or perform data risk assessments.

Why This Is Important

Traditionally, data security has been delivered by disparate products that operate in silos. This has resulted in operational inefficiencies and an inability to support data risk assessments, commercialization of data and innovations and collaborations involving data, for example. DSPs enable centralized deployment of data security policies on both on-premises and cloud-based data stores by connecting previously disparate data security controls and capabilities.

Business Impact

A DSP significantly increases visibility of, and control over, data and its broad usage — for example, in relation to data processing and exchange behaviors, not just narrower, privacy-related compliance goals. It therefore puts organizations in a position to truly secure their data. The increase in visibility and control enables secure data flows between individuals, organizations and governments, and facilitates the implementation of China's National Data Economy Initiatives (Twenty Data Measures).

Drivers

- Data security governance (DSG) is an essential part of staying compliant with the Data Security Law in China. Organizations need an integrated data security platform to support the implementation of DSG and get complete visibility of data residence, circulation and usage. Also, they must be able to implement consistent security policies across disparate products more easily and streamline data risk and compliance assessment processes.
- Enterprise agendas for strengthened data security and privacy are increasingly in competition in terms of their approach to DevSecOps (e.g., test data management). Other competitive areas include open data regulations and advanced analytics enabled by artificial intelligence and machine learning.
- Organizational data is increasingly distributed across different service and trust boundaries, frequently outside traditional on-premises data centers. Data is likely to be processed and stored in private, hybrid and public cloud services of all types — infrastructure-based, platform-based and SaaS. This situation requires organizations to manage their data security far more effectively.
- DSPs support applying consistent data security policies and controls for data products. “Data products” are top of mind for mature clients. This presents a paradigm shift, where the goal is to support higher utilization of “secure data” — data with appropriate guardrails — by making it easier for a diverse set of internal and external consumers to share and use data.

Obstacles

- DSP technology is still nascent to most end users in China. Organizations become aware of it only when they find that their traditional controls no longer suffice or cannot synchronize well. However, substituting a single function product with an integrated platform requires strong business justification, a multiyear transition program, and committed effort and cost.
- Most DSPs can orchestrate well with the security products under the same vendors' original territory. Integration of formerly disparate technologies can be challenging if the buyer's existing product portfolio consists mostly of heterogeneous products from other vendors.
- DSPs have a bias toward structured data. Many businesses would like to protect structured and unstructured data equally. However, leading DSP vendors are slow to provide better support for data discovery, catalog, and classification of unstructured data and file-level encryption.

User Recommendations

- Prioritize DSP investments by assessing DSP for new data security projects. For example, the technology implementation supporting DSG or the transition to data mesh architectures and cloud-based data lakes.
- Prioritize a broad spectrum DSP that provides well-integrated controls combining data stewardship, policies and late-binding access controls. Popular late-binding access controls used by DSPs are cryptographic transform techniques that employ crypto to transform a clear text into an encrypted or less identifiable format (e.g., tokenization and format-preserving encryption [FPE], dynamic data masking [DDM] or proprietary connectors and agents).
- Anticipate coverage gaps or partially resolved data security issues that remain active for a longer time while DSPs are still evolving.
- Choose DSP products offering high levels of integration with heterogeneous products from other vendors, such as a set of APIs based on interoperability standards. This can compensate for coverage gaps.

Sample Vendors

ANKKI; DAS Security; DBSEC; Guanan Info; Hillstone Networks; IBM; NSFOCUS; SkyGuard; Topsec Technologies; Wondersoft

Gartner Recommended Reading

2023 Strategic Roadmap for Data Security Platform Adoption

Innovation Insight: Data Security Posture Management

Market Guide for Data Masking

Market Guide for Data Loss Prevention

Use Enterprise Key Management to Provide Stronger Data Security and Privacy

Data Security Governance

Analysis By: Anson Chen

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Data security governance (DSG) enables the assessment and prioritization of business risks, caused by data security, privacy and compliance issues. This enables organizations to establish data security policies that support business outcomes and balance business needs against associated business risks. These risks arise from security, data residency and privacy issues, as data is processed across ecosystems or shared with partners.

Why This Is Important

DSG enables the assessment, prioritization and mitigation of business risks caused by security, privacy and other compliance issues, as data proliferates across on-premises and multicloud architectures. DSG establishes a balance between business priorities and risk mitigation through data security policies that can be applied across the whole IT architecture so organizations' proprietary datasets can be processed and shared internally and externally, given the prioritized business risks.

Business Impact

DSG offers a balanced approach to define how data is accessed and used to support business performance objectives and client experience, while enforcing appropriate data security and privacy controls to mitigate risks. DSG requires collaboration among security, data and analytics, compliance and business leaders, through a data security steering committee. This would help break down communication barriers and contribute toward business outcomes and compliance with local regulatory requirements.

Drivers

- China's digital development plan announced in February 2023 compels organizations in China to create commercial data value by sharing and trading valuable data assets on top of the protected baseline (see The Central Committee of the Communist Party of China and the State Council issued the Overall Layout Plan for the Construction of Digital China). It is essential to use DSG as a continuous process to manage, assess and prioritize business risks associated with data usage, and create focused data security policies that can mitigate those risks.
- Sustainable enforcement of data security controls requires collaboration across multiple stakeholders from security, data management, legal, compliance and business functions. A set of governance principles, processes and practices needs to be applied to streamline the joint effort, while establishing clear boundaries of responsibilities.
- Implementation of consistent data security policies and controls (e.g., identity access management (IAM), access controls, masking, encryption, auditing, etc.) across a portfolio of datasets is challenging, as multiples internal and external requirements (in terms of privacy, confidentiality, integrity, availability, business purpose and life cycle risks) needs to be considered. DSG helps create data security policies that guide and orchestrate the implementation processes to minimize data security control gaps and inconsistencies.
- No single product in the market mitigates business and data security risks sufficiently, emphasizing the need for centralized creation and coordination of data security policies.
- It is essential to leverage adequate privacy impact assessments (PIAs), data risk assessment (DRA) and outbound data transfer security assessment through DSG to mitigate data residency and sovereignty risks.

Obstacles

- Business stakeholders have fragmented responsibilities for managing data. Security, data and analytics — as well as compliance leaders — have their own agendas and focus on DSG implementation. Unless they agree upon the common DSG operating model and collaboratively create data security policies together with DSG, they will fail to balance business outcomes and risk mitigation.
- The deployment of data security, IAM and application security products are purchased and managed by different leaders. Each product applies independent security controls, as IAM products do not control access to data. Data security products often operate on either unstructured or structured data, and apply controls to specific platforms. It is challenging to deploy consistent data security policies across heterogeneous security products.
- The objectives of implementing DSG in China have a bias toward fulfilling local regulatory requirements, and overlooking business risks mitigation and realization of business outcomes.

User Recommendations

- Consider leveraging the DSSC to reach out to your CIO or risk officer to extend your DSG operating model with connected governance. This would help with the most complex, cross-enterprise and geographic risk governance programs.
- Ensure cooperation and collaboration between the chief data and analytics officer (CDAO), the chief information security officer (CISO) and the data protection officer (DPO) to reduce redundancy and waste in evaluating data management and security.
- Use DSG to create and manage consistent data security policies across your portfolio of datasets, according to the level of business risks defined.
- Consider leveraging data security platforms (DSPs) or data security posture management (DSPM) platforms to automatically identify data security risks and deploy data security policies.
- Use DSG to analyze business risks and their impacts due to specific security monetization choices by using infonomics to evaluate the financial impacts on business outcomes.

Gartner Recommended Reading

Security and Risk Management Leaders' Guide to Data Security in China

Use the Data Security Governance Framework to Balance Business Needs and Risks

4 Critical Steps to Accelerate the Adoption of Data Security Governance

Use a Data Security Steering Committee to Realize Data Security Governance Objectives

Security Leader's Guide to Data Security

Exposure Management

Analysis By: Angela Zhao

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Exposure management (EM) encompasses a set of processes and technologies that allow enterprises to continually and consistently evaluate the visibility, and validate the accessibility and vulnerability of an enterprise's digital assets. EM is governed by an effective continuous threat exposure management (CTEM) program.

Why This Is Important

China is a prime target for cyberattacks due to its economic significance and geopolitical factors. Due to the rapidly expanding attack surface, traditional vulnerability management is not sufficient. An effective EM can reduce the challenges that organizations in China face by inventorying, prioritizing and validating threat exposure. EM also assists organizations in China in complying with cybersecurity regulations that require companies to protect sensitive data and critical infrastructure.

Business Impact

Exposure management governs and prioritizes risk reduction for the modern enterprise that requires assessments of all systems, applications and subscriptions used. In addition, it can:

- Expose the likelihood of exploitation (visibility of the organization's attack surface).
- Inventory and prioritize (vulnerability, threat intel-based, digital assets).
- Validate the potential success of any attack, and if security controls can assist with detecting or preventing them.

Drivers

- China's stringent cybersecurity laws and regulations, such as the Cybersecurity Law and Cybersecurity Requirements for Critical Information Infrastructure Protection, have heightened the focus on managing and reducing exposure (see Information Security Technology Security Protection Requirements for Critical Information Infrastructure).
- Chineses organizations are having an increased volume of applications and cloud services created by digital transformation. This causes expanding attack surfaces and the growing complexity of environments.
- The escalating frequency and sophistication of cyberattacks targeting Chinese organizations have highlighted the urgency of managing exposure to mitigate risks.
- Most commonly, organizations are siloing exposure activities, such as penetration testing, threat intelligence management and vulnerability scanning. These siloed views provide little or no awareness of the complete situation regarding the effective risks that the organization has.
- Innovations such as AI, machine learning and automation are being integrated into exposure management solutions, enhancing their effectiveness and driving interest to organizations in China.
- Lack of scope and understanding of prioritization in exposures, in line with high volumes of security validation findings, is leaving organizations with far too much to do regarding their exposure and little guidance on what to action first.
- A programmatic and repeatable approach to answer the question "how exposed are we?" is necessary for organizations. This must have the aim of allowing reprioritisation of priority, as environments change in a rapidly changeable IT landscape.

Obstacles

- The constantly evolving IT landscapes of organizations in China can complicate the identification and management of all potential exposures. This causes increased scope of exposure management, new complexities and additional budget.
- Many organizations in China struggle with differentiating risk-based vulnerability management and exposure management, which makes them still aim at patching vulnerabilities.
- Processes to manage end-to-end awareness (from visibility of possible attack vectors to response to breaches) is virtually nonexistent in most organizations, which often simply scan and test their networks for compliance reasons.
- There is no effective platform to consolidate the dispersed data across various tools, such as attack surface management, vulnerability assessment (VA) and breach and attack simulation (BAS), and to generate a holistic view of an organization's exposure.

User Recommendations

- Start with realistic objectives and a phased approach, focusing on critical business assets and known high-risk areas, such as external attack surfaces and top threat vectors in China.
- Embrace broader CTEM programs to include unpatchable attack surfaces, rather than simply processing vulnerabilities with VA tools. Supplement patching with configuration management and software upgrades in remediation actions.
- Focus on visibility, as end users must have an awareness of where risks are, and plan to respond to threats — even if the organization has no way to reduce exposure to them.
- Be sure to include assets that your organization doesn't directly own in your exposure management program, such as social media accounts, SaaS applications and data held by supply chain partners.
- Continue security tools and/or data consolidation in this space to simplify day-to-day operational processes.

Gartner Recommended Reading

Implement a Continuous Threat Exposure Management (CTEM) Program

Predicts 2023: Enterprises Must Expand From Threat to Exposure Management

Top Trends in Cybersecurity 2023

Breach and Attack Simulation

Analysis By: Angela Zhao

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Breach and attack simulation (BAS) technologies allow enterprises to gain better visibility of their security posture weak spots by automating the continuous testing of threat vectors such as lateral movement and data exfiltration. BAS complements, but cannot fully replace, red teaming or penetration testing. BAS validates the security posture of organizations by testing their ability to detect a portfolio of simulated attacks run from SaaS platforms, software agents and virtual machines.

Why This Is Important

The key advantage of BAS technologies is to provide automated and consistent assessment of an enterprise's threat vectors. Frequent automated BAS assessments enable organizations to detect gaps in their security posture due to configuration errors, or reevaluate priorities of upcoming security investments. BAS also helps organizations in China identify priorities to build real-combat capabilities and prepare for mandatory security validations (e.g., the national attack and defense drills).

Business Impact

BAS allows organizations to validate the impact of what attack surface assessments and security posture management tools indicate as potential exposure to a specific threat. Organizations can continuously execute these assessments to gain more frequent visibility into a larger percentage of their assets. They can evaluate the efficacy of their security controls and discover attack paths leading to their most critical assets, allowing them to prioritize remediation.

Drivers

- Organizations with establishing cybersecurity validation programs use BAS technologies primarily to ensure consistent, yet improved, security posture over time and across multiple locations.
- BAS tools can integrate with preventive security control technologies, through management APIs or by reading alert logs, enabling security configuration management and improving the visibility of defense gaps.
- BAS provides “safer” validation. It can run in a production environment without affecting data and causing disruption.
- BAS automates assessments that organizations value to prepare for mandatory cybersecurity validations (e.g., compliance penetration tests, China’s national attack and defense drills), or to refocus red team activity on more advanced scenarios.
- IT and business stakeholders often sponsor the deployment of BAS technologies as they perceive it as a safer way to assess the competency of current security controls, their configuration and the incident response processes for the organization. BAS also supports continuous threat exposure management (CTEM) programs by enabling deeper automation of the “validation” step.
- BAS provides a quantifiable and visualized security overview of how each security control contributes to the security posture. This helps guide and optimize security investment.

Obstacles

- BAS requires investment in time for effective configuration, customization to integrate with an organization's security stack and ongoing maintenance. Currently, only higher-maturity organizations in China have the dedicated competency and resources.
- Due to their early stage of maturity, BAS tools are not fully known or understood by Chinese organizations. It would be challenging to prioritize BAS and to explain the need for using BAS on top of existing cybersecurity validations such as penetration tests.
- BAS tools need extensive internal sponsorship, not only from the security team, but from other IT teams, such as networks and applications. Issues that BAS tools discover create complex remediation pathways.
- BAS technologies suffer from increased competition with more adjacent tools adding attack simulation, such as vulnerability management, attach surface management and automated penetration tests. BAS needs to expand and cover more environments, such as cloud infrastructure and SaaS.

User Recommendations

- Prioritize your organization's use cases and focus on simple but common scenarios. Favor the BAS solutions with easy deployment and maintenance, or the vendors that offer expert services to support the BAS implementation initiative.
- Understand the use cases, benefits and challenges of BAS technologies before making a purchasing decision. Integrate BAS into a cybersecurity validation roadmap, as part of a CTEM program.
- Ensure that the results delivered by the BAS products are actionable. Mobilize other IT teams to agree on the remediation action plan.
- Assess the BAS vendors' capabilities to deliver value continually by regularly adding new capabilities, such as external attack surface management (EASM), highlighting changes in the security posture, and providing reports in a form that minimizes diagnostic fatigue.

Sample Vendors

360 Digital Security Group; ASants; Beijing Zhi Qi An Technology; Chaitin Tech; Moyun Technology; NSFOCUS; VUL.AI

Gartner Recommended Reading

Quick Answer: What Are the Top and Niche Use Cases for Breach and Attack Simulation Technology?

Implement a Continuous Threat Exposure Management (CTEM) Program

Top Trends in Cybersecurity 2023

Using Security Testing to Grow and Evolve Your Security Operations

Confidential Computing

Analysis By: Anson Chen, Feng Gao

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Confidential computing is a security mechanism that executes code in a hardware-based trusted execution environment (TEE), also known as an enclave. Enclaves isolate and protect code and data from the host system and the host system's owners, and may also provide code integrity and attestation.

Why This Is Important

- Regulatory requirements in China are pushing enterprises to look for data protection. The Digital China 2023 Plan encourages organizations to create commercial data value on top of the protected baseline.
- Confidential computing combines chip-level TEE with conventional key management and cryptographic protocols. It enables computation facilities — inaccessible to the infrastructure provider — to support projects where cooperation is critical without sharing data or intellectual property (IP).

Business Impact

Confidential computing mitigates data security concerns for highly regulated enterprises and organizations preoccupied with unauthorized, third-party access to data in the public cloud. It facilitates advanced data analytics, business intelligence and training of AI models based on data confidentiality and privacy controls between competitors, data processors and data analysts — which is very difficult to achieve with traditional cryptographic methods.

Drivers

- China's Data Security Law (DSL) and Personal Information Protection Law (PIPL) became effective in 2021. The stringent data security and personal information protection regulations drive the adoption of confidential computing to protect data-in-use, particularly in the public cloud inside and outside China.
- The security specification and technical testing method of TEE have been published by the National Information Security Standardization Technical Committee (TC260) and the China Academy of Information and Communications Technology (CAICT). An increasing number of commercial TEE platforms passed the CAICT assessment — more than 15 platforms prior to 2021.
- Enterprises in China increasingly seek to exchange and process data for analytics, business intelligence (BI) and training of AI models with third parties to maximize the value of data. This drives the adoption of confidential computing to provide secure computing environments — for example, clean rooms — for data exchange and process activities.
- The combination of software and hardware solutions, such as privacy-enhancing computation (PEC) integrated platforms, is increasingly appreciated by users in China. From the PEC vendors' perspective, this combination is considered the perfect solution to overcome performance issues while guaranteeing the promised level of security through adopting confidential computing.
- Competitive concerns are adding to the drivers of confidential computing — not just around personal data, but also IP. This includes the need for confidentiality and protection against third-party access.
- China's 14th Five-Year Plan has increased the number of innovative initiatives on frontier technologies, such as chips, biotechnology and AI. This led to more local chip makers launching CPU and graphics processing unit (GPU) chips supporting TEE based on x86 or TrustZone platforms. This provides heavily regulated organizations with more options for TEE hardware — for example, HYGON, Kunpeng, PHYTIUM and Zhaoxin — and international vendors, such as Intel, Arm and AMD.

Obstacles

- Confidential computing brings potential performance impacts and extra costs. For example, to ensure the existing software stack can run within confidential computing environments, you will have to use special development tools, libraries or APIs. Confidential computing instances based on infrastructure as a service (IaaS) will cost more to run, whether based on Intel Software Guard Extensions (SGX) or Trusted Domain Extensions (TDX), Arm TrustZone, confidential computing architecture (CCA) or other approaches.
- The heterogeneity of the different technology frameworks and the lack of trained staff and understanding of best implementation methods may hinder adoption or weaken deployments.
- Confidential computing isn't just a plug-and-play deployment and should be reserved for high-risk use cases. Depending on the vendor, it may require a high-level effort. However, it offers diminishing marginal security improvement over more pedestrian controls, such as Transport Layer Security (TLS), multifactor authentication (MFA) and customer-controlled key management services.

User Recommendations

- Design or duplicate a sample application using one of the available abstraction mechanisms and deploy it into an instance with an enclave. Perform processing on datasets representing the kinds and amounts of sensitive information you expect in real production workloads. Doing so will help you determine whether confidential computing affects application performance and seek ways to minimize negative results.
- Capitalize on confidential computing vendors whose products have trusted third-party certifications, such as CAICT.
- Depending on the use case and the robustness required, review alternatives that achieve similar protection of sensitive data-in-use, such as multiparty or homomorphic encryption.
- Examine confidential computing for projects in which multiple parties, who might not necessarily trust each other, need to process (but not access) sensitive data so that all parties benefit from the common results. In this scenario, none of the parties should control the TEE.

Sample Vendors

Alibaba Group; Ant Group; Baidu; Huawei; Impulse Online; Intel; Tencent

Gartner Recommended Reading

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Select the Right Key Management as a Service to Mitigate Data Security and Privacy Risks in the Cloud

2022 Strategic Roadmap for Compute Infrastructure

CPS Security in China

Analysis By: Angela Zhao

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Cyber-physical systems (CPS) are engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans). When secure, they enable safe, real-time, reliable, resilient and adaptable performance.

Why This Is Important

Driven by the “digital economy” and “new infrastructure” initiatives, CPS underpins critical infrastructure and sectors, such as transportation, energy, medical care and government affairs. However, there are both legacy infrastructures that were deployed years ago without built-in security and new assets, which are also full of vulnerabilities. It is imperative to improve CPS security by establishing a systematic security protection system to reduce security risks.

Business Impact

CPS, such as operational technology and Internet of Things, are one of the key components in China's digital economy and the 14th Five-Year Plan. Security incidents of CPS could affect citizens, organizations and a government's finance, authority, survival and reputation. Impacts range from breach of personal privacy and safety to the disruption or failure of critical functions, e.g., traffic paralysis, power outage, and medical system failure.

Drivers

- Multiple CPS security-related national standards have been published in China in the recent years, such as The Multi-Level Protection Scheme (MLPS 2.0), GB/T 37971-2019 on Framework of Smart City Security Systems, GB/T 41400-2022 on Industrial Control System Information Security Protection Capability Maturity Model. These standards emphasize CPS security's importance in supporting mission-critical domains from the government perspective.
- The consequences of a CPS security incident go beyond cybersecurity-centric data loss, to include operational shutdowns, environmental impacts, damage and destruction of property and equipment or even personal and public safety risks.
- China is one of the leading countries to develop smart cities. A large number of smart terminals and sensors are connected to the integrated network of the smart city, so CPS are becoming ubiquitous, making them an ideal target of malicious attacks.
- The deployment of AI and IoT sensors technologies involve large amounts of personal and business data and represent an uncharted risk territory. This creates privacy concerns from citizens and partners who expect their data in good custody, and CPS security solutions are needed to ensure the data is well-protected or securely processed.
- The various types of CPS and protocols result in complex and diverse access methods. Unified and effective CPS security management of not only the terminals but also the interfaces of data transmission is needed, to address the risk of information leakage, data eavesdropping, illegal hijacking and tampering.

Obstacles

- CPS are often deployed by business units without consultation with the security team. Lack of overall planning, sufficient resources, cross-department collaboration and clear roles and responsibilities on CPS security management.
- CPS usually composes multiple layers of hardware, software and networks and different protocols, which makes it complex to identify and manage security risks.
- Many CPS in China were designed and deployed before security considerations became a priority, making them vulnerable to attacks. Upgrading or replacing these legacy systems can be difficult and expensive. Many devices lack storage and compute power to facilitate security mechanisms.
- The overall awareness of CPS security management is prioritizing cyber over physical. Physical security is sometimes not addressed enough.
- Though with the existing government standards in place, there is currently a lack of widely accepted standards for organizations to assess and compare security solutions.

User Recommendations

- Educate business executives of the importance of CPS security to digital business initiatives.
- Establish a CPS security governance model, including a steering committee with all stakeholders' involvement, a reasonable organizational structure, and formalized roles and responsibilities.
- Develop, recruit or purchase sufficient competencies for dedicated CPS security management.
- Incorporate security in the full life cycle from development to deployment and ongoing maintenance. For legacy vulnerabilities that cannot be mitigated in a short-term, implement compensating controls such as access control, intrusion detection and prevention, encryption, and network segmentation.
- Evaluate physical security risks such as physical access breach, asset loss and wireless network interference, and implement corresponding controls and monitoring systems.
- Inventory existing CPS security solutions and evaluate the growing list of solutions with identified generic and vertical-specific use cases.

Sample Vendors

360 Digital Security Group; DAS Security; H3C; Huawei; NSFOCUS; QAX; Tianfang Sec; TOPSEC; Venustech

Gartner Recommended Reading

CPS Security Governance — Best Practices From the Front Lines

Predicts 2023: Cyber-Physical Systems Security — Beyond Asset Discovery

Tool: Cyber-Physical Systems Protection Platform Rating and Selection

Cloud Security Resource Pool

Analysis By: Feng Gao

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

The cloud security resource pool is a software-based security set integrated with unified management and monitoring, security orchestration and automation, and compliance management services. It is integrated with various security tools from vendors' ecosystems and can be incorporated into third-party security tools. Additionally, it offers on-demand and flexible usage of security resources.

Why This Is Important

Traditional security tools working in silos are slow in delivery, lack scalability and ineffective monitoring and management. With the increasing cloud adoption in China, organizations require new ways to deliver security capabilities. Moreover, building security capabilities by sourcing security tools from different vendors increases complexity and cost. The cloud security resource pool provides a simple integrated solution to address these challenges for organizations in China.

Business Impact

As a security platform solution, the cloud security resource pool enables organizations to:

- Design enterprise security solutions based on a holistic approach.
- Reduce integration complexity and risks, as most security tools are from the same vendor or its own ecosystem.
- Improve efficiency and reduce the burden on security staff by employing unified management and monitoring, as well as security orchestration and automation services.
- Reduce compliance risks by scanning incompliant configurations and providing required security capabilities by China's regulation.

Drivers

- The increasing adoption of cloud services, especially private cloud in China, requires a simple platform security product to address security needs and protect organizations' cloud assets.
- The cloud security resource pool meets the trend of security vendor consolidation. It provides integrated single-vendor security solutions with open integration to other vendors' tools.
- China's skilled security professionals shortage increases the demand for simplified security tools that deliver unified management and monitoring, security automation and orchestration services, and require fewer integration efforts.
- China's regulations in cybersecurity create demand for security products that can help clients meet compliance requirements. The cloud security resource pool can provide the required security capabilities to meet regulatory prerequisites, such as the multilevel protection scheme (MLPS).
- Local vendors are consolidating fragmented security products into platforms for more efficient and effective growth.

Obstacles

- Lack of standards and most capabilities come from vendors' ecosystems. These factors could restrain the support for third-party security tools. Clients may show strong concerns about vendors' lock-in.
- Both outside and inside deployment modes have challenges. The former brings risks such as latency, throughput bottleneck and single point of failure. The latter requires close integration with cloud technologies, which can lead to further integration issues.
- Its complex integration with multiple technologies makes it difficult for clients to implement and operate the cloud security resources pool.
- Integrated solutions come with bundling pricing, making partial exit very difficult. Clients may be unable to save resources as vendors claim the original price is based on bundling.
- Mainly adopted by government and telecom private clouds, and lack of many use cases in other industries or with public clouds.

User Recommendations

- Consolidate security capabilities by evaluating the cloud security resource pool (single platform) against other consolidated platforms, such as SASE, CNAPP and XDR (multiple platforms).
- Shortlist vendors by first asking about support for cloud technology and integration with existing security tools. Always run a full RFP for shortlisted vendors.
- Conduct proofs of concept for shortlisted vendors by verifying integration with already in-place cloud technology and security tools. In addition to evaluating required security capabilities, scrutinize offerings for unified monitoring and management, scalability, automation and orchestration.
- Avoid vendor lock-in by evaluating API enablement, reviewing support standards and conducting tests with explicit partners for security capabilities the vendor doesn't have.
- Negotiate discounts including dropping a specific component or buying more in the future. Be aware of bundling discounts that look attractive at first but may lock the offer into an inflexible consumption model over time.

Sample Vendors

ABT Networks; Asiainfo Security; DAS Security; H3C; Hillstone Networks; NSFOCUS; QI-ANXIN; River Security; Sangfor Technologies; TOPSEC

Gartner Recommended Reading

Innovation Insight for Cloud Security Resource Pools in China

Software Composition Analysis

Analysis By: Angela Zhao

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Software composition analysis (SCA) products are specialized application security tools that detect open-source software (OSS) and third-party components known to have security vulnerabilities and identify potentially adverse licensing and supply chain risks. It is an essential element in strategies to ensure an organization's software supply chain includes secure and trusted components and, therefore, that the strategy aids in secure application development and assembly.

Why This Is Important

In the digitalization era, the use of open-source components in software development is prevalent in China. SCA promotes using OSS in application development by identifying known vulnerabilities, ensuring components are properly licensed, and advancing trust in the software supply chain. Given the ubiquity of OSS in applications and the potential for significant risk, SCA is an essential activity.

Business Impact

SCA is pivotal in application security to identify known vulnerabilities and supply chain risks in open-source packages and other artifacts. Addressing the integrity of open-source and third-party components at an early stage reduces the need for repeated security assessments, thereby speeding up the development process. License assessments — once the primary use case for SCA — remain an important function for legal and sourcing groups.

Drivers

- With the increasing frequency and severity of cyberattacks, organizations in China are becoming more aware of the vulnerabilities that can arise from third-party software components. Organizations are increasingly focusing on addressing these risks associated with open-source and third-party code in response to high-profile incidents.
- Compliance requirements in China, such as Security Requirements for Supply Chain of Software, demand organizations to thoroughly assess and manage software components.
- Repeated instances of high-impact vulnerabilities in OSS have become pervasive because of the underlying components' broad use across organizations. This, along with ever-present supply chain attacks, demonstrates the need to better understand the risks posed by OSS and commercial software packages.
- The adoption of DevOps practices is growing in China, but the rapid development may lead to overlooking security aspects. Security teams look for SCA tools that can be integrated into DevOps pipelines to help balance agility and security by scanning code early in development.
- New requirements around the ability to address supply chain risks and enhance developer productivity when remediating issues have prompted organizations to revisit their SCA tooling. More effective SCA tools now provide guidance on a preferred update version — balancing stability, remediation of flaws and potential adverse impacts on the functionality of existing code. There are also varied levels of support for software bill of materials (SBOM) analysis and generation — another rapidly emerging requirement.
- Meeting compliance requirements, and ethical and legal standards is a growing concern for organizations, and SCA technology can help ensure developers meet these requirements. SCA technologies help reduce the likelihood of unwanted or unapproved code that creates risks to an organization's intellectual property.

Obstacles

- Many organizations in China currently use SCA tools as a separate step out of the software development process. This slows down software delivery and may even lead to bypassing or ignoring SCA tools before potential security risks are brought into the production environment.
- During the rapid delivery of digital projects in Chinese organizations, different project and product teams may use different source-code warehouses. When a new vulnerability emerges, it is difficult to use SCA tools to trace back to the various code warehouses quickly, resulting in the failure of the emergency response to the incident.
- Organizations in China do not commonly use SCA for continuous monitoring of newly discovered OSS vulnerabilities for applications postdevelopment.
- The use of SCA involves multiple departments, each with different priorities. These include security, development, business, legal and sourcing departments. Sometimes, overall planning and cross-department collaboration are lacking.

User Recommendations

- Implement SCA technologies as a key ingredient of every software security program. Select tools with strong compatibility with development environments and continuous integration/continuous delivery (CI/CD) pipeline.
- Favor SCA tools with strong supply chain risk management support, capable of consuming and generating SBOMs.
- Use SCA tools regularly to audit OSS and third-party component repositories. Whenever OSS and third-party component vulnerability information is disclosed, immediately check whether your software is impacted based on the established repositories.
- Communicate with all stakeholders and evaluate the ability of tools to support multiple use cases when evaluating solutions. Develop alternative interfaces for SCA tools to support different users.

Sample Vendors

Antiy Labs; CodeForce; DAS-Security; Hongjian Technology; MoreSec; Moyun Technology; QAX; Tencent; Venustech; XMIRROR

Gartner Recommended Reading

Critical Capabilities for Application Security Testing

Magic Quadrant for Application Security Testing

Tool: Vendor Identification for Application Security Testing Tools in China

Attack Surface Management

Analysis By: Angela Zhao

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Attack surface management (ASM) involves a combination of people, processes, technologies and services deployed to continuously discover, stock and manage an organization's assets. These assets can be internal and external, and pose digital risks. ASM can help organizations overcome persistent asset visibility and vulnerability challenges. The visibility of attack surfaces can help reduce asset exposure that malicious threat actors could exploit.

Why This Is Important

The digital economy in China has led to an unprecedented increase in the number and complexity of digital assets for most organizations. ASM aggregates asset visibility from other products or services, including digital assets, internet-facing systems and associated exposures, and any potential digital risks. It assists security analysts in continuously identifying known and unknown assets, assessing and reducing exposures, and providing early warnings of threats.

Business Impact

ASM enables security teams to improve basic security hygiene by gaining visibility of digital assets and vulnerabilities, finding security issues that attackers are most likely to exploit, and prioritizing resources to remediate. ASM supports security teams to identify attack paths, visualize security tool coverage, adjust and improve security controls, enhance security posture, and mitigate risks which may impact business operations or reputation.

Drivers

- With the increasing needs of cybersecurity validation (e.g., the national attack and defense drills), organizations in China are interested in understanding what organizations are exposed to from an attacker's view. A full visibility of an organization's potential attack surface and existing security gaps is a foundation.
- Organizations in China usually have scattered asset data and diverse asset types. Streamlining the management of assets across departments becomes a priority for security teams, driving the push for continuous and automated asset discovery processes.
- New risks are presented by digital initiatives such as cloud adoption, agile application development, hybrid working, and cyber-physical systems (CPS) convergence like the Internet of Things (IoT) and operational technology (OT).
- Evolving business landscape and the expansion of public-facing digital assets extend use cases beyond organizational holdings. Scenarios include digital footprinting, brand protection, account takeovers, data leakage detection, and high-value target (e.g., VIP/executive) monitoring. Those demands accelerate the growth of ASM offerings in the Chinese market.
- Equipped with comprehensive visibility, ASM opens up possibilities for organizations to strategize their asset information's utilization, forming a solid foundation for numerous cybersecurity initiatives.
- The market of external attack surface management (EASM) and digital risk protection services (DRPS) are being consolidated in China, enabling users to get an integrated set of capabilities in one solution. This supports users' desire to build exposure management programs.

Obstacles

- Users are struggling with “yet another” tool; there are overlaps with cyber asset attack surface management (CAASM) vendors and an organization’s existing tools for asset inventory and vulnerability management.
- The asset visibility and dynamic management capabilities of ASM solutions in China are still in an early stage. Most ASM products in China have limitations to integrate with third-party data sources and require a lot of human effort to verify different data.
- The priority setting rules in ASM solutions are relatively simple, or cannot support customer customization. The level of risk is primarily determined by the level of vulnerability and asset criticality, lacking context correlations.
- Many ASM solutions focus on the organization’s own IT environment, but lack visibility for cloud and CPS.
- The ultimate goal of attack surface management is to reduce exposure. It is difficult to rely on ASM products alone, but also needs the involvement of security professionals.

User Recommendations

- Check existing security solutions gaps in attack surface visibility against cybersecurity validation results (e.g., the national attack and defense drills). If purchasing another new tool is required, leverage proof-of-concept opportunities in order to “try before you buy.”
- Investigate ASM’s capabilities to integrate with the organization’s existing tools and automate the cross-validation and deduplication.
- Assess the solution maturity to define customized risk models or integrate ASM outputs with other security insights. This will improve risk evaluation and decisions.
- Favor vendors that understand Chinese cloud services, IoT, OT and IT systems capabilities, particularly for organizations that own assets on the cloud and in CPS environments.
- Evaluate and build the competency of your security teams to ensure there are appropriate resources that you can use to deal with identified attack surfaces. Integrate with security tools that perform responses where possible for remediation actions.

Sample Vendors

360 Digital Security; Beijing Huashun Xin'an Technology; Chaitin Tech; MoreSec Technology; NSFOCUS; QAX; Tencent; ThreatBook; Tophant; VUL.AI

Gartner Recommended Reading

Innovation Insight for Attack Surface Management

Emerging Tech: Security — The Future of Attack Surface Management Supports Exposure Management

Implement a Continuous Threat Exposure Management (CTEM) Program

At the Peak

Privacy in China

Analysis By: Bernard Woo, Anson Chen

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Privacy in China is regulated by the Personal Information Protection Law (PIPL), along with accompanying sector-specific, cross-sector and cross-border data transfer regulations. While similarities with privacy laws such as the EU's General Data Protection Regulation (GDPR) exist, there are distinct requirements and enforcement is guided by multiple regulatory bodies.

Why This Is Important

The PIPL significantly alters the legal and regulatory landscape in China. Previous enforcement had been based primarily on provisions in the cybersecurity law and personal information security standard. The PIPL offers Chinese citizens a much more expansive framework for protecting personal data about them, and includes the potential for powerful financial sanctions: 5% of previous year's annual revenue or 50 million renminbi, whichever is higher.

Business Impact

The compliance risks and potential penalties for violations are real. Business leaders must account for privacy in their market growth strategy, especially in sectors related to national security, such as financial services or multinational operations expanding in China.

While the regulatory framework is similar to principles found in laws in other regions, complex data localization, consent and cross-border transfer requirements must be carefully analyzed and addressed in the privacy strategy.

Drivers

The current regulatory framework follows a path of continued evolution to drive a balance between innovation and societal well-being when processing personal data. Consider the series of laws that have been implemented since 2017:

- 2017 — The Cyber Security Law (CSL) of the People's Republic of China (The National People's Congress of the People's Republic of China) (an English translation is available from Stanford University's DigiChina Project) began establishing requirements around the processing of personal data.
- 2018 — The CSL was supported by the Personal Information Security Specification, also known as, "Privacy Standard" (Secretariat of National Information Security Standardization Technical Committee) and the Guideline for Internet Personal Information Security Protection.
- 2019 — The Multi-Level Protection Scheme (MLPS) 2.0 (Reed Smith), which describes security practices for IT systems, including those that process personal data, went into effect.
- 2020 — The Chinese Civil Code (State Council of the People's Republic of China) was adopted that provided individuals with the right to privacy.
- 2021 — The PIPL (Stanford University' DigiChina Project) went into effect.
- 2022 — Cross-border data transfer (CBDT) regulations were established (see Prepare for the Security Assessment of Outbound Data Transfers From China and Office of the Central Cyberspace Affairs Commission [an English translation is available from Stanford University's DigiChina Project]).
- 2023 — China has indicated a desire to create a new regulator with local branches that would together enforce regulations related to the management of data in the country, adding another set of regulatory bodies to the mix (see announcement from Big Data Administration of Hainan Province).

Regulators have shown a desire to enforce penalties for noncompliance, as witnessed by the $1.2 billion fine issued to the rideshare company DiDi Global.

Obstacles

- The PIPL indicates a heavy reliance on obtaining individual consent for a range of processing activities, with organizations bearing the burden of proof.

- The CBDT regulations dictate strict controls around cross-border data transfers. This creates significant burdens for strategies managing the flow of data in or out of the country. Further, the regulations apply to both consumer and employee personal data.
- The regulatory environment includes IT security frameworks, such as the MLPS 2.0., meaning assessment and certification by locally approved entities is needed. As such, local partnerships are critical in helping organizations understand all applicable requirements (e.g., CBDT), implement correct measures and keep up with changes in a rapidly evolving environment.
- Significant additional investments may be required. Possible new technology investments include IT infrastructure, application architecture and data management solutions. New roles, controls and policies would also be needed.

User Recommendations

- Extend existing corporate privacy practices to incorporate China's regulatory requirements where appropriate and establish new processes when required.
- Discover, map and classify personal data being processed to lay the foundation for gaining control over processing activities and addressing localization requirements.
- Focus on building a privacy user experience (UX) to bring transparency to personal data processing activities, collect and manage user consent plus preferences, and support subject rights requests.
- Establish and document purposes for processing personal data as part of privacy impact assessment (PIA) process; ensure a minimum amount of data is processed for each purpose.
- Implement controls to protect personal data commensurate with that information's sensitivity, such as encryption, data masking/anonymization or access controls (including logging and monitoring).
- Ensure data localization and outbound transfer requirements are addressed within the overall business strategy.

Gartner Recommended Reading

Still a Moving Target — What to Do With the Chinese Data Security Law

State of Privacy — China

Executive Leaders: Top 10 Questions About Digital Business in China, 2022

Security and Risk Management Leaders' Guide to Data Security in China

SASE

Analysis By: Evan Zeng, Feng Gao

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Secure access service edge (SASE) delivers converged network and security-as-a-service capabilities such as SD-WAN, SWG, CASB, next-generation firewall (NGFW) and zero trust network access (ZTNA). In addition to its global use cases, in China, SASE supports community cloud and customers' on-premises access security use cases. CASB is a recommended rather than a core capability, as enterprises in China adopt cloud PaaS and SaaS services less than their worldwide peers.

Why This Is Important

SASE is a key enabler of digital business transformation, increasing visibility, connectivity and security by using a platform approach, rather than a point-product approach, to deliver network and security services. In China, SASE platforms are often bundled with commonly needed capabilities, such as low-latency access to cloud (public and community clouds) and pay-as-you-go pricing models, increasing its importance.

Business Impact

SASE delivers:

- A platform approach for unified management across WAN and security, which significantly reduces the complexity of operations and enhances cybersecurity capabilities.
- A security and networking platform with local footprints in China, which can meet compliance requirements and can reduce WAN infrastructure and security services costs.

- Enhanced security and governance for enterprise digital assets at data centers, cloud and edge locations.

Drivers

- Enterprise digital business transformation needs secure connectivity to distributed hosting and cloud-based workloads without increasing complexity and buying overlapping capabilities.
- Chinese enterprises cite zero trust networks and SD-WAN as important capabilities, both of which are core capabilities in SASE solutions.
- SASE provides as-a-service infrastructure and reduces procurement and deployment time for customers. It also enhances security protection and shortens remediation time to provide much better observability for cloud and edge-based resources.
- A distributed digital workforce and similar dynamic access needs of modern businesses are common and widespread in China. SASE brings a more complete and transformative approach to network security, which is better-suited to these use cases than legacy solutions.

Obstacles

- Organizational silos, incumbent investments, cultural change, maturity of security management and skills gaps are major obstacles to SASE adoption in China.
- Enterprises in China prefer on-premises environments more due to the organizational and regulatory risks of public cloud, making the cloud-delivered architecture of SASE less relevant in China.
- Indigenous SASE offerings are generally immature in China, as most solutions still lack fully converged capabilities such as a unified management platform and policy control.
- Due to security concerns and cloud security service regulation in China, non-China-based SASE providers require considerable time to navigate the regulatory and business landscape to decide their business strategy and how to land their SASE solutions into China.
- Managed SASE offerings — a different SASE adoption option — are still at an early stage in China because they are low priority for most technology providers.

User Recommendations

- Adopt SASE offerings to deliver the business benefits of security and network vendor consolidation.
- Involve the chief information security officer (CISO) as well as security and network leaders when evaluating SASE offerings and roadmaps from incumbent and emerging vendors to ensure an integrated platform approach.
- Avoid SASE solutions with more than two participating vendors, favoring single vendors where possible. Only consider SASE offerings with three or more vendors when they are offered as a managed service.
- Give higher consideration to vendor offerings that deliver unified management and operation approaches across services in the SASE platforms.
- Shortlist SASE vendors that can not only address global use cases but also China-specific use cases such as the global SaaS acceleration across China's internet borders.
- Combine branch-office access and remote access into a single implementation to ensure consistent policies and minimize the numbers of vendors required. Deploy ZTNA to augment or replace legacy VPN.

Sample Vendors

Alibaba Cloud; Huawei; NSFOCUS; QAX; Sangfor Technologies; Topsec; Wangsu

Gartner Recommended Reading

Accelerate SASE Adoption by Leveraging the Security Vendor Consolidation Wave

Emerging Tech: Leverage Cloud Connect Infrastructure to Improve Connectivity Experience of Cloud Workloads for SASE Solutions

Market Guide for Single-Vendor SASE

2022 Strategic Roadmap for SASE Convergence

Security Service Edge

Analysis By: Feng Gao, John Watts

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Security service edge (SSE) secures access to the web, cloud services and private applications. Capabilities include adaptive access control, data security, visibility and control. Further capabilities include an advanced threat defense and acceptable use control enforced by network-based and API-based integrations. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.

Why This Is Important

SSE improves organizational flexibility to secure the usage of web, cloud services and remote work. SSE offerings are the convergence of security functions (at least, secure web gateways [SWGs] and zero trust network access [ZTNA]) in China, with additional SaaS security to reduce complexity and improve user experience. They can be delivered on-premises or from the cloud. When SSE is paired with software-defined WAN (SD-WAN), it becomes the secure access service edge (SASE) architecture.

Business Impact

Hybrid work continues to drive the adoption of public cloud services, especially of SaaS applications. Both hybrid work and the adoption of public cloud services remain business enablers for most Gartner clients. SSE allows the organization to support anytime-anywhere workers by using a cloud-centric approach to enforce a security policy when accessing the web, cloud services and private applications. Simultaneously, SSE reduces the administrative complexity of running multiple products.

Drivers

- Increasing cloud and hybrid cloud adoption in China needs secure remote access for distributed organizations' digital assets.
- Administrators can have enhanced visibility on user traffic and a single configuration and monitoring location for this traffic.
- SSE allows organizations to implement a posture based on identity and context at the edge.
- SSE provides improved visibility and control for data access and transfer to reduce compliance risks under China's security regulations, such as outbound data transfer regulation.
- By consolidating vendors, organizations reduce complexity and costs used to enforce security policy.
- SSE allows doing sensitive data inspection and malware inspection in parallel, leading to a better performance and more consistent configuration than doing them separately.
- An adaptive access can take into account more input signals and be more consistently enforced, regardless of the application location or type.
- Organizations look for deeper security capabilities when building a SASE architecture compared to vendors that may have a minimal set of security features as part of their SD-WAN offering.

Obstacles

- As the market is being formed by the convergence of capabilities, vendors may be strong in certain capabilities and weak in others, such as visibility and data security. In China, most vendors still lack overall tight integration between SSE capabilities or with SD-WAN vendors.
- Most vendors in China do not provide sufficiently sensitive data identification and protection to manage business risks.
- Lack of SaaS security and integrations due to limited API available from SaaS providers in China. However, businesses need this visibility and protection.
- Clients in China prefer on-premises deployment, which is still tied to local network infrastructure and connectivity.
- Poorly managed or implemented on-premises appliances (SSE gateways) introduce additional attack surfaces.
- Most local vendors are fully China-focused and have limited support for global rollout.
- Switching costs from incumbent vendors or timing of contract expirations prohibit near-term consolidation.

User Recommendations

- Replace stand-alone security products, such as SWGs and VPNs, by adopting SSE to reduce complexity and fill the gaps with SSE's various capabilities.
- In favor of cloud-based delivery of SSE, which has more comprehensive control with better user experience, unless there is regulation prohibition.
- Avoid outbound data transfer issues by selecting vendors who have China local point of presence (POP) and process data locally.
- Actively engage with initiatives for branch office transformation, SD-WAN and Multiprotocol Label Switching (MPLS) offload to integrate cloud-based SSE into the scope of project planning.

Sample Vendors

NSFOCUS; Palo Alto Networks; Qianxin; Sangfor Technologies; Wangsu-CDNetworks

Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Adopt Security Service Edge (SSE) to Replace Stand-Alone SWG, CASB and ZTNA Products

Sliding into the Trough

IoT Authentication

Analysis By: Mia Yu

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Internet of Things (IoT) authentication is the mechanism of establishing trust in the identity of a thing (typically a device) interacting with other entities, such as devices, applications, cloud services or gateways operating in an IoT environment. Authentication in IoT takes into account potential resource constraints of IoT devices, the bandwidth limitations of networks they operate within and the mechanized nature of interaction among various IoT entities.

Why This Is Important

From automotive to smart houses and smart buildings, the smart appliance market, industrial IoT (IIoT), operational technology (OT) and onward, IoT is exploding as a market. However, these connected devices can bridge cyber and physical worlds, and open up entirely new threat vectors. Sound IoT security requires strong identity in IoT devices coupled with strong IoT authentication, with the goal of mitigating and minimizing cyberattacks, and/or other issues and vulnerabilities.

Business Impact

IoT authentication can mitigate:

- Attacks against connected devices that could lead to disruption in product or service offerings.
- Attacks against industrial devices that lead to operational impacts and, potentially, catastrophic events in safety-critical production areas.

Drivers

- China Academy of Information and Communications Technology predicts the number of IoT connections will reach up to 8 billion by 2025 in China (see Internet of Things White Paper [2020]). The increasing IoT connections will drive attention and spend on IoT authentication methods for security concerns.
- Secure credential storage and rotation approaches for IoT authentication are sorely needed. Ongoing work for defining this, as well as for identifying devices, is happening in the public sector, such as healthcare in China (see China Food and Drug Administration Releases Technical Review Guidelines for Cybersecurity Registration of Medical Devices).
- Certificates continue to be the primary way devices are identified and authenticated. Public key infrastructure (PKI) vendors in China, such as BeijingCA, TrustAsia invest and focus in this space leveraging their PKI capabilities to solve IoT authentication use cases.
- Global standards helping to provide consistent approaches include RFC 8628, OAuth 2.0 Device Authorization Grant extension and the ACE working group within the Internet Engineering Task Force (IETF). This also specifies how OAuth 2.0-based authentication and authorization exchanges can be optimized for constrained devices for use over Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT) and other messaging protocols.
- China local regulations and standards drive organizations' investment on IoT identities and authentications, such as the multi level protection scheme (MLPS) 2.0 basic requirement for trusted computing, and the extended requirement for IoT.

Obstacles

- The IoT security landscape is complex, including determining the right people, process and technology to employ due to a fragmented market, and difficulties productizing due to inconsistent device types and operating environments.
- Some authentication methods are not good candidates due to certain IoT devices that are resource- or feature-constrained with low computing power and limited secure storage capacity.
- Support of authentication methods via IoT platforms is immature or incomplete. Use-case areas, such as IIoT, have protocols that are not interoperable with each other and, many times, not operable with standards like TCP/IP, creating ongoing challenges for authentication approaches. In addition, most IIoT systems are self-contained and use native proprietary means for authentication.

User Recommendations

- Discover and categorize IoT devices and networks, and discern the capabilities and security requirements for each category of them. Leverage device- and network-based contextual information to gain additional assurance.
- Evaluate and adopt authentication frameworks that can support the authentication needs of different device types across the IoT realms in operation.
- Utilize trusted computing techniques (i.e., hardware root of trust) to help to protect against physical attacks on devices and sensors, and against the external software attacks that could enable unauthorized reading, analyzing and manipulating of software code. When doing so, critical information infrastructure operators (CIIOs) in China should pay attention to China's cryptographic law when choosing trusted computing techniques and vendors.
- Use fusion teams to manage the disparate technical and regulatory requirements of IoT projects and implementations (see Fusion Teams: A Proven Model for Digital Delivery).

Sample Vendors

Alibaba Cloud; BeijingCA; ParaView; QI-ANXIN; TianFang Security; TrustAsia

Gartner Recommended Reading

Innovation Insight for Cyber-Physical Systems Protection Platforms

Managing Machine Identities, Secrets, Keys and Certificates

Secure Multiparty Computation

Analysis By: Anson Chen

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Secure multiparty computation (SMPC) is a method of distributed computing and cryptography that enables entities (e.g., applications, individuals, organizations or devices) to work with data, while keeping data or encryption keys in a protected state. Specifically, SMPC allows multiple entities to share insights while keeping identifiable or otherwise sensitive data confidential from each other.

Why This Is Important

The challenge of achieving a balance between data sharing/exchange and privacy is further complicated by new regulations in China (e.g., the Personal Information Protection Law and Data Security Law) and local business goals. Traditionally, data protection has focused on securing data-at-rest and in-transit. However, SMPC-based methods introduce data protection in-use. It enables the processing of data confidentially in analytics and business intelligence, using untrusted computing environments.

Business Impact

SMPC enables data analysis in an encrypted state and allows multiple entities to share insights using data protected in-use — though with specialized software. SMPC supports the secure enablement of business, thus allowing organizations to uncover and exchange information while addressing security and privacy concerns. This can be applied to many data analytics and AI-based use cases, such as credit risk detection, joint marketing and customer profiling, and joint medical research, etc.

Drivers

- China's Personal Information Protection Law (PIPL) and Data Security Law (DSL) became effective in 2021. Accordingly, the stringent data security and personal information protection regulations drive SMPC adoption to protect data-in-use, particularly in the exchange of sensitive data with untrusted third parties.
- Traditional implementation of data-at-rest encryption does not provide strong protection against data theft and breaches in the context of data-in-use and data-sharing scenarios.
- New use cases — such as big data analytics, AI or machine learning (ML) model training — present further privacy and cybersecurity concerns that require data-in-use protection.
- Increasing SMPC successful proofs of concept (POCs) in finance, healthcare and the public sectors lead to more practical implementations. POCs in finance include joint risk control and joint marketing and, in healthcare, include cross-institution medical research. Finally, the public sector comprises cross-agency data sharing, open government data and regulated data trading.
- More open-source SMPC projects (e.g., CrypTen, OpenCheetah, PySyft, Rosetta and SecretFlow) and available industry standards provide lower entry barriers for new joiners. Also, they lay the basis for cross-platform integration among siloed data sources in the long term.

Obstacles

- SMPC algorithms can be very latency-sensitive. In some cases, performance might not meet client requirements or expectations.
- Most SMPC implementation projects are highly customized for individual clients, from business processes to data and systems. This hinders SMPC adoption, leading to elevated efforts and costs.
- Similar to homomorphic encryption, SMPC requires specialized, recoded tools to conduct data analytics. The lack of understanding of the specialized nature of the technology inhibits adoption by end users.
- SMPC products may have limitations and exclude certain data types, such as floating points. They may also have issues with recursive ML.
- When compared with existing techniques (i.e., cryptography based on hardware-generated and stored keys), end customers could have potential issues with audits, like when their accreditation authority isn't familiar with SMPC.

User Recommendations

- Consider integrated hardware (Trusted Execution Environment-TEE) and SMPC-software solutions that can alleviate performance issues faced by pure-software SMPC technologies, while guaranteeing the promised level of security and ease of use.
- Work with developers, architects and data analysts to establish a high-level position on SMPC relevance and a vision for future adoption, including POCs.
- Evaluate use cases focusing on data confidentiality in a cloud environment and privacy-enhancing (personal) data analytics initiatives.
- Look at secure and private data mining for data and analytics use cases, including data lake security and blockchain security — for example, wallet protection and quorum-based multisignature operations.
- Engage with vendors whose SMPC products have been certified by trusted third parties from security, performance, functionality and usability perspectives. Examples of trusted third parties include the China Academy of Information and Communications Technology (CAICT), the Bank Card Test Center (BCTC) and the China Financial Certification Authority (CFCA).

Sample Vendors

Alibaba Cloud; Ant Group; AsiaInfo; Baidu; BaseBit.ai; Hua Kong TsingJiao; InsightOne; Nuowei Tech; Tencent Cloud; WeBank

Gartner Recommended Reading

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Climbing the Slope

Zero Trust Network Access

Analysis By: Feng Gao, Thomas Lintemuth

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Gartner defines zero trust network access (ZTNA) as products and services that create an identity- and context-based, logical-access boundary that encompasses an enterprise user and an internally hosted application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a collection of named entities, limiting lateral movement in the network.

Why This Is Important

ZTNA is a technology for enabling dynamic user-to-application segmentation through a trust broker to enforce a security policy that allows organizations to hide private applications and services, and enforce a least-privilege access model for applications. In China, it reduces the surface area for attack by creating individualized “virtual perimeters” that not only encompass only the user, the device and the application, but also the data.

Business Impact

ZTNA logically separates the source user/device from the destination application to mitigate full network access and reduce the attack surface within the organization. This improves user experience (UX) and remote access flexibility, while enabling dynamic, granular user-to-application segmentation through simplified policy management. In China, ZTNA replaces VPN to provide improved security posture and data security for remote work under increasingly strict security regulations.

Drivers

- The rise of zero trust initiatives within organizations has led to the need for more precise access and session control in on-premises and cloud applications.

- There is an increasing need to modernize and simplify traditional VPN deployments that were optimized for static user locations connecting to data center environments rather than applications, services and data located outside an enterprise.
- China's data regulation has led organizations to seek a more secure user access to data solution — especially under hybrid work environments.
- Some highly regulated scenarios, such as connecting to regulatory systems in China, require isolated network access, while users don't want a separate endpoint.
- Some organizations need to acquire the ability to observe application access patterns before enforcing granular controls.
- Organizations have a need to connect third parties, such as suppliers, vendors and contractors to applications securely without exposing their entire networks over VPNs — or to connect the applications to the internet for access.

Obstacles

- **Cost:** ZTNA is typically licensed per named user on a per-user/per-year basis at a price roughly twice or three times that of traditional VPNs.
- **Weak identity and access management (IAM):** Organizations with weak IAM find it challenging to either implement ZTNA and end up with another VPN, or long-term coexistence with VPN.
- **Concern about physical data location:** Cloud-based trust brokers (whose operations are outside of China) are not preferred in China due to concerns about data security. The on-premises-only ZTNA deployment limits its benefits, like high availability and quick expansion of capacities.
- **Lack of DLP Capabilities:** Most vendors lack DLP capabilities with very weak data security, while data security is a top concern for organizations in China. This reduces the client's interest to adopt ZTNA.
- **Granularity of access policy:** Organizations must map application access for users, but many lack this understanding and end up with access rules which are either too granular or not granular enough.

User Recommendations

- Prefer SaaS ZTNA and adopt on-premises ZTNA only if there is a regulatory requirement.

- Ensure SaaS ZTNA vendors by the number of POPs within China mainland for redundancy, and avoid outbound data transfer.
- Adopt device application sandboxing only in specific user scenarios, such as development or meeting regulation requirements.
- Evaluate ZTNA products by focusing on DLP, as most vendors lack DLP capabilities, especially for Chinese content.
- Align ZTNA vendor choice with security service edge (SSE) vendor choice to support unified security controls for hybrid workers and remote branches, and ZTNA policies with the organization's zero trust strategy. Measure risk reduction using outcome-driven metrics.
- Demand universal ZTNA capabilities from vendors offering secure remote access to unify access control policies both on- and off-premises with added Internet of Things (IoT) support to replace legacy network access control (NAC) or software-defined network (SDN) implementations.

Sample Vendors

Alibaba Cloud; Chiansec; Cloudaemon; CloudDeep Technology; DataCloak; NSFOCUS; Paraview Software; Tencent Cloud; Topsec

Gartner Recommended Reading

Market Guide for Zero Trust Network Access

How to Select the Right ZTNA Offering

7 Effective Steps for Implementing Zero Trust Network Access

2023 Strategic Roadmap for Zero Trust Security Program Implementation

2022 Strategic Roadmap for SASE Convergence

Data Classification

Analysis By: Anson Chen

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Data classification is the process of organizing information assets using an agreed-upon categorization, taxonomy or ontology. This can include applying a tag or label to a data object to facilitate its use and governance, employing controls during its life cycle or activating metadata using data fabric. Typically, data classification results in a large repository of useful metadata for making informed decisions.

Why This Is Important

Data classification facilitates effective and efficient data prioritization of data within data governance and data security programs concerned with value, access, privacy, storage, ethics, quality and retention. China's data security regulatory requirements make data classification a vital step for security, data governance and compliance programs. Data classification helps organizations distinguish the sensitivity of the data and improves the effectiveness of data protection controls.

Business Impact

Data classification augments analytics on a dataset, structures data within repositories and allows immediate control over the use of data assets. Security controls such as data loss prevention (DLP) and data access governance (DAG) benefit enormously from data classification or labeling. Data classification enables organizations to meet regulatory compliance obligations cost-effectively by making data easier to find and validate while avoiding overprotection and retention.

Drivers

- The current legal and geopolitical situation has increased concerns regarding data residency and sovereignty, particularly for important data and personal information. However, the inefficiency of current firefighting data security governance practices boosted the desire to streamline and automate these processes, starting from data classification.
- The maturing data classification approaches, which include classification by type, owner, regulation, sensitivity and retention requirement, enable organizations to focus their security, privacy and analytics efforts on important datasets and their classification.
- The emergence of automated data classification tools featured with predefined industry-specific categories — for example, for finance, telecommunications, healthcare and government — lowers the amount of business and security knowledge required to initiate data classification programs.

Obstacles

- Legacy data classification initiatives have often failed because of insufficient training and dependence on user-driven classification.
- Data classification efforts mainly reflect a security-centric mindset. This means their purposes are not explained to users using business language and context, which results in low levels of engagement.
- Although many vendors offer automated data classification tools that can classify data more accurately while minimizing user effort, the accuracy of results does not meet expectations. This applies especially to machine learning or artificial intelligence algorithms for which models require ongoing training.
- From a compliance perspective, organizations not operating in heavily regulated industries and without classification standards published by the industry regulators might find it difficult to measure and justify the effectiveness of data classification results.

User Recommendations

- Determine organizationwide data classification use cases and efforts by conducting a thorough assessment of the types and sensitivity of data present within the organization and collaborating with business departments and data analytics teams to identify specific use cases where data classification is crucial.
- Implement user training and a combination of user-driven and automated data classification as part of a data security governance program.
- Analyze data classification guidance and standards released by industry regulators or national standard committees to develop a data classification scheme that aligns with regulatory requirements in China.
- Prioritize data classification tools that can be better integrated and interoperable with other data security technologies — such as anonymization, encryption, DLP and data security platforms (DSPs). Also, other aspects include richer built-in categorization templates and flexible self-defined tagging and labeling.

Sample Vendors

DAS Security; Guan An Info.; Meichuang Technology; NSFOCUS; Quanzhi Technology; Topsec Technologies; Wondersoft

Gartner Recommended Reading

Still a Moving Target — What to Do With the Chinese Data Security Law

Building Effective Data Classification and Handling Documents

Case Study: An Active Metadata Augmented Data Classification System to Boost Analytics Efficiency

Improving Unstructured Data Security With Classification

How to Succeed With Data Classification Using Modern Approaches

Situational Awareness

Analysis By: Angela Zhao

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Situational awareness technologies in China are modern, centralized and evolved versions of security information and event management (SIEM) platforms. They integrate with other security tools and collect data from assets, network traffic, logs, vulnerabilities, user behaviors and threats. Situational awareness technologies gather data to analyze and display the security situation of the organization, and then predict future trends.

Why This Is Important

Aggregating and standardizing security data to centralize and visualize an organization's security situation is a core element of effective security programs. Situational awareness technology can support security operations centers (SOCs) to identify, prioritize and investigate security incidents. The broad-based visibility is the basis for SOCs to make decisions in daily security operations.

Business Impact

Situational awareness platforms can help SOCs identify and process information in near real time or real time, and visualize the holistic security posture of an organization. Moreover, built-in threat intelligence and threat hunting functions can support SOCs to anticipate what might happen and develop effective protection measures. SOCs can unify security information in a single console — that is, a situational awareness platform — instead of logging onto different tools.

Drivers

- Large organizations possessing sensitive data are at a higher risk of being targeted by cyberattacks due to the expansive nature of their systems and the value of their data. Consequently, these organizations have a pressing necessity to use situational awareness solutions as a foundational technology within their SOCs.
- In 2023, a national standard General Technical Requirements for Network Security Situational Awareness was introduced in China. This development is playing a pivotal role in streamlining the market and fostering the advancement of technological maturity.
- The landscape of cybersecurity risks is continuously evolving in terms of diversity, scalability, complexity and continuity. The growing reliance on the digital realm has significantly accentuated the demand for situational awareness technologies because they offer a risk assessment of potential cybersecurity threats and deliver proactive responses.
- Modern SOC teams need a centralized platform that consolidates real-time information from diverse tools, enabling them to efficiently coordinate security procedures and allocate resources.

Obstacles

- The naming, capabilities and functionalities can vary across situational awareness solutions. This often leads to challenges for end-user organizations when it comes to making purchasing decisions.
- There are products that provide partial functions of situational awareness technologies, causing increased buyer confusion.
- Getting situational awareness solutions to perform well against detecting attacks requires sufficient staffing and skills. Many organizations in China have resource shortages and cannot support 24/7 monitoring, analysis and incident handling.
- The effect of situational awareness technology depends not only on its own functions and configurations, but also on front-end telemetry data. At present, additional costs are involved when situational awareness solutions are integrated with third-party tools provided by a different vendor.

User Recommendations

- Define and plan for the monitoring objectives that best meet the organization's requirements. Use those requirements to correctly identify purchasing criteria such as analysis methods, performance, sizing and retention.
- Evaluate whether a situational awareness solution can mitigate the gaps in the existing technology stack. Request live demos, case studies and proofs of concept.
- Allocate dedicated staff to execute on the detection and response use cases on situational awareness solutions and reach the organization's objectives. Alternatively, engage in a co-managed partnership with security services providers as an extension of the internal team.
- Choose a situational awareness solution that supports Open API and seamless integration if your existing security technology stack is complex. Negotiate clear terms and clauses related to integration efforts and costs to minimize unexpected expenses.

Sample Vendors

360 Digital Security Group; H3C; Hillstone Networks; Huawei; NSFOCUS; QAX; Sangfor Technologies; Tencent; Topsec Technologies Group; Venustech

Gartner Recommended Reading

Magic Quadrant for Security Information and Event Management

Critical Capabilities for Security Information and Event Management

Cloud Workload Protection Platforms

Analysis By: Feng Gao, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Cloud workload protection platforms (CWPPs) protect workloads in hybrid and cloud deployments. CWPPs provide consistent visibility and control over physical machines, virtual machines, containers and serverless workloads, regardless of location. CWPP offerings protect the workload using a combination of system integrity protection, application control, behavioral monitoring, intrusion prevention and optional anti-malware protection.

Why This Is Important

Organizations in China prefer hybrid or private clouds, which drives the need for workload protection tools that support public and private clouds, and on-premises data centers. Simply using a solution designed for on-premises data centers or end-user endpoints is a poor approach to these diverse workloads. Cloud workload protection platforms can maintain the visibility, control and integrity of the workload at runtime and are integrated into the workload creation toolchain.

Business Impact

Cloud services play a critical role in digitalization for organizations in China. Also, cloud hosting protection has become an equally critical strategy to help organizations meet the unique Chinese cloud security requirements, such as high private cloud and hybrid cloud adoption. Accordingly, CWPPs differ significantly from end-user systems. They provide consistent cloud protection for container and serverless workloads, traditional data centers and infrastructure as a service (IaaS).

Drivers

- Increasing cloud adoption in China drives the need to protect ever-increasing cloud workloads. Moreover, the high adoption of hybrid and private clouds requires a workload protection tool that can cover public and private clouds, and on-premises data centers.
- There is a need to address the speed, scale and complexity of cloud workload protection tools to integrate them with cloud toolchains.
- Workloads are no longer exclusively hosted within organizations' traditional physical perimeters and are increasingly deployed across platforms. This increases the need for runtime visibility to all workloads, regardless of the types and locations.
- Simply using a solution designed for on-premises data centers or end-user endpoint protection is suboptimal. Thus, many vendors — including both startups and established endpoint protection platform (EPP) vendors — are now explicitly targeting the CWPP market.
- Cloud server workload protection strategies must be based on a foundation of solid operational hygiene — including proper administrative control, patching discipline and workload configuration management, and CWPP tooling enables this to be enforced.
- Workloads are no longer remotely homogeneous. Tools must protect containers, virtual machines and serverless workloads, and grant the appropriate levels of visibility and security to each.
- Unlike end-user endpoints, server workloads do not commonly encounter and execute unknown arbitrary code, thus lending themselves to a default deny, zero-trust-based protection strategy that well-engineered CWPPs are built to support.
- As vendor convergence continues to be important to Gartner clients, the convergence of CWPP and cloud security posture management (CSPM) into a cloud-native application platform (CNAPP) consolidates previously siloed offerings, and provides the same or greater value.

Obstacles

- Some CWPP tools in China are modified versions of endpoint protection tools that do not meet cloud workload protection requirements.
- Organizations incorrectly choose endpoint tools, such as EDR/EPP for cloud workload protection, due to the complexity of cloud workload protection technologies and the lack of skilled staff.
- Not all vendors offer all cloud workload protection capabilities. Some specialize in only one or two forms of workload protection.
- Some organizations are maturing their approach to cloud protection and have not identified a need for cloud-native security toolsets, or prefer to continue with existing endpoint tools, despite their lack of suitability for cloud deployments. Such organizations often still wish to extend on-premises controls and control patterns to the cloud, regardless of suitability.

User Recommendations

- Avoid using an end-user endpoint detection and response (EDR) or EPP solution to protect cloud server workloads.
- Select a CWPP tool that supports current and future platforms and different workload types.
- Plan for consistent visibility and control of all workloads, regardless of location or size.
- Extend workload scanning and compliance efforts into development (i.e., DevSecOps), especially for containers and serverless functions. Prefer platforms that support container and serverless environments.
- Require CWPP offerings to expose all functionality via APIs.
- Require CWPP vendors to offer integrated cloud security posture management (CSPM) capabilities to identify risky configurations.

Sample Vendors

Alibaba Cloud; AsiaInfo Security; Chaitin; Hillstone Networks; Huawei; MoreSec; NSFOCUS; QI-ANXIN; SafeDog; Tencent Cloud

Gartner Recommended Reading

Market Guide for Cloud-Native Application Protection Platforms

How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB

Magic Quadrant for Endpoint Protection Platforms

Entering the Plateau

Attack and Defense Teaming

Analysis By: Angela Zhao

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Attack and defense teaming is an exercise in which attack teams ("red teams") are tasked with demonstrating the impact of successful attacks on an organization's systems using all the means available to an attacker. These include phishing, social engineering, physical penetration, stealth and surprise. Complementary to this approach, defense teams ("blue teams") are in charge of detecting and responding to the attacks from red teams.

Why This Is Important

Ensuring uninterrupted business, the attack and defense teaming simulate real cyberattacks as much as possible with organized attack actions. They can test the actual security posture and emergency response capabilities of the organization, and mitigate the gaps for not only technology, but also people and processes. As one type of cybersecurity validation methods, the attack and defense teaming can also guide continuous optimization of security investment.

Business Impact

The attack and defense teaming allows China organizations to:

- Identify exposures in an organization's systems and processes, allowing organizations to implement targeted risk mitigation strategies.
- Test security operations center (SOC)'s ability to detect real attacks, and the collaboration model among all stakeholders in the event of a security incident.
- Foster a security-conscious culture and encourage all employees to be proactive in identifying and reporting potential threats.

Drivers

- The national attack and defense drills have been treated as a compliance mandate for many organizations in China. Forward-thinking organizations want to exceed compliance requirements and continuously validate their security posture.
- Organizations in China are now moving away from the traditional passive and more compliance-driven model to a combat-driven model. Viewing the threat from the attacker's perspective makes organizations more proactive in their ability to spot imminent risks, which ultimately promotes remediation as a top priority.
- The attack and defense teaming is usually tailored to each organization's environment and architecture, so organizations would expect more specific outcomes to improve their security posture.
- Given its longer timetable, results produced by attack and defense teaming are generally more detailed than other types of cybersecurity validations, such as penetration tests, breach and attack simulation (BAS), and provide insights from more perspectives.
- The attack team uses any and all methods during the defined time window for attacking. These include, but are not limited to, penetration, vulnerability exploitation, weak password exploitation, brute force, phishing and social engineering. Organizations in China embrace this approach to not only raise the security awareness of the SOC, but also that of IT teams and business departments.
- More and more tools have emerged to help improve the efficiency by automating some activities. For example, there are tools to automatically collect cyber assets and vulnerability information for the attack team, as well as an audit platform to log both sides' activities and monitor the test execution.

Obstacles

- Comprehensive attack and defense teaming require significant time, expertise and resources, making frequent testing challenging for many organizations in China.
- Some organizations do not make good use of the practice to test their security teams' capabilities, but take simple and extreme remediation actions by shutting down the systems to reduce attack surfaces.
- There are no common ways to measure the effectiveness and outcome of attack and defense teaming exercises, because all test scenarios are customized for each organization.

- A temporary third-party service might be used to augment the organization's SOC workforce for attack and defense teaming, but there are risks, such as data leakage or system interruption.
- Human-led attack and defense teaming is highly dependent on the capabilities of experts from both sides. However, there is currently a shortage of such talent in China's security market, and it is expensive to develop in-house.

User Recommendations

- Embed attack and defense teaming as part of the overall long-term security framework, and prioritize testing based on critical assets and high-risk areas.
- Analyze and learn from the test results to gain the overview of an organization's security posture. From there, define remediation actions accordingly.
- Define clear objectives and success metrics before conducting exercises. Start with smaller-scale testing and remediation actions to demonstrate positive outcomes.
- Conduct proofs of concept and due diligence before engaging a third-party service provider. Consider using an audit platform to manage access rights and log all testing activities.
- Choose a combination of tests, such as penetration test and BAS. Mature organizations with sufficient headcounts and budget can consider investing in training and certification programs for existing staff.

Sample Vendors

360 Digital Security Group; Antiy; DAS Security; H3C; Hillstone; NSFOCUS; QAX; Sangfor Technologies; Topsec; Venustech

Gartner Recommended Reading

Top Practices for Security Operations in China

Using Security Testing to Grow and Evolve Your Security Operations

Appendixes

See the previous Hype Cycle: Hype Cycle for Security in China, 2022.

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (October 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (October 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	Status	Products/Vendors
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (October 2023)

Document Revision History

Hype Cycle for Security in China, 2022 - 10 October 2022

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Top Cybersecurity Trends in China for 2024 and Beyond

Table 1: Priority Matrix for Security in China, 2023

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational		SASE Security Service Edge	Data Risk Assessment Data Security Governance Exposure Management Secure Multiparty Computation Software Composition Analysis	
High	Attack and Defense Teaming	Data Classification IoT Authentication Privacy in China	Breach and Attack Simulation CPS Security in China Data Security Platforms	
Moderate	Cloud Workload Protection Platforms	Situational Awareness Zero Trust Network Access	Attack Surface Management Cloud Security Resource Pool Confidential Computing	
Low				

Source: Gartner (October 2023)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase	Definition

Source: Gartner (October 2023)

Table 3: Benefit Ratings

Benefit Rating	Definition
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (October 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (October 2023)