2024 Planning Guide for Security

Published 4 October 2023 - ID G00796440 - 81 min read

By Analyst(s): Richard Bartley, Patrick Hevesi, Jon Amato, Dennis Xu, Eric Grenier, William Dupre, Nahim Fazal, Anthony Carpino, Greg Harris, Fred Sotolongo, Mike Huskey, Steve Santos, Kevin Schmidt

Initiatives: Security Technology and Infrastructure for Technical Professionals; Meet Daily Cybersecurity Needs; Security Operations for Technical Professionals

The risk landscape remains in flux, with factors such as geopolitical issues and generative AI disrupting business and IT plans. Security and risk management technical professionals must understand the major security trends if they are to execute sound plans for security initiatives in 2024.

Additional Perspectives

- Invest Implications: 2024 Planning Guide for Security
  (11 October 2023)

Overview

Key Findings

- Geopolitical risks arising from supply chain issues, regional tensions and expanding regulation are leading to strategic risks and the need to develop more efficient and effective technical security programs.
- Layered defenses ranging from core capabilities through to highly advanced technologies such as machine learning (ML) help defend against modern threats. However, understaffing and immature practices will hinder any technical advantage.
- Generative artificial intelligence (GenAI) is being used to enhance products ranging from enterprise to security solutions. This is raising concerns about privacy, intellectual property (IP) and data leakage that are challenging security teams.
- Organizations face a security product landscape that is wide and varied, with different levels of integration and interoperability. In this environment, organizations cannot make contextualized enforcement decisions fast enough to meet business needs.
- Ransomware gangs are using increasingly sophisticated techniques, but organizations are not establishing necessary baseline security fundamentals. To provide effective defenses, organizations require a program of foundational security techniques and processes.

Recommendations

Security and risk management technical professionals should:

- Mitigate geopolitical risk by identifying challenges across the organization and increasing internal visibility and governance of its locations and supplier relationships. They should also audit their own organization's cyberresilience plans and do the same for every part of their supply chain. Use of third-party risk management tools and increased monitoring diligence will help identify potential threat behaviors across all supplied services.
- Define a GenAI governance policy to stipulate acceptable usage together with risk management of GenAI in their organization. Provide end-user training and technical controls such as security service edge (SSE) to prevent sensitive data leakage to unauthorized GenAI SaaS applications. Investigate the efficacy and efficiency gains of using GenAI-enhanced security products.

- Plan to implement tools that align with cybersecurity mesh architecture patterns by starting with security intelligence layer capabilities that perform data analysis and risk scoring. Adopt modern security patterns such as zero trust architecture (ZTA), and look for opportunities to consolidate security tools.
- Use security automation and orchestration to perform well-defined, repetitive tasks that may be prone to human error when scripted playbooks are used. This will increase efficiency and effectiveness in the security operations center. Do not automate for the sake of it.
- Implement endpoint and mobile data security controls to provide data security and threat protection. To combat the inevitability of ransomware and other advanced attacks, implement a mix of detective and preventive controls, as well as recovery mechanisms.

Security and Risk Management Trends

Geopolitical challenges have provided the backdrop for security risk globally over the past few years, with physical conflicts and cyberattacks having affected organizations directly and indirectly. Many of these risks emerge as supply chain exposures and need to be addressed with combinations of policy and technical controls. Alongside this, we observe the disruption caused and the potential opportunity created by ML, GenAI and data analytics capabilities. The technical upheaval caused by the introduction of these technologies which are increasingly used by attackers, causes risk exposures. But the same technologies also provide potential for enormous opportunities. ML and AI capabilities are being offered as part of security tools, so organizations need to prepare for their rapid introduction.

IT security risks emerge from sharing information with suppliers, from using shared infrastructure and services, and from acquired software and hardware. There are also supply chain risks to organizations from the tools introduced by IT security — such as secure access service edge (SASE), identity and access management (IAM) and extended detection and response (XDR) tools — all of which create dependencies and can themselves be targets of attackers. Organizations need to build effective security controls to manage all the types of supply chain risk they face.

The key trends begin with strategic concerns that will affect technical security decision making and further influence technical trends.

Strategic concerns influencing security:

- Technical security strategy needs to incorporate drivers and must meet the supply chain risks to IT head-on.
- Risks from broader geopolitical threat groups need to be identified, and existing IT security adjusted or expanded accordingly.
- Privacy and security legislation increasingly requires egress limitations and compliance assertions.
- Emerging governance demands surrounding AI and ML and its consumption of data and synthesis of results.

IT trends that require a security focus include the following:

- New security tools are pivoting toward data analytics and dynamic risk modeling to enhance visibility and avoid past problems with stovepiping and limited ability for security data sharing and integration.
- Data is rapidly being stored and processed “everywhere” as organizations move more and more workloads to various cloud deployments.
- Zero trust is now a key design principle for IT systems as a result of its maturity. There are burgeoning efforts from standards bodies internationally to meet zero trust expectations, as well as some national guidance and U.S. federal regulation.
- Organizations are forced to cultivate more effective communications with IAM teams to help establish identity-first security strategies.
- The evolution to platform engineering impacts how applications are secured in the pipeline.
- API deployments are expanding to make more business functionality accessible.
- Cloud migration of business-critical applications continues to accelerate, with more focus on platform as a service (PaaS) and software as a service (SaaS).
- In direct response to ransomware risks, resilient systems and data are increasingly required as part of enterprise design.

For the purpose of building and adapting a security roadmap, this guide focuses on six trends, as illustrated in Figure 1. This provides a means of grouping controls that support strong threat analysis, tool selection and architectural processes.

Figure 1: Key Trends in Security, 2024

Clients are at many different levels of security maturity. Thus, the planning considerations for 2024 cover a range of security controls within each trend. Within each trend are considerations for controls ranging from basic hygiene and monitoring to highly advanced capabilities. Some of last year's recommendations have evolved to provide a steady foundation for building maturity.

In 2024, continued digital transformation, network modernization, changes to application delivery and increased cloud implementations will increase risk exposure. Security teams will need input from different organizational areas to help build a strong security roadmap.

For 2024, our DevSecOps trend pivots toward platform engineering, increasing the use of self-service developer platforms for software development and delivery.

Our other trends have also evolved from last year, with the inclusion of architectural considerations around cybersecurity mesh, zero trust and security by design, as well as assimilation of the increasing use of ML, AI and especially GenAI capabilities.

This Planning Guide focuses on advising IT security professionals, with a heavy slant toward security architecture. It does not address all aspects of security and risk management (see Note 1 for a list of out-of-scope areas). The subsequent sections expand on the recommendations above as well as the following key security and risk management trends, which will broadly affect organizations, of varying sizes, in many industries and geographies:

- Strategic opportunities and risks ranging from AI to geopolitical changes will drive security technology planning
- Emerging architectural patterns will redefine security
- Platform engineering will become a critical tenet of DevSecOps
- SecOps with automation will enhance capabilities
- Data security will be key to a “data everywhere” world
- Computing hosts will need specialized protection profiles

The relative importance of each of the trends and its related planning considerations will depend on an organization’s current maturity in digital business and IT, as well as its security posture.

Strategic Opportunities and Risks Ranging From AI to Geopolitical Changes Will Drive Security Technology Planning

Security technology programs are driven by internal and external influences on our organizations. Internally, we have budget challenges, technical debt and transformation demands. Externally, we are subject to influences caused by geopolitics, challenges with hardware and software supply chains, and regulatory and legislative impacts. AI and ML are rising to the top of our concerns, and without effective governance and security controls they will have damaging unforeseen impacts on our organizations.

Open warfare, trade disputes, nationalism and their human and economic impacts will continue to add to security challenges. Financial risk exposures causing price fluctuations, the cost of operations and inflation all have the potential to impact a cybersecurity program. This applies both locally (due to recessionary pressures on IT budget) and globally, where it may become impossible to implement security successfully with common tools. Organizations may be the direct target of a cyberattack or become collateral damage in a more widespread attack. Geopolitical cybersecurity risks may appear as supply chain impacts, as partners and trusted third parties may be affected. Cybersecurity attacks may take the form of direct malware attacks, attacks on cloud infrastructure, attacks on system integrity and availability, such as distributed denial of service (DDoS) attacks, ransomware, and data theft or loss.

Supply chain challenges are intrinsically linked to geopolitical risk. They have caused hardware shortages, cost increases, licensing changes and capacity limits. Availability of raw materials — for example, neon gas used in semiconductor manufacturing — has a direct impact on computer manufacturing. Supply chain and logistics failures due to a wide range of geopolitical risks have also contributed to shortages. These disruptions cause organizations to look to unconventional sources, which could bring in counterfeit goods and items whose integrity may have been compromised. Exposures need to be identified and mitigated. Examples of mitigations include protecting shared information with suppliers, enforcing control over shared infrastructure with suppliers, and ensuring the integrity of supplied IT hardware, software and firmware.

There are changes in regulatory environments globally, which usually arise from national or industry-specific compliance mandates to protect sensitive data. While regulation seeks to reduce risks, uncertainty remains about how to effectively comply with regulatory mandates that are nonspecific about which controls to use, how to implement them in distributed environments like cloud or what the consequences of failure to comply will be. A sustainable security program that provides data-driven risk decision making and measurable treatments as an outcome is essential to manage the new normal. Up-to-date risk assessments and risk communication practices are the driving forces for improving the current state. Technical professionals must be prepared to realign standards and processes with recent changes that affect the attack surface, such as by enabling remote work environments and moving workloads to the cloud.

The hype and potential of GenAI technologies is having a substantial impact on strategic business planning as organizations scramble to understand and identify how it can benefit them. Leaders want to leverage and enhance their business, but have not really accounted for the risks posed by these technologies. Good security governance is needed to initially limit and temper expectations and user ability to share corporate data. Business tools need to be investigated, secured and then used to build competitive advantage. Threat actors are attacking GenAI solutions (for example, by prompt injection), as well as adapting and developing attacks that use these technologies offensively. Security technology companies are seeking to enhance their tools with ML.

But time and resource pressures continue to motivate some organizations to follow the easier route of maintaining compliance checklists, rather than implementing effective risk analysis and control selection. Visibility into supply chains is challenging and needs work to become effective, but the agility needed to handle emerging security threats from unpredictable geopolitical events is demanding for all security teams. Reacting fast and implementing AI security governance to protect your organization in the near term is a priority.

Planning Considerations

Adapt Security to Be Responsive to Current and Emerging Geopolitical Risks

Organizations, even if not directly targeted, can be impacted by a host of geopolitical risks. For example, organizations using offshore sourcing models for application development or incident response services must factor in risks to the wider supply chain. Increased geopolitical tension will result in a continuously changing threat landscape, with targeted and disruptive attacks becoming more likely. Organizations must not only prepare and audit their own cyberresilience plans, but also do the same for every part of their supply chain. It is important to note that many geopolitical risks impact organizations via their physical and software supply chains.

Geopolitical risk creates a set of challenges ranging from social impacts caused by war, pandemics, nationalism, trade disputes and political posturing, to technology impacts including digital ethics and privacy concerns. Environmental impacts — from extreme weather to sustainability issues and the social impacts of climate change — may also become sources of emerging cybersecurity risk to organizations and their staff.

Significant cybersecurity challenges from geopolitical risks include the following:

- Isolated and focused operations in specific geographies can lead to availability risks.

- Manual processes create risk around business agility. Organizations may not be responsive enough in the face of significant change.
- Supply chain threats (both physical and software) have increased substantially over recent years and are proving to be sources of cybersecurity risk.
- Existing incident response mechanisms may not be sufficient or robust enough to handle the diversity of geopolitical risk events.
- Data fragmentation and increased nationalistic tendencies have led to onerous legal, regulatory and bureaucratic challenges.
- The complexity of geopolitical risk means that organizations might not be even tracking the real threats.
- Lack of visibility into diverse and global services and systems means there are potential blind spots for exploitation.
- Current resilience plans, if they exist at all, may not sufficiently address identified geopolitical challenges.

Figure 2 illustrates mitigations to address these geopolitical risk challenges.

Figure 2: Mitigating Geopolitical Risks

Supply chain cybersecurity risks need to be addressed as sociotechnical challenges. Bear in mind that not all approaches to address them will be technical in nature, although they present a technical risk. They are not solely IT security risks, but emerge from challenges such as hardware and software sourcing, business continuity and transportation problems. Supply chain risks emerge from the complex organizational matrix of relationships needed for business. Technical controls that can help track these risks include third-party risk management (TPRM) tools as well as enterprise tools to manage governance risk and compliance.

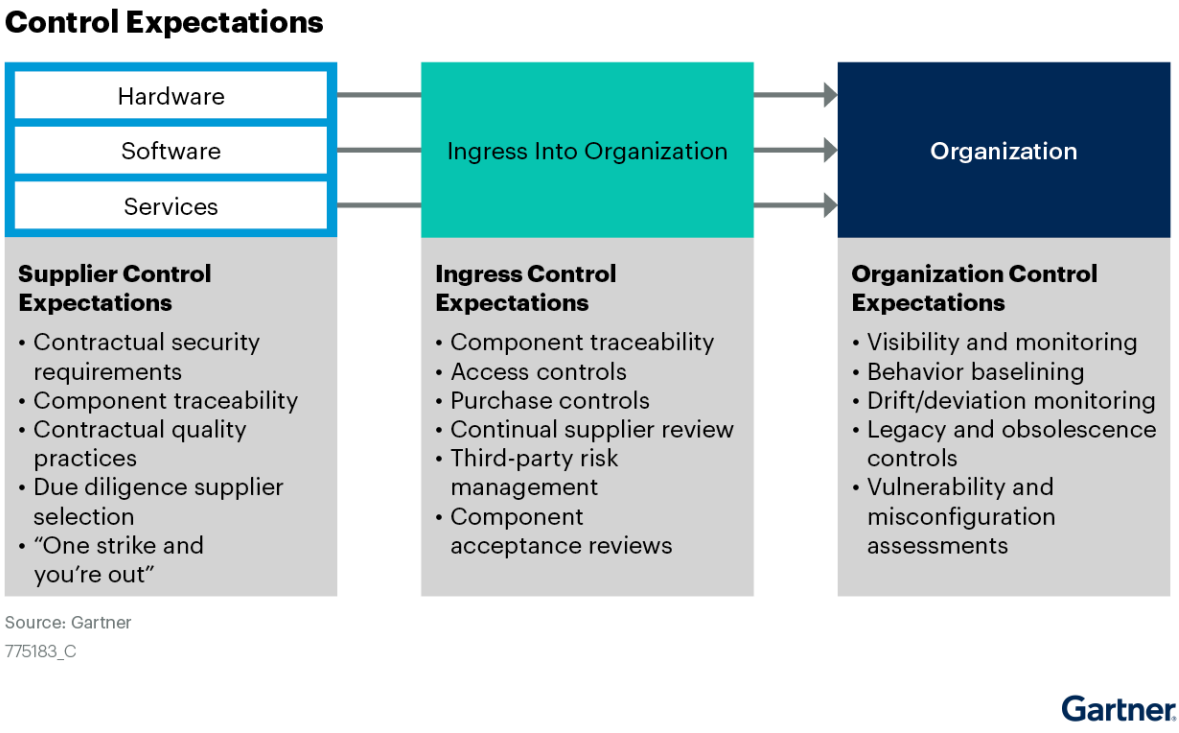
The tools introduced by IT security represent another area of supply chain risk. Reliance on such tools, including SASE, IAM, SSE and XDR, creates its own supply chain dependencies and risks by acting as a possible force multiplier for attackers who compromise these tools' vendors. TPRM programs become imperative to manage these dependencies.

Security and risk management technical professionals need to be aware of the different types of risks that can impact organizations, including the following from the U.S. National Institute of Standards and Technology's (NIST's) Best Practices in Cyber Supply Chain Risk Management:

- Third-party services providing everything from environment and office control through to outsourced software development.
- Cybersecurity risks caused by security control gaps down the supply chain.
- Malicious and infected software and libraries.
- Counterfeit goods.
- Supplier data storage and aggregation.

Supply chain risks must be addressed with compensating layers of defense, on the assumption that a breach is inevitable. Layers will likely include changes in processes, as well as physical and IT security. Figure 3 shows control expectations, from setting up business relationships with suppliers, to controls that need to be put in place as services are received and used within the organization.

Figure 3: Control Expectations



Related research:

- Building the Foundations for Basic Security Hygiene
- Emerging Best Practices to Manage Digital Supply Chain Risks
- What should I know about Supply Chain Risk Management?
- How to Address Geopolitical Risks in Software and Cloud Contracts

Identify How New Privacy and Security Legislation Will Affect Your Technology Security Program

IT system implementation and security controls are subject to external influences such as regulations, privacy concerns and other legislative demands. There has been a flurry of cybersecurity assertions and regulations as a result of recent incidents.

These sociotechnical influences affect both the design of IT systems themselves and the selection and inclusion of particular security tools. While many areas of technology are impacted, particular areas of concern include:

- **Data:** Concern focuses on storage location, confidentiality, integrity and access to data.
- **Processes:** Concern focuses on why processes should occur, where they are performed, their integrity, and who has access to them.
- **Communications:** Concern focuses on how communications are carried out, why, where, and who has access to them.

Each of these areas attracts external control expectations under various circumstances. Key examples that Gartner clients face regularly include:

- **Sovereignty expectations:** National privacy and sometimes national security rules prevent data from leaving a particular country or geographic zone. This is primarily a cloud security challenge, but organizations with large global infrastructures also need to be cognizant of sharing, access and replication causing breaches to sovereign data rules. Security controls need to be implemented across the stack to assure sovereignty, from selections made regarding regions in a cloud through to data loss prevention controls.
- **Breach notification:** Where there are strict obligations to issue notifications of breaches in a timely manner, certain capabilities and arrangements need to be in place. These include contractual obligations with suppliers to notify their breaches of your data, as well as data and infrastructure security systems that detect unauthorized behaviors, including exfiltration.
- **Privacy by design:** This is becoming a common feature either directly referenced or strongly implied by privacy legislation. The aim is to prevent data controls from being an afterthought, but rather planned explicitly into the original design of a solution. This may require changes to security architecture processes, so that security controls supporting privacy can be contemplated in the design phase instead of being emergency add-ons later.
- **Identity-first security:** This approach to security design makes identity-based controls a foundational element of an organization's protection architecture. It represents a fundamental shift away from perimeter-based controls, which became obsolete due to the decentralization of assets, humans and machines. Identity-first security requires tighter collaboration of IAM and cybersecurity teams to ensure alignment, and placement of IAM at the heart of security strategy. It also requires better alignment of IAM with other business and IT functions because secure digital access is key to enabling almost every business function.

- **Encryption regulations:** FIPS 140-2 validation is a U.S. standard that is adopted widely (beyond the U.S. Government) as a benchmark for encryption algorithm implementation. However, FIPS 140-2 will expire in three years. It will be replaced by FIPS 140-3, which will require additional checks as a result of its incorporation of two standards (ISO/IEC 19790:2012 — Security Requirements for Cryptographic Modules and ISO 24759:2017 — Test Requirements for Cryptographic Module). This inclusion means that evaluation is performed at all stages of crypto-module creation, from design and implementation to deployment. Both vendors and buyers need to keep ahead of these changes to ensure expectations are met.
- **5G implementation:** This is made challenging by a wide range of issues, such as vendors being subject to import restrictions, regulatory controls on spectrum allocation and privacy issues. As 5G is introduced, regulatory demands must be met and deployments protected from attack.
- **Governments' internal regulations:** Around the world, governments are issuing compliance control requirements for cybersecurity. Generally, these standards are for clients who work in government departments and agencies, but they also place obligations on suppliers. These requirements include:
  - Architectural principles such as zero trust, security by design and application security
  - Cyberincident response
  - Cybersecurity resilience
  - Cloud security use
  - Cybercrime prevention

Related research:

- Emerging Legal, Compliance and Privacy Risks (2Q23)
- Build for Privacy

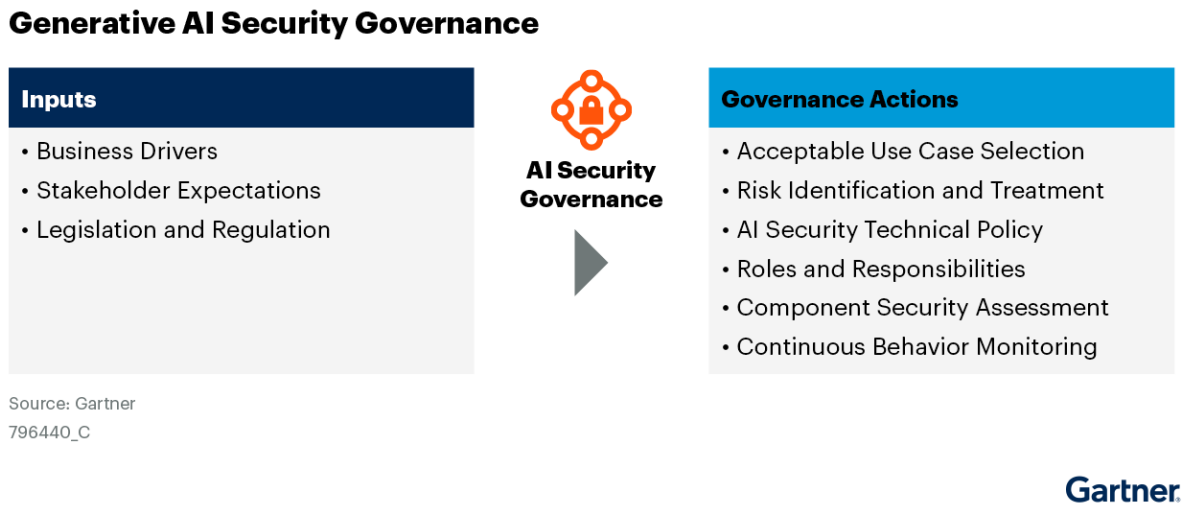
Define AI Tool Governance That Includes Security, Ethical and Human Impact Concerns

New forms of ML such as GenAI are becoming increasingly popular. Their use must be carefully governed by organizations to prevent emergent risks and abuse. Governance must focus on organizational security as well as ethical and human impacts that could cause organizational risks, such as reputation risks and insider threats.

AI security governance needs to account for a number of drivers (see Figure 4), including aligning governance with business needs (e.g., governance that strictly forbids the use of AI that is contrary to potential organizational benefit will be at best rejected, at worst ignored). Identify key stakeholders across the organization who have accountability or responsibility for both the introduction and control of ML/AI technologies. Work with them to identify suitable governance expectations that span:

- Acceptable use cases
- Risk identification and treatment
- AI security technical policy
- Roles and responsibilities
- Component security assessments
- Continuous behavior monitoring

Figure 4: Generative AI Security Governance



AI security governance policy must align with external regulatory, legislative rules and with ethical best practices in relation to, for example:

- **Unreliable outputs:** Practical controls are needed to identify wrong information, including the hallucinations of AI. These controls can include the use of multiple models, different training and different foundational models to provide different views. Organizational AI governance must attribute a level of trust to outputs. They must be annotated to show with full transparency that they derive from AI, so that decision makers can understand the potential risks of using AI-generated data.

- **Data privacy and confidentiality:** Governance controls must place limitations and controls on which data is shared with GenAI tools (for example, using SSE tools to control data passed to GenAI SaaS). More importantly, access to private or confidential data, and subsequent derived data stored by AI, must also be carefully managed. This includes decision making around limitations of use of public GenAI services which, if sensitive data is shared, would constitute a breach. Finally, users with access to AI-generated data that is likely to contain private or confidential data must also be strictly limited to prevent unfettered access. Care must be taken in specific areas, such as AI capabilities, to deanonymize data or make inferences that themselves could breach privacy or confidentiality conditions.

- **Model and output bias:** AI governance policy must define the conditions under which model or output bias may impact security.

- **IP:** Security governance around IP will include input limitations regarding the sensitivity of organizationally owned IP and whether sharing should be permitted with particular AI tools. Also, the AI governance policy must govern the introduction of third-party IP that may breach the company's ethics rules and legislation.

- **Cybersecurity:** Expectations for cybersecurity must be set out as part of AI governance definitions. These should include the security requirements for the use of organization data with any AI tool, including protective controls for data and processing and detective controls for abuses and attacks.

- **Consumer protection:** Consumers and customers put their trust in organizations. Failing to disclose the use of AI tools, or obfuscating how results from AI tools are relied on can reduce that trust significantly. The alternative — being transparent and presenting how the organization should use AI responsibly as part of a governance policy. Incorporating this offers an enabling feature for businesses.

- **Third-party use:** Downstream use of organizational data and digital data supply chains could pose risks, including data exploitation. Unanticipated use by third parties (such as of shared data where agreements do not expressly control the use of that data) could result in unanticipated risks to an organization.

- **Liability:** Liability for the use of AI tools is untested territory. By having effective governance policy and processes in place, the risk of liability can be reduced. Security governance for AI should ensure that AI use is transparent and controlled, that security tools focus on the security of data, that risks are continually monitored and that there is human oversight.
- **Regulatory compliance:** Legislation is globally fragmented, which makes this challenging. Governance functions must include legal input, so that necessary security controls can be put in place both centrally and geographically to support compliance.

Related Research:

- Emerging Legal, Compliance and Privacy Risks (2Q23)
- Prepare for AI Regulation by Addressing 4 Critical Areas

Emerging Architectural Patterns Will Redefine Security

Understanding how to overlay security controls onto enterprise IT, whether on-premises or in the cloud, is increasingly challenging. It is becoming more difficult to know what security features products have and what their applicability is to particular environments and services. Some products are niche "widgets" that offer singular capabilities or coverage. Some are broader "security platforms." And some are natively built into other solutions. Security teams must be able to identify gaps resulting from new IT strategies (such as moving to the cloud or increasing the use of container technologies), overlaps that lead to increased amounts of shelfware, and poor controls with default settings, as well as capability conflicts. They must identify and monitor emerging threats, so that risks can be prioritized and addressed in roadmaps.

In all cases, the difficulty is figuring out where and how security features can be pieced together to provide the right capabilities in the right places. It is like playing the Tetris puzzle game: The "shape" of product features inevitably leads to gaps and overlaps, and these need to be identified early so that they can be properly addressed. It is also important to review vendors' product roadmaps, because security markets are always consolidating but never consolidated. ZTA principles have been developed that help security architects identify and implement a modern set of compensating controls that can protect dynamic environments with continually changing threats and risks.

Large security vendors are building unified cybersecurity platforms, defined by their underlying data-lake-oriented capabilities, as cybersecurity mesh architectures (CSMAs). These solutions aim to implement a single console; provide integrated ML, orchestration and automation; and support third-party integration. These platforms are built over time, expanding with new types of capabilities and integrations as client needs arise. CSMAs will help organizations simplify the complexity of managing multiple point products. In addition, the new architecture will lay the foundation for cybersecurity to become predictive of upcoming attacks, based on the intelligence in the central data lake/repository.

As security vendors start to realize the benefits of CSMAs, organizations will be able not only to leverage the vendors' point products but also integrate third-party point solutions as "first-class citizens."

SASE is an adjacent architectural approach that aims to converge networking and security capabilities to:

- Increase the use of cloud-based security services and push security out to the service edge itself.
- Permit vendors to add nonsecurity functionality, such as software-defined WAN (SD-WAN) and network optimization.
- Reduce the number of policy administration points across the converged solution.

SASE is also driving the coalescence of previously separate capabilities. For example, some vendors started with a stand-alone secure web gateway (SWG) and enterprise data loss prevention (DLP). They then acquired a cloud access security broker (CASB), zero trust network access (ZTNA) and remote browser isolation (RBI), and integrated them into a single platform now defined as SSE. SSE components are now the most popular elements of SASE being implemented. Many nonsecurity software and service providers, such as hyperscale cloud providers, offer a growing set of native security controls, such as for encryption or monitoring.

Security architecture is implicit in various control frameworks and “top” lists, such as the ISO/IEC 27000 series and Center for Internet Security (CIS) controls. However, these control lists and frameworks do not provide security teams with enough structure for detailed roadmap planning, partly because they do not always reflect the evolution in business, IT or security controls. These methodologies map to enterprise security architecture frameworks, but not all organizations use them or have an enterprise architecture function. Organizations that already use one of the architecture or control frameworks may need to supplement it with additional security architecture models and processes in order to close gaps and align with business needs.

Planning Considerations

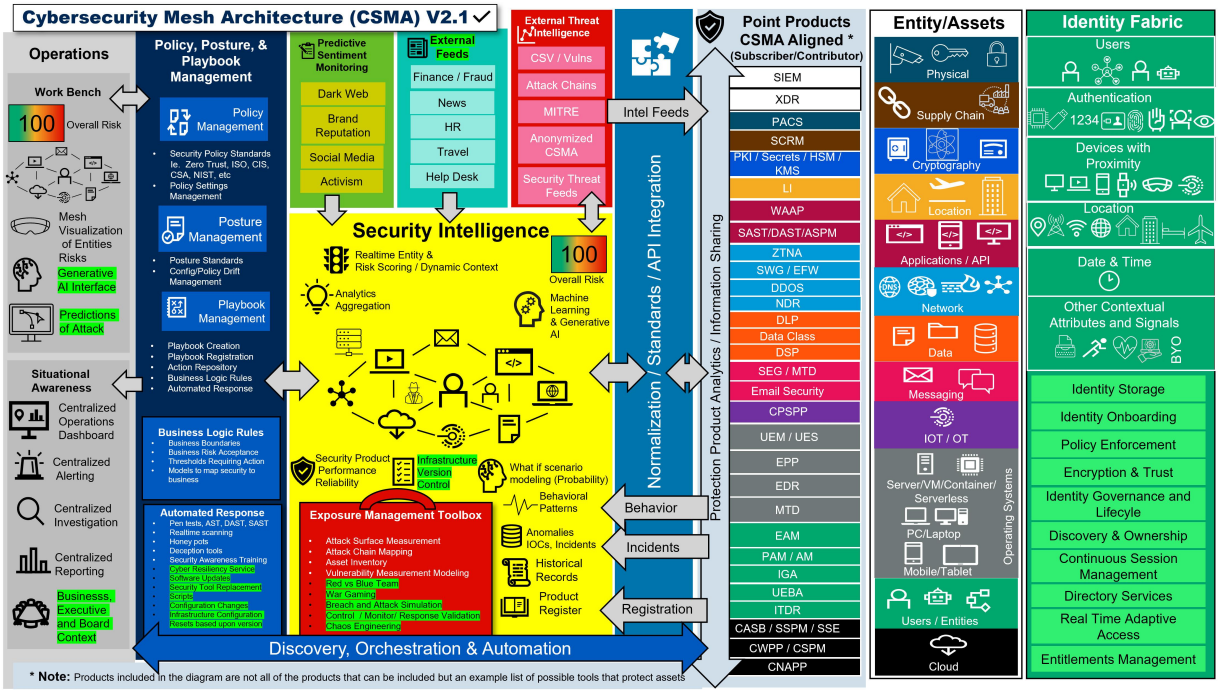
Implement CSMA Principles, Starting With Data Analytics and Risk Modeling

The perimeter is gone. Digital assets — and individuals — are increasingly located outside enterprises, which forces organizations to rethink their approach to security controls. Traditional security controls are hard to adapt to this new reality, so a new architectural model for security is needed.

Enter the CSMA, which represents a composable and scalable approach to extend security controls to distributed assets (see Figure 5). Security controls can be added to various widely distributed assets, wherever they may be. The aim is to transition to a core of security intelligence capabilities based on advanced data analytics/ML for predictive attack defense.

Download a presentation slide of this material

Figure 5: Cybersecurity Mesh Architecture (CSMA) Reference



CSMA is not an individual product but a modern security approach that consists of deploying controls where they are most needed, in a manner that is composable, scalable, flexible and resilient. Rather than every security tool running in a silo, a cybersecurity mesh enables tools to interoperate by providing foundational security services — such as a distributed identity fabric, security analytics, intelligence, automation and triggers — and centralized policy management and orchestration. New open cybersecurity standards like the Open Cybersecurity Schema Framework (OCSF) and Open XDR were announced in 2022, and OCSF moved into general availability in August 2023. These will help security vendors align interoperability and communication between point products and the security intelligence layer. Security architects need to start factoring in CSMA principles now, so that they can take advantage of the benefits later. As you evaluate your existing security products, look for advanced behavioral risk scoring, AI/ML, automation and alignment with the new standards.

CSMA provides a modern architectural construct that helps vendors with convergence of their tools into more comprehensive and effective security capabilities. Some vendors are aiming to present their own interpretations of CSMA. Others are using the construct as a microcosm around intelligent analytics, decision making and orchestration, which will further increase the synergy between point tools to create much better real-time insights and risk mitigation. For example, some SSE component convergence approaches have used open APIs and partnerships and are pivoting toward using a common data lake with a normalization schema (such as OCSF). Also, cloud-native application protection platforms (CNAPPs) are formed from the convergence of cloud security posture management (CSPM) and cloud workload protection platform (CWPP) capabilities, as well as other security tools like entitlement management, API controls and Kubernetes posture control. Some CNAPP vendors use integration approaches with centralized data analytics, log and event normalization, and open APIs.

Related research:

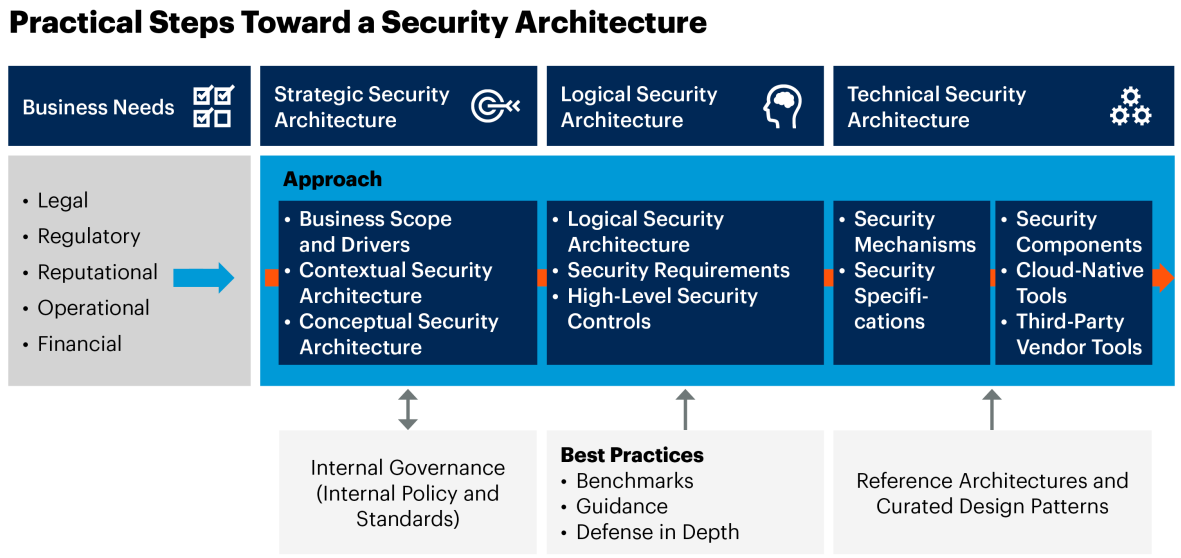
- The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)
- Identity-First Security Maximizes Cybersecurity Effectiveness

Use “Security by Design” Principles

The idea of “security by design” (or “security by default”) emerged as a set of guiding principles by which security can be seen as a key design aim, rather than a bolted-on afterthought. [1] Importantly, these principles define approaches to implementing security. The principles are diverse, ranging from the need to establish secure defaults and taking a “least privilege” approach, through to enforcement of proactive (not reactive) controls and preventative (rather than restorative) capabilities. They can be used to provide the basis of, or a context for, the envisaged security architecture. Solutions, implementations and applications based on this kind of approach are often referred to as “secure by design” in reflection of their early consideration of security in the design life cycle.

Figure 6 shows practical steps on the path toward a security architecture. For more details, see Use Security Architecture to Enable “Security by Design.”

Figure 6: Practical Steps Toward a Security Architecture



Source: Gartner
778425_C

Gartner

Architecture is based on design principles. Design principles are the "guiding forces" that help us reach a solution to a particular technical problem. In the field of security, we can think of architectural principles as helping us achieve security by design. Organizations widely publish their ideas for security-by-design principles. Examples come from the Open Worldwide Application Security Project (OWASP) — with its focused on secure-by-design application principles — and guidance put out by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), with support from governments around the world. We also find them among guidance from cloud providers, such as Amazon Web Services (AWS) with the Security pillar of its well-architected framework, and Microsoft with its security design principles. Typical popular secure-by-design principles include:

- Practice identity-first security — focus on user and identity, and enforce least privilege
- Practice defense in depth
- Enforce security by design
- Minimize attack opportunity
- Implement zero trust
- Design into, not onto

- Secure after failure
- Ensure separation of duties
- Design for simplicity
- Enforce least functionality

Related research:

- Use Security Architecture to Enable "Security by Design"

Make Zero Trust Principles Key to Your Security Architecture

Zero trust has become a fundamental architectural tenet. Expectations regarding zero trust have shifted, with government agencies and standards bodies defining principles, guidance and best practices to follow. The inclusion of zero trust principles should be carefully balanced against perceived risks to ensure that new security capabilities are introduced in terms of priority order in roadmaps. Use architectural processes and carry out a gap analysis to help with this prioritization.

Gartner defines ZTA as "an architecture that replaces implicit trust with continuously assessed risk and trust levels based on identity and context that adapts to risk-optimize the security posture." This means that trust must be explicit, with any request to access a ZTA requiring a risk calculation. The risk calculation takes into consideration various signals, such as device location, believability of user assertion, device hygiene, threat intelligence, time of day, day of week, and the data sensitivity of the application being requested. Access is granted only when the calculated risk is less than the value of extending the access.

Organizations should implement ZTA principles to:

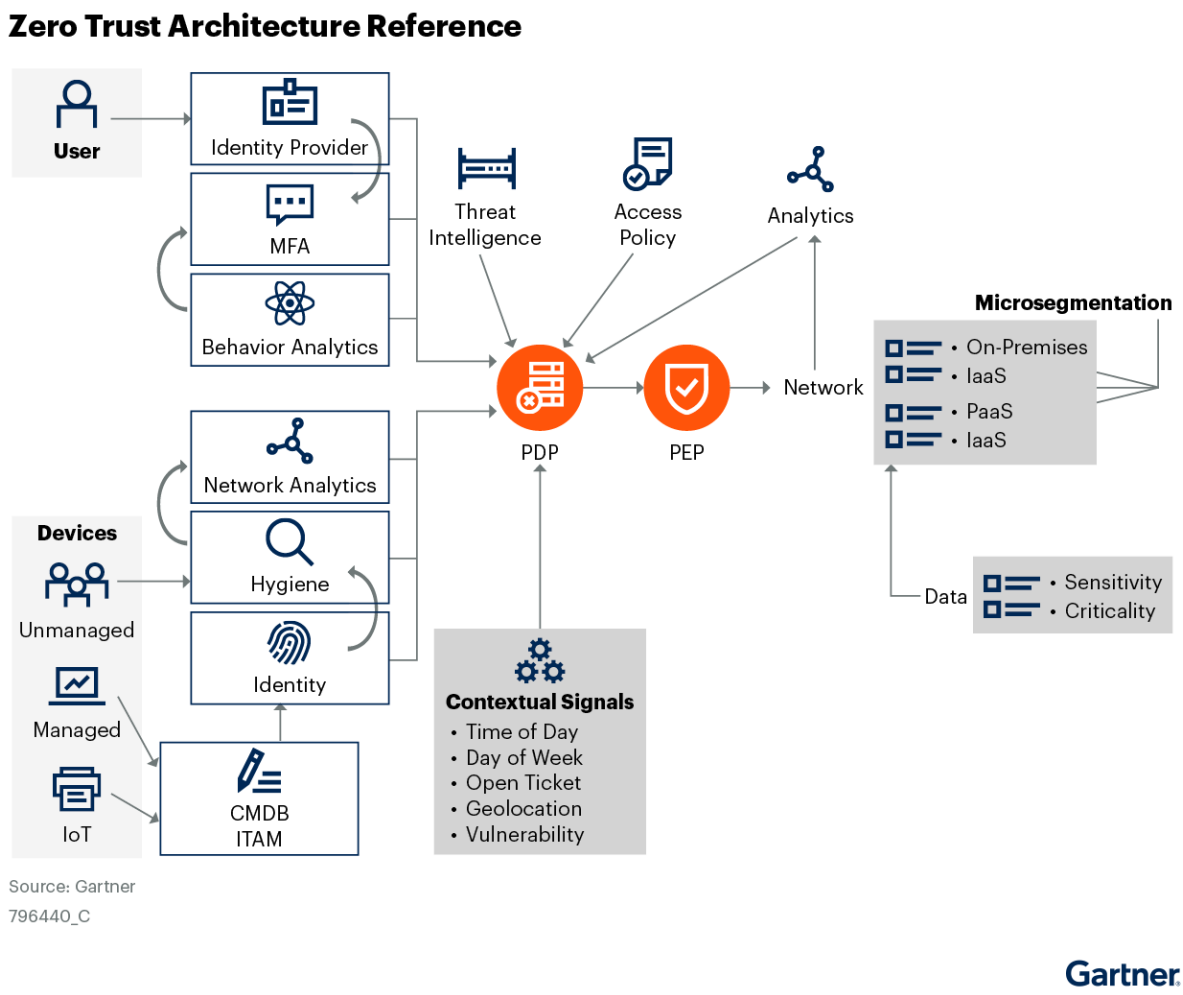
- Replace implicit trust with continuously assessed explicit trust, based on identity and context, supported by security infrastructure that adapts to risk-optimize the organization's security posture.
- Securely connect entities to resources. We securely connect users to applications, services and data, while allowing nonusers to connect only to authorized resources.
- Detect access abuses by using user and network analytics and other forms of monitoring.

- Enforce a consistent and dynamic approach to protect resources using granular access decisions based on context.
- Visualize which users are accessing which applications — assisting with the principle of least privilege via just-in-time and just-enough access.
- Drive consistent security posture and consistent access policies regardless of user, device or location throughout the organization, while minimizing user friction by matching authentication with risk.
- Limit lateral movement of threat actors or malware in an organization by pushing access decisions as close to the requested resource as possible.
- Enhance system confidentiality by enforcing encryption for all data in motion.

Figure 7 shows the primary elements to be assessed and potentially included in your ZTA. To be successful with ZTA, start with the following steps:

- Define the strategy and ZTA principles with which your organization wants to align.
- Identify the risks you are trying to address with zero trust, such as minimizing lateral movement or controlling the spread of ransomware.
- Identify the scope of zero trust and the target for initial implementation, including any gaps and redundancies in technologies.
- Secure the budget required to update, implement or refresh technologies for the ZTA.

Figure 7: Zero Trust Architecture Reference



Related research:

- How to Build a Zero Trust Architecture
- Improve IAM Architecture by Embracing 10 Identity Fabric Principles
- Advance and Improve Your Mobile Security Strategy
- Remote Access Options for Enterprise Endpoints
- Overcoming the Challenges of Implementing Zero Trust Network Access
- 7 Effective Steps for Implementing Zero Trust Network Access

Monitor Malicious Usage, Evaluate Defensive Capabilities and Secure Your Organization's Use of GenAI

Cybercriminals are actively exploiting the power of GenAI to improve the efficiency and efficacy of attacks and create malicious tools. They have created tools like WormGPT and FraudGPT to assist the creation of phishing emails and the development of malicious software, among other tasks. However, they can also use legitimate tools like PassGPT and PentestGPT (both developed to improve security practices) for malicious purposes. Security teams will have to be prepared to defend against increased and more focused attacks as these tools improve the productivity and creativity of cybercriminals.

Potential risks from malicious use of GenAI include:

- Misinformation and disinformation
- More scalable and effective phishing
- Inclusion of malicious code in an organization's products, leading to compromises
- Poisoned datasets
- Consumption of unknowingly biased content
- Theft of IP
- Impersonation (using deepfakes, for example) and identity deception

Security vendors are leveraging large language models (LLMs) for language translation capabilities to build natural-language-based interfaces to interact with their products or to generate software code. A few vendors have ventured into using LLMs to assist threat detection. As we are at the peak of the GenAI hype, organizations should be critical and distinguish marketing messages from tangible technical capabilities. Certain vendors have created security-specific models — fine-tuned from base models — with security-focused datasets, such as those that come from threat intelligence sources. Security-specific models are the current frontier when it comes to using GenAI in a threat detection capacity. Given the potential for high inference costs (both computational and financial), these products might come with a high price tag. Refer to the SecOps section for details of defensive usage of GenAI in a security operations center (SOC).

Ensure secure consumption of GenAI applications delivered as SaaS, such as ChatGPT and Microsoft 365 Copilot, using a SaaS-security-centric viewpoint with additional GenAI risk considerations. GenAI SaaS applications commonly retain a copy of user prompts and GenAI responses for troubleshooting and content safety review purposes. Organizations should evaluate how SaaS providers are securing this copy and whether there is an option to opt out. Retrieval augmented generation (RAG) is a popular approach used for GenAI SaaS applications to retrieve business-specific data to provide a more business-aligned response. Proper business data access authorization is critical to ensure that, with the usage of GenAI SaaS apps, users do not get access to data that they are not authorized to access via the RAG process.

Many organizations are looking to build their own GenAI-enhanced applications using foundational models hosted by commercial cloud providers (for example, Microsoft [Azure OpenAI], OpenAI itself, Google, AI21 Labs, Anthropic and IBM [watsonx hosted GPT models]). Some of these providers may offer better enterprise-grade security controls for organizational and customer data, compared with public GPT models. When using such services, organizations should treat them as they would any other cloud solution when it comes to security, by adhering to the shared responsibility principle, with additional GenAI security design considerations. With the recent release of powerful open-source models such as Llama 2 and Falcon that permit commercial usage, organizations have more options to build GenAI apps that could be securely hosted in the cloud or on-premises.

Related Research

- Quick Answer: How to Use ChatGPT and Generative AI Securely With Minimal Data Loss

DevSecOps Will Become a Key Tenet of Platform Engineering

DevSecOps has reached the Plateau of Productivity on Gartner's Hype Cycle for Application Security, 2023. This is due to security teams' efforts to become more integrated into development processes by automating application security testing solutions, including static and dynamic testing, and establishing security posture management capabilities to protect software supply chains and cloud deployments. While this shift is critical to secure application development, security teams must keep up with the new organizational focus on platform engineering.

Platform engineering is the discipline of building and operating self-service developer platforms for software development and delivery. A platform is a layer of tools, automations and information maintained as products by a dedicated platform team, designed to support software developers or other engineers by abstracting underlying complexity. The goal of platform engineering is to optimize the developer experience and accelerate delivery of customer value. Security teams should look to work or integrate with platform teams to put guardrails around security and compliance.

Diverse application runtime environments continue to pose significant security challenges. Organizations must secure the growing adoption of API, mobile, PaaS, container and microservice deployments. Controls such as API threat protection, CWPPs, container security and CNAPPs must be considered in order to support modern deployment environments. Their automation and orchestration have a strong potential to increase security by enabling standardization and deeper layered defenses.

Planning Considerations

Support Transition to Platform Engineering With Application Security Automation

The goal of platform engineering is to lay out “paved roads” or “golden paths” that support development team efficiency and effectiveness. A road has both guidelines (recommended ways of traveling) and guardrails (hard boundaries the user cannot cross). Platforms should establish guardrails around security and compliance, such as “You must run these automated tests of your security posture before deploying.” They could also suggest particular guidelines, such as “We recommend the following tool for these use cases.”

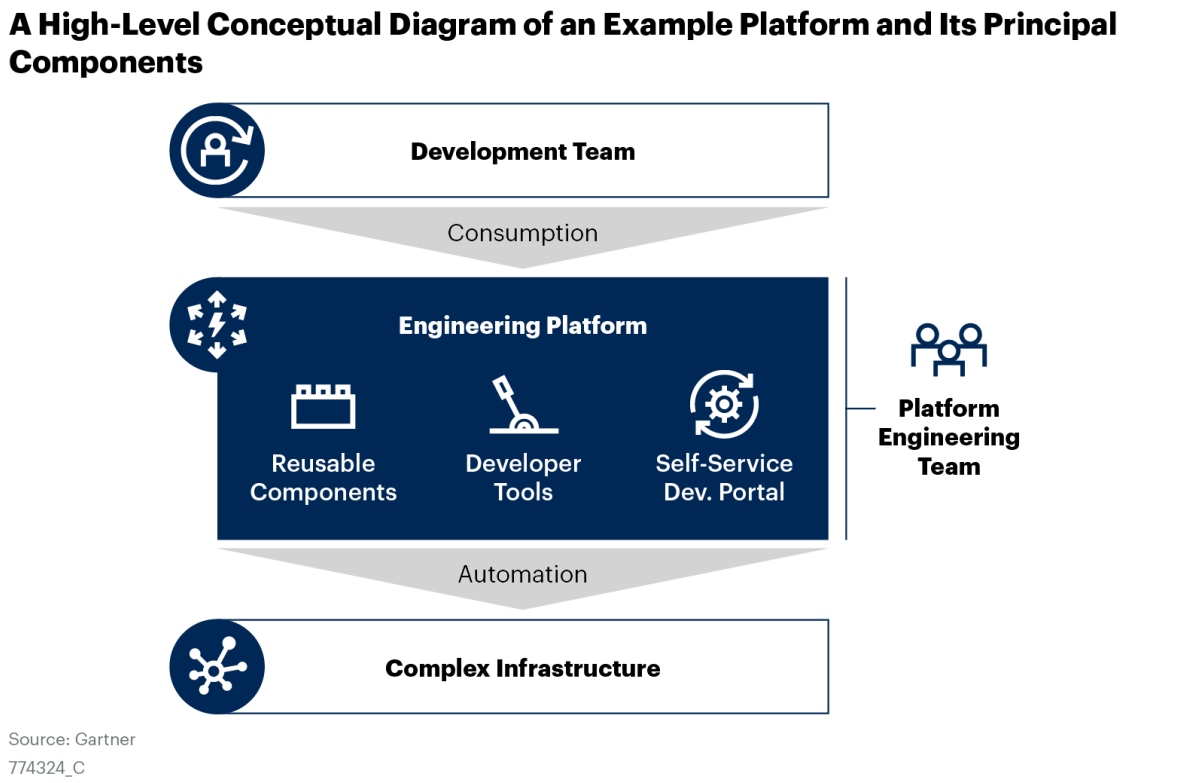
As organizations move to platform engineering, security and risk management technical professionals must align with this transition. They can do this by embedding security into platforms, just as they did with DevSecOps programs. Security teams should work with platform teams to embed security into user workflows as early as possible. However, platform engineers may have the responsibility to incorporate comprehensive, automated security and compliance checks as part of test suites. In such cases, security teams need to be partners in the growth and maturity of platform engineering.

Figure 8 provides a high-level illustration of a platform and its principal components. Security teams should look to integrate tools and processes into these principal components. Examples of such integrations could include:

- **Reusable components,** such as compliant infrastructure-as-code (IaC) and policy-as-code (PaC) artifacts that enable secure cloud resource provisioning.

- **Developer tools,** such as application security testing solutions (for example, static application security testing solutions and software composition analysis [SCA] tools) and compliance-driven component repositories and registries.
- **Self-service portals,** to provide visibility into application security issues or the complete posture of an application.

Figure 8: A High-Level Conceptual Diagram of an Example Platform and Its Principal Components



Related research:

- A Guidance Framework for Establishing and Maturing an Application Security Program
- Using 'Policy as Code' to Secure Application Deployments and Enforce Compliance
- Managing Machine Identities, Secrets, Keys and Certificates
- Guide to Application Security Concepts

- Adopt Platform Engineering to Improve the Developer Experience

Enforce Security and Transparency Across Software Delivery Infrastructure

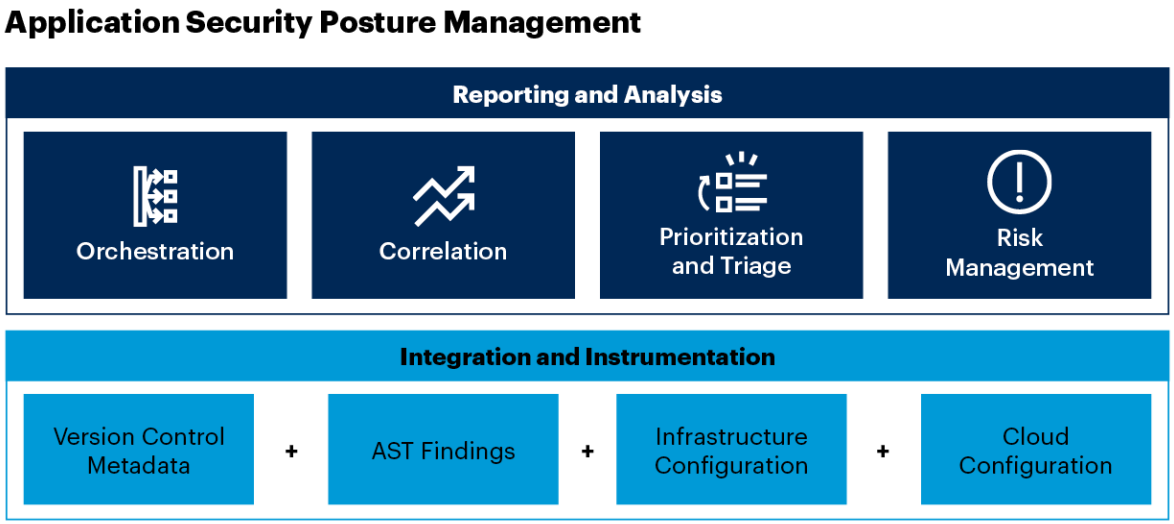
As important as it is to protect the development artifacts going through the delivery pipeline, it is just as important to protect the pipeline itself. Software supply chain attacks continue to be a problem, with malicious actors exploiting weaknesses at every stage of the software procurement, development and delivery life cycle. These exploits include everything from injecting malicious code into application artifacts to installing back doors in third-party software.

Organizations must secure their software delivery pipelines, including components such as code and artifact repositories, continuous integration servers, IaC artifacts and sensitive data (for example, application keys and passwords). Techniques for such security include server hardening, artifact signing, and the use of strong IAM policies. Also, SCA scanning should be used to identify vulnerable components that may have been injected into application artifacts.

Transparency is another critical aspect of the software supply chain. Knowing what constitutes an application is important for understanding where vulnerabilities may impact organizational risk. Software bills of material (SBOMs) are formally structured, machine-readable metadata that uniquely identify a software package and the components used to build it — whether open-source or proprietary. Organizations must incorporate SBOM creation into their development process to better understand application risk.

Application security posture management (ASPM) tools continuously manage application risk through collection, analysis and prioritization of security issues from across the software life cycle. This helps security and software engineering teams by integrating and orchestrating application security tools and controls, improving visibility and giving structure to the process. Implement ASPM to gain a better understanding of your applications and systems. This is especially useful for organizations with disparate development teams, and a variety of software development and security tools (see Figure 9).

Figure 9: Application Security Posture Management



Gartner

Related research:

- How Software Engineering Leaders Can Mitigate Software Supply Chain Security Risks
- Guide to Application Security Concepts
- A Guidance Framework for Establishing and Maturing an Application Security Program
- Using 'Policy as Code' to Secure Application Deployments and Enforce Compliance

Continuously Monitor and Enforce Security on Application Workloads

CWPPs, specifically those focused on protecting containerized workloads and Kubernetes, are essential for securing an organization's production containers. Container-focused CWPPs provide a range of security auditing, monitoring and protection capabilities to secure workloads at build time, delivery time and runtime.

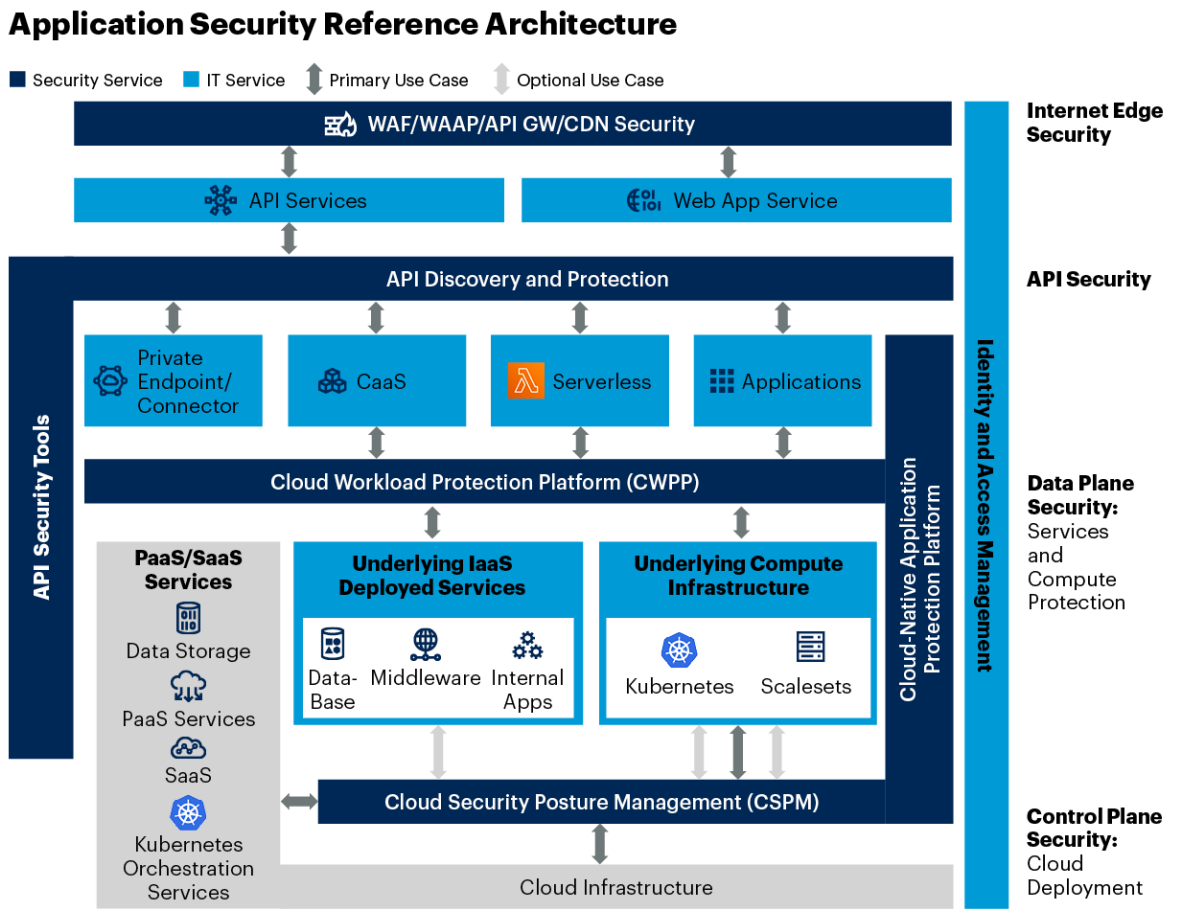
Using a CWPP, scan container images to identify known vulnerabilities when images are pushed to, or stored in, container registries. Also scan deployed containers or running workloads to identify vulnerabilities that are newly reported or that are the result of environment drift.

For workload and data security, apply built-in or add-on encryption for storage and databases as a baseline compliance control, and combine it with CWPP, CNAPP and container security solutions. CWPP and CNAPP solutions provide multifunctional control — including workload-specific protection and network security — for infrastructure as a service (IaaS) environments.

Select cloud security capabilities to address visibility, misconfiguration and privileged activity in each cloud deployment. Start by choosing an appropriate set of native security controls, and then augment those controls with third-party capabilities to provide additional security.

Figure 10 illustrates security components for this architecture.

Figure 10: Application Security Reference Architecture



Source: Gartner
796440_C

Gartner

Workloads host software that is likely presenting using APIs. API abuses and exploits are the most frequent types of attack against organizations, and they can result in serious enterprise data breaches. Take a comprehensive approach to protecting APIs by:

- Discovering APIs in the environment
- Leveraging API management and mediation
- Using web application and API protection (WAAP) platforms
- Mitigating bot and fraud attacks
- Implementing modern authentication and authorization solutions
- Detecting anomalous API usage with behavioral technology

Related research:

- How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB
- Advance Your Platform-as-a-Service Security
- Protecting Web Applications and APIs From Exploits and Abuse
- Container Supply Chain: 10 Security Vulnerabilities and How to Address Them
- API Security Maturity Model
- API Security: What You Need to Do to Protect Your APIs

Work With Development Teams to Secure the Use of Generative AI Coding Assistants

Development teams are experimenting with, and using, AI coding assistants like GitHub Copilot to generate application code and test cases, as well as designs, threat models and technical debt analyses. Although these tools increase development teams' productivity, they pose significant risks that need to be considered by security and compliance teams. These risks include:

- **IP risk:** Because GenAI systems are producing content based on data that has been previously ingested, they can produce content that infringes on the IP rights of the original authors. For example, GitHub Copilot has been found to produce code that is almost identical to copyrighted code functions published by other developers. This has led to a class-action lawsuit (still in progress) against Microsoft, OpenAI and GitHub for violation of software licensing terms.
- **Confidentiality breaches:** GenAI systems often store data in the cloud, which can increase the risk of data leakage, given that these systems are immature and rapidly evolving. For example, in March 2023, there was a leakage of prompt history across user boundaries in ChatGPT, which resulted in OpenAI initially shutting down ChatGPT and then restarting it with that feature disabled.
- **Software vulnerabilities:** GenAI is well-known for "hallucinations" (incorrect statements presented as facts) when generating content. Similarly, generated code, test data, documentation and API specifications can contain potential security vulnerabilities. If a developer relies on AI to generate code, that code may contain bugs that the developer cannot detect.

Security teams should work closely with development teams to understand the usage of these systems across the organization. While it may be tempting to put strict bans on their usage, this may only encourage "shadow AI." Organizations should look to some of the following processes to address the risks posed by GenAI tools:

- Continue application security testing practices by using static and dynamic analysis tools, as well as SCA to identify vulnerable code and third-party packages. This should be done regardless of who writes the code (human or otherwise). If these tools are not currently being used in DevSecOps pipelines, they should be explored before extensively using AI coding assistants.
- Encourage development teams to create processes in which senior developers review the AI-generated code. This could be part of standard code review processes. If such review processes are not currently in place, this may reduce some of the benefits of GenAI tools.
- Advise development teams to use code assistance tools and vendors that offer the ability to refine models based on your own code repositories, and that offer the option to retain full control of these new models and prompts used for generative code.

Related research:

- Emerging Tech: Generative AI Code Assistants Are Becoming Essential to Developer Experience
- Quick Answer: Can Generative AI Help Manage Technical Debt?
- Assessing How Generative AI Can Improve Developer Experience

Security Operations With Automation Will Enhance Capabilities

Security monitoring technologies have seen great evolution and adoption, with security information and event management (SIEM) still acting as a central component of monitoring and response capabilities. The application of advanced analytics, including the use of AI techniques, has been driving the evolution of security monitoring. The goal is to complement static rules and simple correlations with more data sources, ML and advanced visualizations. Additionally, as GenAI technology matures, especially for SecOps, we may see this technology help with staff shortages by allowing organizations to hire less-skilled or even nontechnology-centric personnel for tasks like Tier 1 analysis. This could also help in terms of a diversity of background, because hiring from a pool of candidates who are not traditionally technical could bring different perspectives to an organization and fresh perspectives to operations.

SIEM has incorporated user and entity behavior analytics (UEBA) and security orchestration, automation and response (SOAR) capabilities. It remains the primary threat detection and response center of organizations. Security solutions that are closer to, and purposely built for, protected resources continue to emerge to augment SIEM in providing resource-specific security control (examples are ASM, SSE and CNAPPs). Some of these solutions include threat intelligence and behavioral analytics features that increase the overlap of capabilities across the security spectrum. XDR integrates threat intelligence and telemetry data from multiple sources, primarily with native sensors, and uses security analytics to provide contextualization and correlation of security alerts.

In addition, organizations continue to struggle with staffing and skills for security monitoring. Security monitoring is time-intensive — not only in terms of the actual monitoring of operations, but also of the maintenance of content such as correlation rules. Even when security monitoring is heavily automated, staffing is still an issue when organizations are reviewing events and reports. In advanced security operations, additional staff members are needed to perform threat hunting and threat intelligence operations, but people with these specialized skills are especially hard to find. Managed services, such as managed detection and response (MDR), help organizations address this issue. In addition, increased automation — both integrated into existing tools and provided in the form of SOAR tools — helps scale existing security operations staff.

Planning Considerations

Use Vendor-Validated Detection Stacks for Cost-Effective Detection of Threats

Clients often ask Gartner how to make their threat detection and response, or SOC, "work better." Many clients invest in building a threat detection and response (TDR) practice, but few are able to get the performance results they expect. Often, clients' goals are rather modest. They wish to detect and respond to the most common attacks they face. The default journey is to build their own detection stack capable of detecting current threats and then operate it effectively.

A detection stack traditionally is not something you can purchase. It is something you have to design and build. A detection stack will generally consist of:

- Points of threat-specific observation
- General telemetry ingestion
- External knowledge about threats
- Telemetry aggregation and analysis
- Monitoring
- Workflow and response
- SecOps assistants

The do-it-yourself (DIY) approach to building a detection stack generally involves deploying and integrating several key technologies well, and then operating them excellently. For example, a customer may use network detection and response (NDR), an intrusion prevention system (IPS) and endpoint detection and response (EDR) for threat observations, and then use a web proxy, email and access telemetry for context. One or several threat intelligence services are retained, and a SIEM is deployed as the central data collector, analyzer and point of monitoring. Lastly, a ticketing system or SOAR solution for workflow and response is put in place.

This DIY approach works well on a large scale, and is highly extensible. However, for many clients, the complexity and operation of so many moving parts does not work well, even if the "parts" are of the highest quality.

As a planning consideration, you should evaluate your detection stack approach against your monitoring objectives, your current performance levels and the cost. Or simply compare the value of data in your stack with the quality of alerts. When evaluating your current tools, keep in mind that newer tools are pivoting toward security data analytics and a security intelligence layer (that is, the CSMA approach) to provide enhanced insights and detections. Here are a few key indicators that your current DIY detection stack should be reevaluated against a vendor-validated solution:

- **Cost overruns:** SIEM cost overruns are still cited as a major client issue. Data ingestion and detection are competing priorities. Team members and/or service providers to handle the operations of the DIY approach can also add to cost overruns.
- **Limited needs:** A highly extensive system is great, if you need to be highly extensible. For many clients, however, their detection needs are rather common. Named attacks, or attacks against named asset types, are not unique. Understanding a common threat and building detections is best done at scale. If the primary reason for a DIY stack is common threat detection, you should reevaluate vendor-validated detection stacks.
- **Scale issues:** The work required to maintain and operate the DIY stack exceeds the resources available.
- **Reactionary/tactical:** Security operations teams can often spend many hours building detection rules and content that has been figured out by a vendor. Building detections for common threats is sometimes better left to vendors.

- **Detection misses:** The best efforts of your DIY detection stack miss major common threats.

The use of DIY detection stacks to build TDR practices is being challenged by both product vendors and service providers. A number of vendors now offer converged detection stack solutions that promise to reduce the many burdens involved in designing and building a practice yourself. Effectively, the vendor is the detection stack architect, and how well the overall stack performs is a major hire/fire criterion, more so than the feature criteria of any one particular part.

For service providers, a validated detection stack is one they build themselves or one whose design they greatly influence. It is a lot easier for providers to offer a predictable service on top of a known detection stack than it is for them to try to learn your DIY detection stack and then offer a service.

Clients wishing to learn more about this planning consideration should investigate solutions such as XDR, threat detection, investigation and response (TDIR), MDR and co-managed SIEM.

Related research:

- The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations
- Is Security Operations Ready for XDR?
- Quick Answer: Key Questions to Ask When Selecting a Managed Detection and Response (MDR) Provider
- Quick Answer: Insourced, Outsourced or Hybrid? Which SOC Model Is Right for You?

Evaluate Your Automation Strategy for Increasing Security Operations Efficiency

Automation for security operations is having a renaissance. It remains a popular topic of client inquiry, and Gartner has yet to meet a client who does not want to automate something in operations.

As a planning consideration, automation as part of operations should be a key consideration. However, Gartner recommends that you be very selective about automation goals and the ways in which automation is consumed.

Automation goals should be based on anticipated measurable gains (or improvements) in your security operations. Can something you do now be made better, faster or cheaper by introducing automation? These assessment goals should align with specific objectives or use cases. A use case should not only be conducive to automation but also a big-enough concern that the automation would be cost-effective.

Common good Phase 1 automation goals include:

- Enhance alert fidelity by enriching context.
- Facilitate common alert-handling tasks.
- Document incidents and incident candidates.
- Provide ticket and workflow support for incident handling.
- Investigate and respond to phishing and email security incidents.
- Codify and execute a response playbook.

Examples of bad Phase 1 automation goals include:

- Automate all responses to alerts. This is bad because there are too many decisions to codify.
- Automate all alert investigations. This is bad because critical thinking is involved, for which an investigative method is better.
- Automate all alert handling. This is bad because playbooks are deterministic and not great at handling the unknown.

Another planning consideration is how best to consume automation. Should an independent automation platform like SOAR be used? Or can onboard automation functions be used as part of a SIEM, IT service management, threat intelligence, XDR or other platform?

Gartner is seeing an increase in automation functionality being offered by non-SOAR vendors. Although there are many criteria to consider when looking at an automation platform, the area of domain expertise stands out. Automation by itself serves no purpose. Automation is made to make something else better or faster. What that something else is constitutes a domain area unto itself. For example, a domain expert for threat intelligence will have great insights (and likely automation playbook content) into how to enrich an alert with threat intelligence. Similarly, a domain expert in ticketing and workflow will likely have the best knowledge about automating workflows. And a security alert pipeline expert will likely have the best idea of how to automate things inside a SIEM solution.

As a planning consideration for automation, carefully weigh the unbiased freedom of an independent SOAR vendor against the automation features provided by a domain expert, as part of their core platform. If you find your true automation goals mostly relate to improvements in one domain area, the choice of automation as a feature becomes easier.

Related research:

- SOAR: Assessing Readiness Through Use-Case Analysis
- A Guidance Framework for Architecting and Deploying a Modern SIEM Solution
- Charting Your Journey to a Modern SOC in 3 Steps

Enrich Asset Risk Data by Aggregating Indicators to Optimize Exposure Management in Security Operations

Maintaining an accurate asset inventory has consistently been the No. 1 critical security control advocated by many independent security organizations, and for good reason. How can you protect against all the threats you have identified without knowing what you have? Now, with multicloud and diverse software architectures, it is more difficult than ever to understand what you have. It is not that the data does not exist in some form, but rather that aggregating it efficiently and effectively has eluded most organizations. Additionally, maintaining an asset list is mostly a manual endeavor.

Security operations cannot solve the asset inventory challenge. However, they can enrich asset context with risk indicators from security tools and nontraditional tools that exist in the enterprise. The additional risk context will contribute to a more effective exposure management that focuses on threats that can actually be realized. Some indicators will be easier to incorporate into asset data. Others will take some level of risk mapping to realize the contextual benefit. Cyber asset attack surface management (CAASM) tools can automate ingestion and aggregation of these indicators to enrich exposure management processes.

There are several indicators that can assist:

- Compensating/mitigating controls data from vulnerability assessment, EDR, web application firewall (WAF), proxy and other security tools.
- Data classification information from data classification tools, instead of manual entry into a configuration management database.
- Architecture attributes that are defined in IaC in DevOps and cloud environments.

Related research:

- A Guidance Framework for Developing and Implementing Vulnerability Management
- Using Security Testing to Grow and Evolve Your Security Operations

Evaluate Generative AI to Enhance Detection and Response Automation

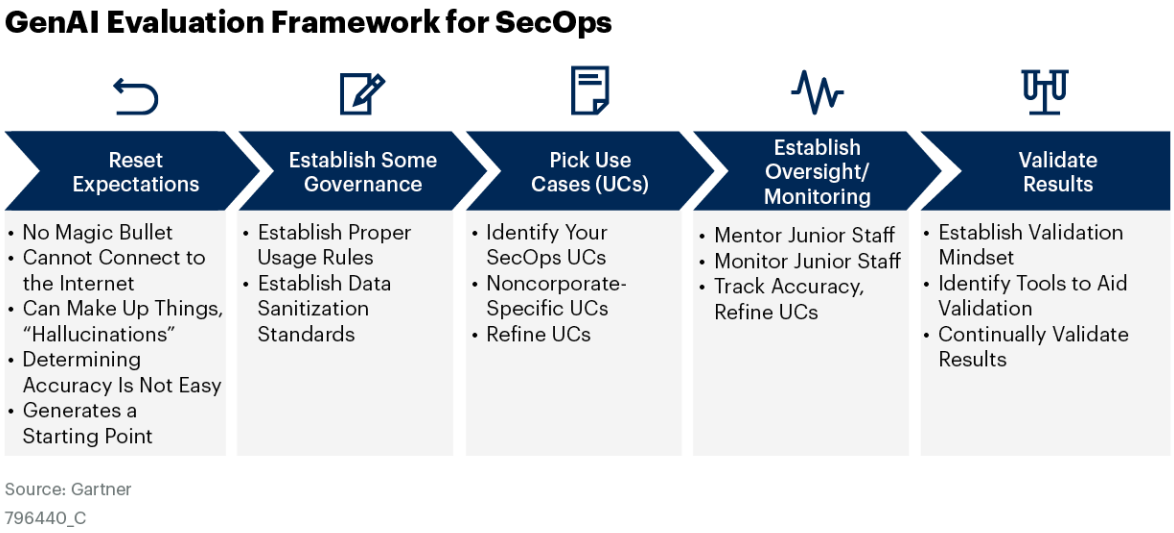
GenAI has been at the forefront of many organizations in recent times. In recent months, Gartner has seen an increase in client interest in this technology. SecOps organizations are primarily interested in understanding what vendors are planning to do with GenAI, how best to use it in their organization, and how to secure its usage. This technology, and its adoption, is changing day by day. We are seeing vendors announce GenAI capabilities before they have fully understood how they will be used; it is almost like it is a solution looking for a problem. Gartner recommends that SecOps organizations take an evaluative approach to this technology, whether previewing a vendor's implementation or making a build decision. To the extent possible, perform a proof of concept (POC) in order to understand if this technology fits into your organization. It is also recommended that you utilize a nonproduction environment, such as a quality assurance (QA) or preproduction environment, in order to conduct the evaluation.

As a planning consideration, SecOps organizations can use the following framework as a guide to help them plan how to evaluate GenAI technology:

- **Reset expectations:** This technology, at least today, is no magic bullet, and is likely never to be one. It can help organizations generate starting points for things like playbooks, tabletop exercise scenarios and so on. However, care needs to be taken to evaluate responses generated from this technology, as it can generate made-up information.
- **Establish governance:** Even for a POC, proper governance should be established and followed. This includes educating users about what is and is not permissible and what data can and cannot be used in a GenAI POC (such as sensitive data and personally identifiable information)
- **Pick use cases:** Today, most GenAI technology, whether ChatGPT or technology built into a security product, focuses on solving particular use cases (detection engineering, incident response, playbook creation and so on). It is critical that SecOps organizations identify use cases that are amenable to such technology, but that also do not have implicit real-time response requirements. This is because you will need time to evaluate the responses and outputs from such technology for correctness.
- **Establish oversight/monitoring:** Monitoring the usage of GenAI technology is critical in a POC. For example, if junior team members will use this technology, senior staff members should oversee and evaluate output from junior staff.
- **Validate results:** Identify people, processes and technologies that can aid in validating results from GenAI technology. For example, if you need to validate a recommended regular expression for parsing a log message, there are any number of online tools that can quickly help with this task. Be aware and test for the nondeterministic nature of GenAI to ensure consistent security outcomes are achieved.

Figure 11 summarizes these recommendations.

Figure 11: GenAI Evaluation Framework for SecOps



Gartner

Related Research:

- Quick Answer: How Can Security Operations Teams Leverage ChatGPT?
- Quick Answer: How to Use ChatGPT and Generative AI Securely With Minimal Data Loss

Data Security Will Be Key to a "Data Everywhere" World

Data is growing at an impressive rate. In 2024, global data storage is forecast to be double what it was in 2022. [2] Many organizations have been using a "file and forget" data storage strategy, so there is truly little visibility into this growing data. Stored data that businesses have zero visibility into is "dark data." Estimates point to anywhere from 55% to over 80% of the data that a business stores as being dark. [3] Lurking within this dark data are unknown risks to organizations' security posture, as it may be tempting for malicious actors to steal or tamper with such data.

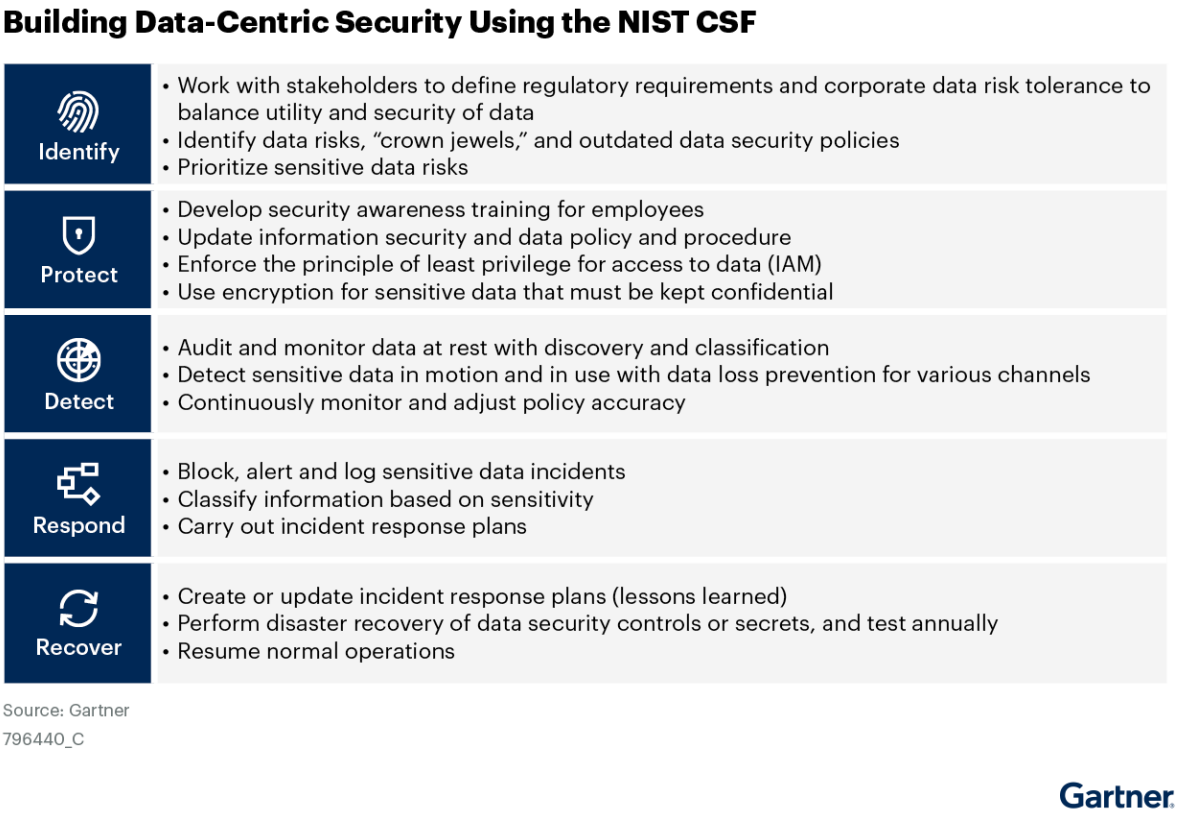
At the same time, organizations' regulatory obligations to govern this data are multiplying. Gartner predicts that, by the end of 2025, 75% of the world's population will have its personal data under the purview of some privacy regulation. Data that was not regulated 10 years ago when it was stored is possibly subject to regulation today. Privacy regulations are rarely technically prescriptive and sometimes appear contradictory or at least highly nuanced. However, Gartner does see consistencies in these regulations that support a more simplified strategy. Securing data and enabling privacy compliance within data warehouses and big data/advanced analytics pipelines are topics of increasing concern for many clients, where regulations may be seen to conflict directly with the needs of businesses.

Planning Considerations

Get Visibility Into Dark Data Using Discovery, Classification and DLP for Proactive Data Protection

Data-centric security, based on architectures that ensure that data is the focus of protection, is essential in today's "always on," "data everywhere" world. Attempts to tackle all aspects of data security at once are not only expensive but may not show immediate benefits and can have a severe business impact. Therefore, a targeted approach for each business use case is more effective when rolling out a protection strategy. Organizations should augment their core security architecture using a data-centric approach, adopting tools and techniques from Sherwood Applied Business Security Architecture (SABSA) and NIST. Figure 12 is a data-centric security framework based on the NIST Cybersecurity Framework (CSF).

Figure 12: Building Data-Centric Security Using the NIST CSF



The NIST CSF framework starts by laying the foundations for data security with people and policy, and for the controls and processes to put in place later. Next, discovery of and visibility into business data is critical because it is increasingly important to know where data is and to get deep insight into how users and machines are using it. Organizations seek to understand how authorized applications are being used and to identify the unsanctioned ones ("shadow IT") and where their data is being stored.

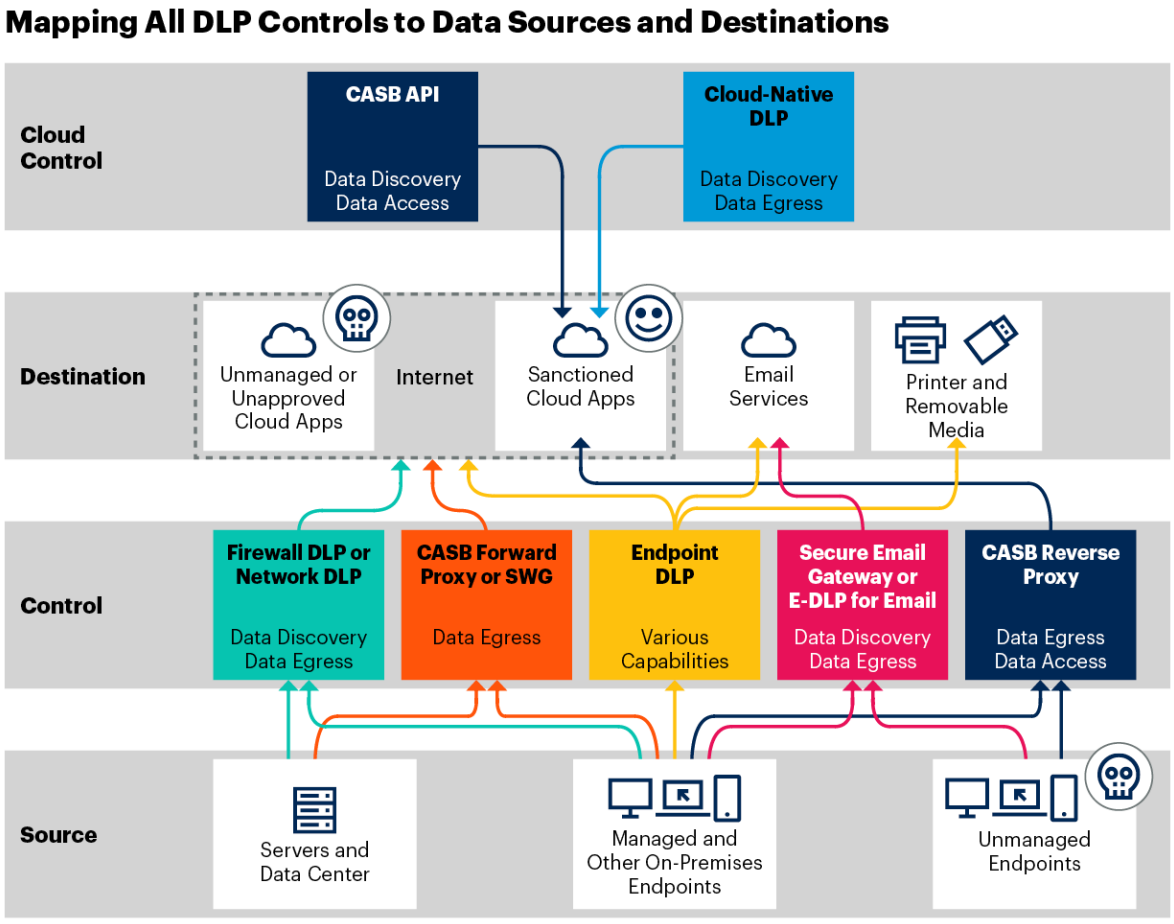
You cannot protect the sensitive data that you do not know exists. Get visibility into this data using data discovery and classification capabilities. These are found in file analysis (FA), data access governance (DAG), data security posture management (DSPM), CASB, SSE and even data loss prevention (DLP) tools. They can apply a tag or a label data for later identification or for immediate actions such as blocking the content with DLP, applying encryption or protecting with enterprise digital rights management (EDRM). These identifiers can simplify policy rule logic and maintenance. However, while the above tools include classification capabilities as part of their decision-making processes, a common complaint from Gartner clients concerns the resource overhead for maintaining them. Although some SSE vendors can provide their own classification capabilities, this activity should be centralized and use a common policy for all DLP use cases.The good news is that most solutions can assist with the growing privacy regulations and consolidate data visibility and monitoring among different data sources.

Discovery and classification solutions can automate classification using techniques like ML and AI. These solutions can help determine data sensitivity, as well as other categorizations such as source code, HR data and purchase orders. These solutions come in many different forms, such as pretrained, user-trained and dynamically trained. Using data discovery and classification, organizations can efficiently maintain data catalogs of their sensitive data on-premises and in the cloud, and begin:

- Gaining visibility into dark data, while uncovering any risk lurking within it, and prioritizing and mitigating those risks.
- Reducing redundant, obsolete or trivial (ROT) data to decrease storage costs and compliance risks.
- Reducing overly permissive access to data by applying the least privilege and “need to know” principles in order to lower data risk.
- Continuously monitoring, auditing and protecting data.

See also Figure 13.

Figure 13: Mapping All DLP Controls to Data Sources and Destinations



Data is everywhere, and now so is DLP. DLP capabilities are found in many other tools that cover the many different areas where unstructured or semistructured data is found. For instance, DLP capabilities are found in email, cloud, firewall, SSE and CASB SWG products. Aside from data encryption, DLP remains the last line of defense to protect data in motion, in use and at rest when all other measures have failed. It is important to note that DLP does have its limitations, which motivated attackers could use to work around it, so it is by no means a catch-all (see 5 Steps to Successfully Implement Data Loss Prevention). Use a data-centric approach to build your data security, based on concepts from SABSA and NIST. Build security hygiene further upstream in the data life cycle by focusing on people and processes. This lays the foundation for a good DLP program and data security in general. Use a risk-based approach to prioritize DLP deployment based on where data is used most in the organization (for example, email, cloud and endpoints). Identify where DLP is available within your existing controls. Decide whether "best in class" is necessary or if "good enough" will suffice; there is often a trade-off between the two.

Related research:

- Improving Unstructured Data Security With Classification
- Choosing the Right Data Loss Prevention Architecture
- 5 Steps to Successfully Implement Data Loss Prevention
- EDRM, Your Key to Unstructured Data Protection Through Encryption
- Top 5 Data Security Use Cases You Must Address With Unstructured Data

Promote Zero Trust by Utilizing Data-Centric Security Architecture

The CISA Zero Trust Architecture model outlines five pillars of zero trust: identity, devices, networks, applications and workloads, and data. Given the complexity of deployment and the potential associated costs, it is often not pragmatic for organizations to simultaneously implement the underlying controls within each pillar. Organizations should not take an "all or nothing" approach to improving their zero trust maturity. Instead, they should focus on implementing or improving controls within a specific security domain (or pillar), such as the data pillar, and strengthen data security by utilizing Gartner's Data-Centric Security Architecture (DCSA). The data-centric controls outlined in the DSCA, such as data mapping, data discovery, data categorization and classification, access controls, data masking and encryption, EDRM, and data loss prevention (DLP), are closely aligned with the data functions listed in the CISA Zero Trust Maturity Model (ZTMM). Therefore organizations should use the DCSA framework to design and implement a holistic approach to data security that can feed into ZTAs to make better access decisions.

The DCSA yields a holistic strategy that ensures comprehensive protection of sensitive data, both structured and unstructured, which directly promotes zero trust principles. The first step of the DCSA framework is data mapping, and it provides the foundational context that informs other data-centric controls. Mapping data answers key questions surrounding data categories, data locations and business processes. Key questions in the data-mapping process should include:

- What types of data does the organization have?
- Where is data stored?
- What is the purpose of the data?
- Who should (or should not) have access to the data?

Data discovery, categorization and classification expand on the data-mapping process by recording what is found, providing additional context, and assigning levels of criticality and sensitivity to data in an organization. By meticulously and continually assessing the value and sensitivity of different data types, organizations can tailor their security measures accordingly. This proactive approach aligns with both zero trust and data-centric principles, as it enables precise targeting of protective measures, based on the unique attributes and risk profiles of each data category.

Data access governance reinforces an overall data security approach by promoting and enforcing the philosophy of “least privilege” and can provide foundations for continuous adaptive trust (CAT). This practice not only prevents unauthorized access but also mirrors the data-centric concept of protecting data itself, irrespective of its location. The level of granularity achievable with access controls is often dictated by several factors, such as the organization’s size, the supporting infrastructure, the amount of data that needs protecting, and IAM maturity. Organizations should continuously evaluate and enforce role-based and attribute-based access controls at the most granular level achievable to limit the number of people that have access to sensitive data, promote efficiency of subsequent security controls, and reduce overall risk. In tandem with this, DLP mechanisms ensure constant surveillance over data interactions. By monitoring data movement within and outside an organization, these mechanisms align with the data-centric notion of safeguarding data wherever it travels, reducing the risk of breaches and maintaining data’s integrity.

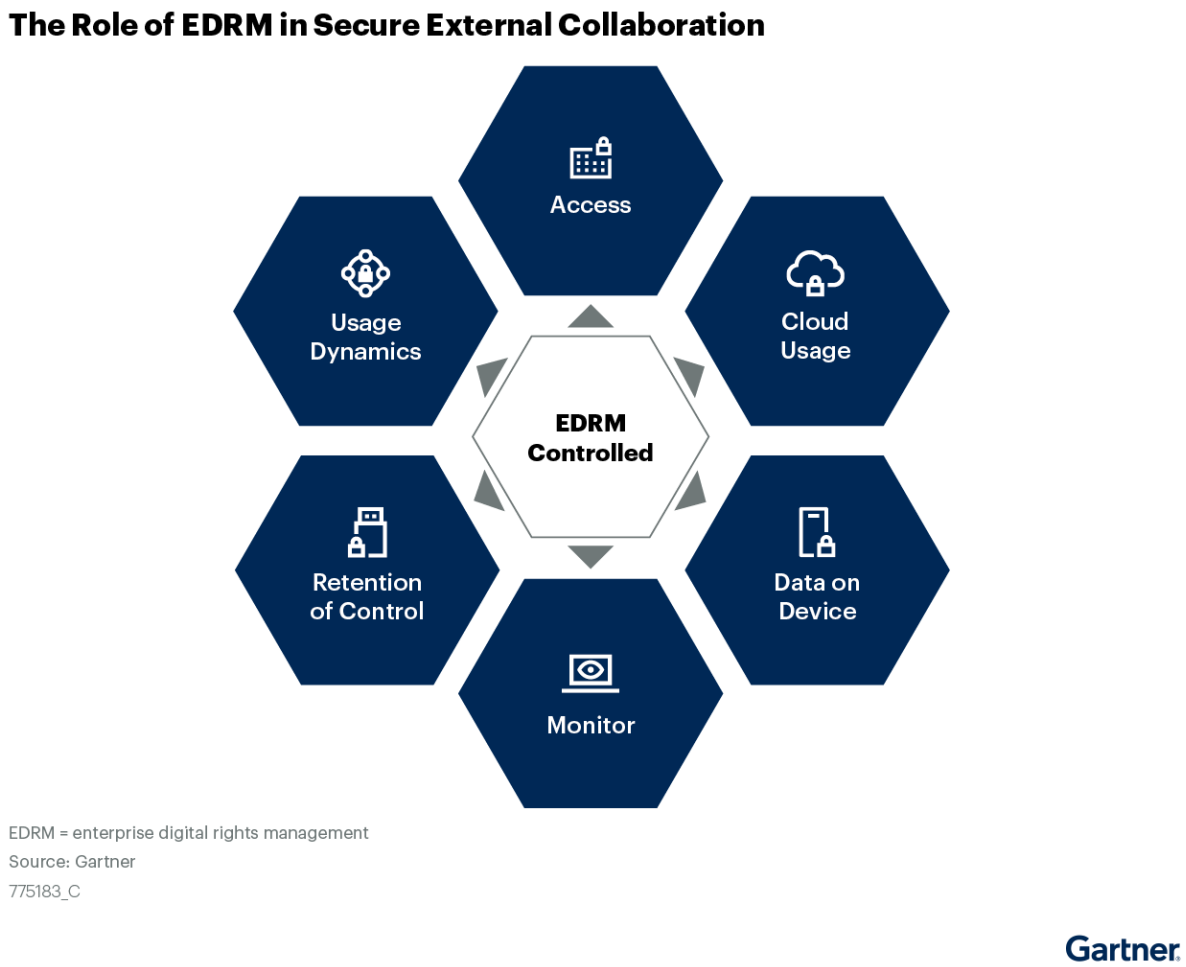
Implementing encryption at rest and in transit underscores the commitment to protecting sensitive data, regardless of the circumstances or location. By achieving confidentiality, separation and controlled access using encryption, you meet the aims of the DCSA and align with zero trust principles. You align with both approaches by ensuring that even if a breach occurs, the information remains indecipherable to unauthorized parties. Given advances in quantum computing and the potential for cryptanalytically-relevant quantum computer (CRQC) capabilities, quantum-resistant cryptographic algorithms could become foundational for authentication mechanisms. Therefore, CISA, the National Security Agency (NSA), and NIST have suggested that organizations begin to create quantum readiness roadmaps. Readiness activities should include conducting inventories, applying risk assessments and analysis, and engaging vendors.

Perhaps the most notable data-centric control that promotes zero trust is enterprise digital rights management (EDRM). EDRM comprises solutions that provide fine-grained and identity-aware control over persistently protected information using:

- **Cryptography:** Information is encrypted so that protection travels with data no matter where it moves or rests.
- **Identity:** Users must authenticate before consuming rights-protected data (even on their systems), and policies relate to specific user roles and groups.
- **Granular usage controls:** Users are granted specific rights within applications, such as the ability only to view, review, edit, print, copy/paste or screen-capture sensitive information.

EDRM protects, tracks and revokes rights to data even after it is shared. Figure 14 illustrates the role of EDRM in the context of secure external collaboration.

Figure 14: The Role of EDRM in Secure External Collaboration



Related research:

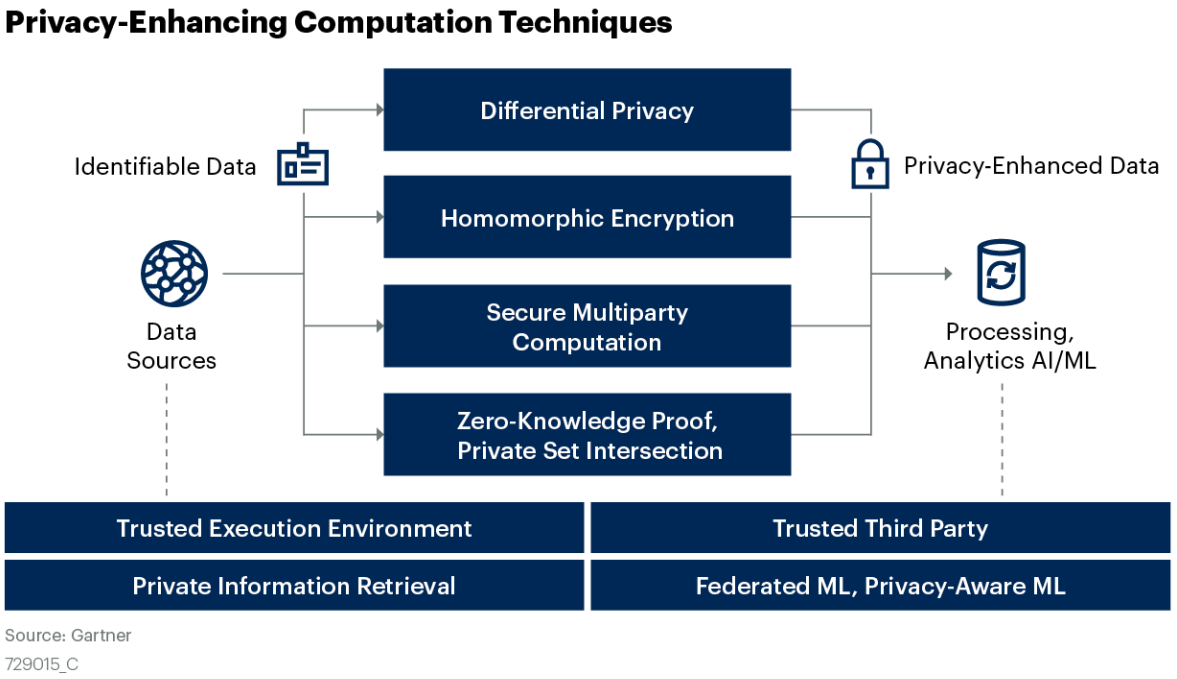
- Guide to Data Security Concepts
- Build Once, Use Many Times: Use Privacy Engineering to Support a Data-Centric Security Architecture

Define Use Cases to Address the Data and Analytics Pipeline's Unique Security Risks

The data and analytics pipeline has many different uses, and there are many different data paths and storage locations for each of them. The use cases include insights from transactional data, reports, test data, analytics and ML, and other business insights pulled from data primarily stored in extraction, transformation and loading (ETL) tools, databases, data lakes, data warehouses, and now data lake houses. The practice of protecting the data within them is called structured data security. Each of these unique use cases has controls that should be matched to the risk tolerance and utility requirements of the business. Encrypt data at rest (DAR) using transparent database encryption (TDE), format-preserving encryption (FPE), or tokenization to address specific threats, attacks, or other use cases such as sharing data with a third party or allowing computations without revealing any sensitive data. Caution must be taken when deciding how, where, or even if this protection should be applied. Decisions such as whether protection should be used at ingest time, in the data store, at data access, or after the data is retrieved must also be considered. For instance, it makes more sense to have the data encrypted at the application level using application layer encryption (ALE) than to focus on separate data stores for certain instances. The options available all depend on what is consuming the data downstream, while access control and monitoring form the foundation of structured data security.

Advanced analytics — ML and GenAI — has taken center stage as enterprise functions have become increasingly data-driven. Technical professionals frequently have difficulty designing security and privacy into a big data and advanced analytics platform, where data silos, data flows and entitlements are largely opaque. In addition to the currently dominating “walled gardens” or enclaves for advanced analytics (where data scientists are largely unrestricted), clients should evaluate more granular data-centric controls that address privacy, entitlement or visibility of data across many silos. In particular, for use cases involving data sharing, multiparty data analytics and computation in untrusted environments, clients should consider the emerging privacy-enhancing computation (PEC) techniques shown in Figure 15.

Figure 15: Privacy-Enhancing Computation Techniques



Hyperscale cloud providers have recently started to offer trusted execution environments, and these can be readily adopted to provide enhanced security and privacy in the cloud. Other technologies, such as homomorphic encryption, secure multiparty computation and private information retrieval, have transitioned from academic research projects to commercial solutions. Security teams should assess the differences between these technologies, and support business and data teams in understanding how privacy-enhancing approaches enable greater use of data.

Related research:

- Securing the Data and Advanced Analytics Pipeline
- Protecting PII and PHI With Data Masking, Format-Preserving Encryption and Tokenization
- Achieving Data Security Through Privacy-Enhanced Computation Techniques

Computing Hosts Will Need Specialized Protection Profiles

Endpoints remain a big target for advanced adversaries, and are often the first foothold for further incursions. Instead of just stealing sensitive information from endpoints, adversaries are now launching much more commercially attractive attacks, such as ransomware, supply chain attacks and business email compromise attacks.

Popular modern endpoint, mobile and server operating systems (OSs) generally provide a strong security baseline, as long as the security capabilities and settings are carefully managed. However, these settings can be compromised with low-level exploits delivered through a phishing email or downloadable payload. Threats are not limited to phishing or malicious applications; users can also accidentally give unwanted apps privileges that are too powerful. Behavioral analysis and EDR techniques are required to block and/or detect more advanced malware and fileless attacks. The larger endpoint protection platform (EPP)/EDR vendors traditionally focused on Windows, macOS and Linux protection. But with the continued growth in mobile usage, vendors have expanded their solutions to include mobile security features from mobile threat defense (MTD) products. Adding MTD to EPP/EDR offers a unified view into all endpoints, putting such solutions into the unified endpoint security (UES) category. Security professionals will need to review the settings within those OSs on a regular basis as new features are often deployed with updates. Special attention needs to be paid to default settings as they constantly evolve with updates.

The use of employee-owned devices outside corporate networks has accelerated, and Gartner expects this to be an irreversible trend. Endpoint management and endpoint protection continue their move to the cloud, enabling not just continued management and monitoring of remote devices but also the scale, flexibility and analytics capacity required for advanced TDR. Some organizations use mobile application management (MAM) tools to provide secure access with personal mobile devices, given the recent large-scale work-from-home situation. We are now seeing vendors providing MAM-like capabilities on macOS and Windows devices, which will enable more organizations to let employees work from personal devices.

The security of endpoints is closely linked to cloud and collaboration technologies. Providing secure access to collaborative cloud services, such as Microsoft 365 and Google Workspace (formerly G Suite), is a key consideration for many organizations. CASBs, themselves often cloud-based, play a role in providing insight into, and exerting control over, cloud usage and user activity. Security teams should be aware of convergence across other security tools to support endpoint protection at the service edge (for example, SSE).

In addition to growth in end-user endpoints, organizations have to deal with a growing number of other devices that need access to their networks and agents that need to interface with applications and data. Internet of Things (IoT) devices are often not designed with enterprise security and manageability in mind — security is often weak by default, and configuration and patching are nontrivial. In addition, some of these devices are multihomed, combining a Wi-Fi or hard-wired network connection with cellular communications, thus creating possible entry points into an enterprise network. Various intelligent agents, such as virtual personal assistants (VPAs), and robotic process automation (RPA) take over human tasks, but their security is not yet well-understood and, consequently, best practices are still nascent.

Planning Considerations

Implement Preventive and Detective Controls, Including Ransomware Protection, on All Hosts

Today's definition of endpoint security is not restricted to laptops and desktops. Whether physical or cloud-based, all workloads that run on handheld devices such as mobile phones and tablets should be covered by a UES strategy that implements preventive and detective controls.

> **The question is: "On what systems in your organization do you want to deploy endpoint security tools to prevent attacks, seek complete visibility, conduct investigations and run incident response activities?" If you want the best breadth and depth of prevention and detection, your answer has to be: "All systems."**

However, the approach to implementing this strategy typically varies. Many organizations start their deployments with the most mission-critical systems, and then gradually cover the less critical endpoints.

You must review your malware protection architectures across networks, client endpoints and server endpoints:

- Assess standard hygiene practices — including vulnerability and configuration management and data backup — across OSs and applications.

- Audit configurations of security solutions to ensure they are optimized and integrated for detection across networks and endpoints.
- Use one or more endpoint and mobile solutions to provide not only prevention capabilities but also detection and response capabilities that help reduce the time to recover from a successful attack. EDR and MTD are examples of these solutions.
- For high-risk or high-threat environments, consider technologies that sacrifice some user experience or solution complexity for increased security. Examples include RBI and content disarm and reconstruction (CDR) technologies. Look first for integrations with your existing solutions, such as secure email gateways (SEGs) and SWGs, before expanding to broader use cases.
- Set standards for the minimum supported hardware and OS versions, and configure them securely. Update these standards yearly at minimum. Use native device features, such as isolation, and maintain proper hardening and patching of OSs and other software. Use third-party endpoint anti-malware and/or application controls where vendor-provided controls have proven insufficient.

Various technologies have matured and are used on a large scale. These include exploit mitigation, malware detection and prevention, containment, behavior analysis and EDR. Some technologies, such as CDR, are emerging as preventive approaches.

It is no longer enough to have controls in place. Monitoring is now a requirement for organizations that want to secure their endpoints completely.

To reduce friction, organizations should consider reducing the number of consoles being used for monitoring the data captured by their EDR solutions, whether through vendor consolidation or use of vendor-supported MDR.

The market for EPP solutions is changing, and traditional vendors are no longer the obvious choice for some buyers. On mobile devices, MTD solutions provide application risk management, network protection, device protection and mobile phishing protection beyond what is provided by the OS, unified endpoint management (UEM) and mobile device management (MDM). For consumerized mobile use cases, consider building security checks and device independence into apps. For example, build in kernel mode attack and jailbreak detection, software updatability, and application shielding/runtime application self-protection by leveraging software development kits (SDKs) from MTD and mobile app security vendors.

Network protection of users and endpoints is still necessary, and the availability of cloud-based network protection solutions simplifies deployment. SWGs and SEGs are critical for most organizations' malware and phishing defenses, and network sandboxing approaches have become common for better malware detection. Roaming users also need protection from other network attacks, such as rogue Wi-Fi access points, and MTD provides this capability.

In addition, security awareness initiatives, such as anti-phishing and anti-malware training, are usually required. Well-designed programs meaningfully increase awareness and thus render people less likely to make bad security decisions by accident or on purpose. Clarity, reinforcement and timeliness — such as sending a bulletin when a phishing email gets through the email filter — are key.

As more advanced attacks surface, human-operated ransomware is becoming an inevitable threat. To combat it, a mix of multiple detection and prevention controls and a solid backup/recovery process is essential. The importance of EDR to the modern enterprise is well-illustrated by the following statement, which was included in an executive order issued by the U.S. federal government in May 2021: [4]

> **"FCEB Agencies shall deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response."**
>
> — *The White House*

XDR is a maturing offering from EPP/EDR vendors. Gartner defines XDR as follows: “Extended detection and response (XDR) … delivers security incident detection and automated response capabilities for security infrastructure. XDR integrates threat intelligence and telemetry data from multiple sources with security analytics to provide contextualization and correlation of security alerts. XDR must include native sensors, and can be delivered on-premises or as a SaaS offering. Typically, it is deployed by organizations with smaller security teams.”

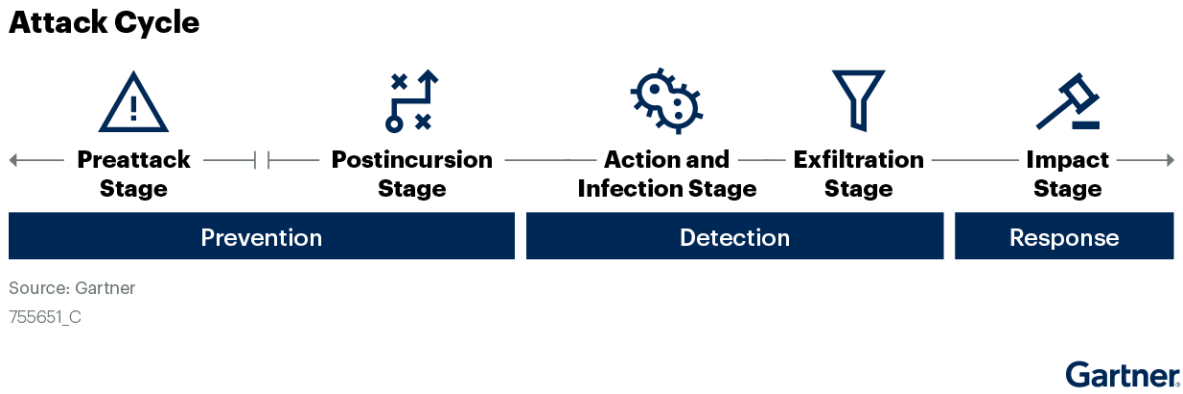
Gartner recommends that the following be part of any XDR offering:

- Threat intelligence
- Data lake
- Presence on the endpoint
- Orchestration
- A source of identity data for correlation

We see XDR as being best suited to midmarket organizations or organizations without SIEM.

As shown in Figure 16, any attack cycle, if split, has multiple stages. The preattack and postincursion stages are predominantly where prevention happens. Once the attacker has successfully infiltrated, detection controls become imperative to identify stealthy anomalous behaviors. Irrespective of the device the attacker is on, further harm can be avoided by having the appropriate response mechanisms. No single technique or control is a magic bullet, but implementing the right balance of multiple techniques assures a robust endpoint security ecosystem.

Figure 16: Attack Cycle



Related research:

- Understanding the Capabilities of Modern Endpoint Protection Platforms
- How To Choose an EPP/EDR That Fits Your Organization
- Mobile OSs and Device Security: A Comparison of Platforms
- Designing and Implementing a Ransomware Defense Architecture
- Guide to Endpoint Security Concepts
- Advance and Improve Your Mobile Security Strategy

Address Workload and Control Plane Security in the Cloud With a CNAPP

Cloud environments' inherent complexity and dynamism make it challenging to maintain a consistent, comprehensive overview of security risk exposure, thereby leading to potential undetected misconfigurations and vulnerabilities. CNAPPs aim to address these risks by consolidating a variety of cloud security functionalities into a unified platform, enabling comprehensive protection for cloud-native applications and their related infrastructure throughout their life cycle, from development to production.

CNAPPs represent an evolutionary approach to securing IaaS and PaaS cloud environments.

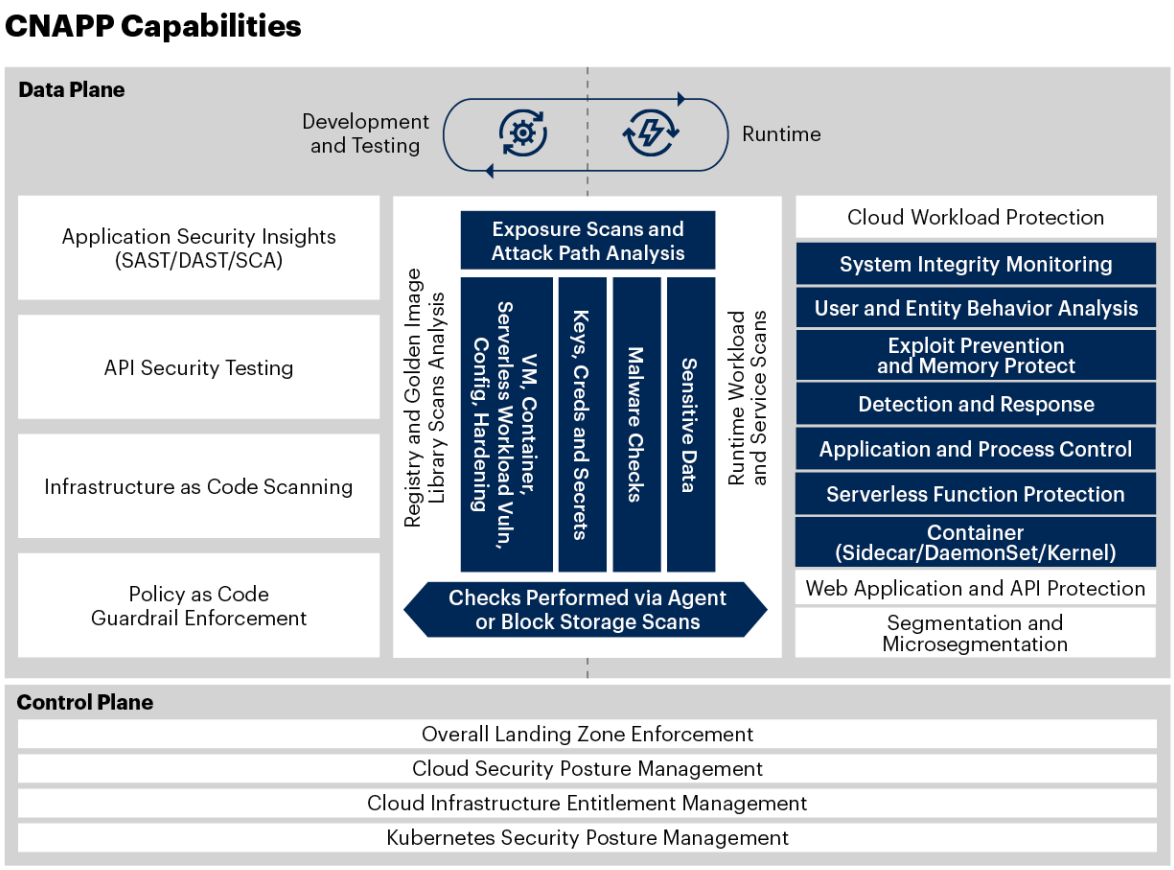
Unifying many previously disparate capabilities, CNAPPs incorporate features such as container scanning, CSPM, infrastructure as code scanning, cloud infrastructure entitlement management, and runtime vulnerability/configuration scanning in one platform. In doing so, they provide synergy (for example, posture context for workload security assessments and workload insights in posture management views). This consolidation marks a departure from earlier, fragmented tools that required multiple vendors. These often led to a lack of integration, creating an unclear view of risks and potential inefficiencies in developers' efforts to prioritize and remediate them.

CNAPPs put the cloud security puzzle together by combining stand-alone security tools to build functionality for shared insight. This functionality includes:

- CWPP
- CSPM
- Cloud infrastructure entitlement management (CIEM)
- Kubernetes security posture management (KSPM)
- IaC template testing
- Policy-as-code (PaC) creation and enforcement
- Application security testing software insights

Figure 17 describes the capabilities that Gartner sees comprising CNAPP offerings from vendors.

Figure 17: CNAPP Capabilities



CNAPP = cloud-native application protection platform; DAST = dynamic application security testing; SAST = static application security testing; SCA = software composition analysis; VM = virtual machine

Source: Gartner

775183_C

Gartner

A single, unified CNAPP solution offers a comprehensive platform that harnesses the power of shared insight across its capabilities. A single management plane reduces switching between multiple consoles to contextualize security findings, as opposed to having disparate management systems loosely integrated via API. An organization may need to deploy 10 or more tools with separate consoles to fully meet the capabilities of a CNAPP. A unified CNAPP solution reduces the potential for overwhelming and confusing security alerts by filtering out false positives and less critical issues. This targeted focus on significant risks greatly enhances the efficiency of security teams in their risk mitigation efforts and consequently optimize the overall security posture of their cloud-native applications.

An example of how contextual information from multiple capabilities can help prioritize data is a malware alert from a toward CWPP tool. A malware alert on a workload in an isolated development environment without internet exposure or access to sensitive data should have a lower priority than one for malware found on a high-value production system with access to sensitive data, a direct path to the internet, and accompanying suspicious activity. However, to properly prioritize malware alerts, you must obtain information from multiple capabilities to gain more context, such as network connectivity mappings, data sensitivity, suspicious activity and so forth.

CNAPP vendors have entered the market from different areas. Some were CSPM vendors that added CWPP along with other CNAPP capabilities. Some were container security vendors that moved into CNAPPs. Others were CIEM vendors looking to expand their portfolios. Consequently, no single vendor is best-of-breed in every capability.

Assemble a cross-functional team when evaluating CNAPP vendors, including development and security. Let the combined development and security team categorize and prioritize the enterprise's functionality needs into required, preferred, and optional tiers. This is essential, given that no single vendor excels in every aspect of CNAPP capabilities. Be wary of immature CNAPP solutions with missing core capabilities.

Before selecting a single-vendor CNAPP offering, conduct a functional pilot involving real developers and applications. This will ensure the system's functionality and the developer's experience align with your needs. During the pilot phase, ensure the system truly assists you in prioritizing risks effectively.

Related research:

- Solution Path for Security in the Public Cloud
- How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB

Treat Mobile Security as a Critical Element of Your Enterprise Attack Surface

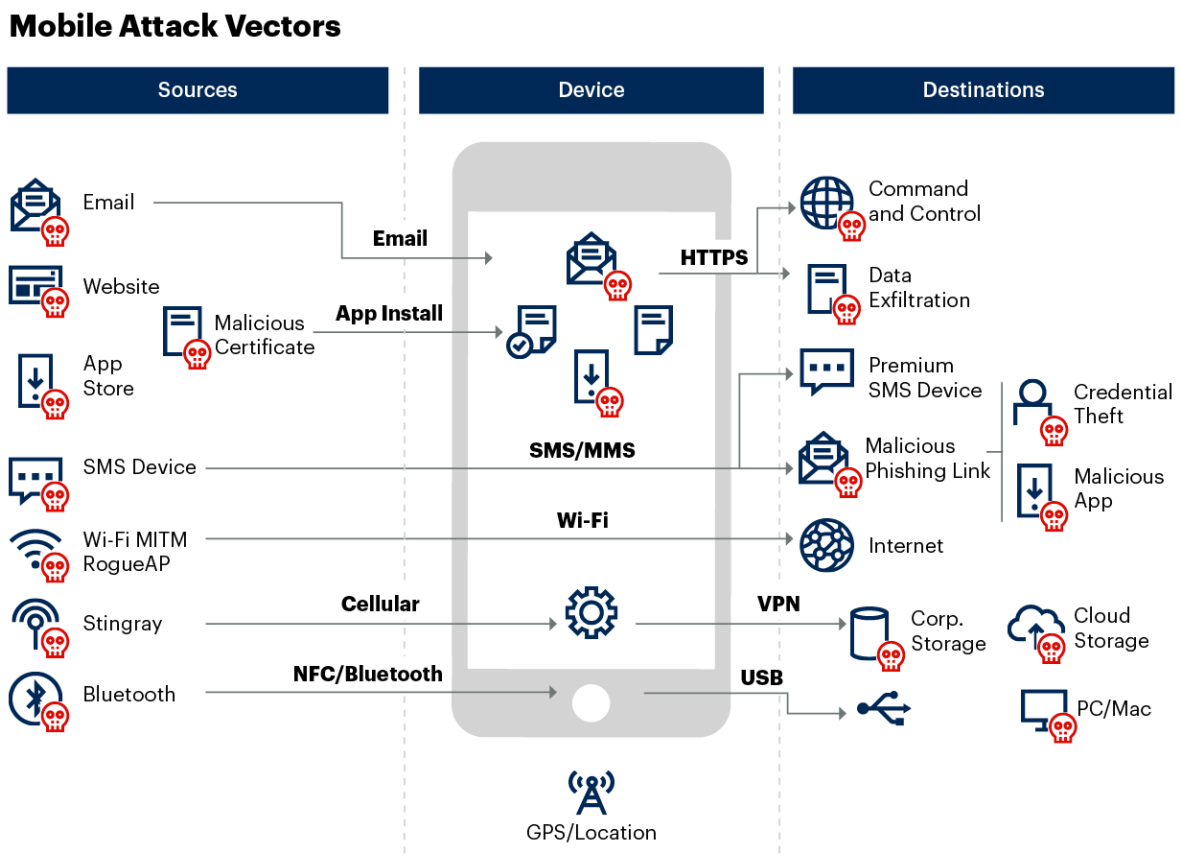
Security teams often overlook mobile devices when assessing their enterprise risk, or feel that if these devices are managed with MDM or a UEM solution that they are secure. Both approaches are incorrect and need to be changed. Think about your mobile phone and your tablet, and ask yourself the following questions:

- How many of your enterprise credentials are on them?
- What type of corporate data do you have access to or have stored on these devices?

- Are your devices really secure?
- Does your company allow unmanaged devices to connect to corporate assets?
- Are you sure there are no security gaps?

These questions form the basis of how you should think about mobile security risk, which is a departure from traditional endpoint security risk. With more and more people working from home, Gartner has seen organizations adding a “bring your own everything” (BYOE) option to their IT processes. Many of the same organizations are still struggling to implement zero trust and conditional access, which in turn greatly increases their enterprise attack surface. Figure 18 illustrates how to assess the different mobile attack vectors as you look to implement a mobile security strategy.

Figure 18: Mobile Attack Vectors



MITM = man in the middle; NFC = Near Field Communication

Source: Gartner

775183_C

Gartner

As you think about your mobile security strategy, you need to factor in a few things. The first is the need to add a mobile security component. UEM solutions are management tools, not security tools. MTD offerings are agent-based solutions that work to protect iOS and Android devices from phishing attacks, malicious mobile apps, network-based attacks and some low-level device-based attacks.

As you look to fully integrate mobility into your endpoint security strategy, vendors have begun to integrate MTD into EPP/EDR solutions to have UES solutions. MTD and UES solutions integrate with UEM solutions to fully secure and manage devices. The other option is to manage enterprise applications on personal devices integrated with MTD/UES security through MAM. This gives enterprises options for fully managed and unmanaged devices to maintain mobile security and data protection.

For more information, see Advance and Improve Your Mobile Security Strategy.

Identify and Remediate Device Misconfiguration

EPP/EDR vendors are starting to include capabilities that can alert endpoint security teams to misconfiguration on devices. This capability offers a “second set of eyes” on device configuration and provides the endpoint security team with a way to remediate misconfigurations without having to involve the endpoint management team. This reduces the need for a manual hand-off for remediation and reduces the time to remediation. For organizations where multiple endpoint management tools are in use, this becomes the “single source of truth” for device configuration.

Related Research:

- Understanding the Capabilities of Modern Endpoint Protection Platforms

Setting Priorities

Gartner clients cover a wide spectrum of cybersecurity maturity and operate a range of capabilities, based on their organization’s needs. They have neither the time nor the money to follow and address all the trends and considerations recommended here. Organizations across all industries, geographies and sizes will have differing security initiatives. The trends’ many impacts range from geopolitics, to new architectural principles, to the introduction of AI — there are many potentially competing areas.

With this in mind, we advise focusing on the following priorities:

1. **Focus on supply chain challenges and directly address geopolitical risks.** Supply chains are being actively exploited as attack vectors. Sacrificing security as a result of cost-saving measures could be a big mistake in this environment of increased risks and new threats. Look to consolidation and where tools are converging to find efficiencies and enhanced capabilities.

2. **Steer toward a CSMA-driven architecture** with a focus on cloud-based security tools for data, compute hosts, networks and applications. Seek out converged capabilities that facilitate better risk prioritization using integration to provide insights and contextual information.

3. **Investigate where AI capabilities can provide opportunities** for security, and monitor for malicious uses that may not be accounted for in your protection profile. Ensure strong governance practices are in place to enforce technical security measures on internal AI tool usage to mitigate (or reduce the number of) data breaches and other incidents.

4. **Use platform engineering to establish good security practices** for application deployment. Ensure that guardrails are defined for developers to be able to work effectively and security activities are embedded within user workflows.

5. **Build from zero trust and security by design.** Ensure basic security hygiene is addressed, and make sure security is "in at the start." Organizations should place strong focus on assets that are highly exposed. Secure cloud resources, email, client endpoints, privileged user accounts, data stores, file shares and applications, as these can be easily misused or misconfigured. Attackers often identify and enumerate targets and weaknesses within these areas, which makes them common vectors for compromise. Creating visibility into, and protection within, these areas is of utmost importance.

Evidence

[1] The idea of security by design emerged from software engineering. It was later built into the OWASP Top 10 as "insecure design," and became an extension of the Ontario Privacy Commissioner's "Privacy by Design" in its white paper entitled "Privacy and Security by Design: An Enterprise Architecture Approach."

[2] See Practical Privacy — Managing Data Retention and Backups; also Data Genomics Index Report 2017, Veritas Technologies, Veritas Technologies, 2017.

[3] See:

- Data's Dark Side, Veritas Technologies.
- The State of Dark Data, Splunk.
- P. Southekal, Illuminating Dark Data In Enterprises, Forbes, 25 September 2020.
- Illuminating Dark Data: Shedding Light on Unutilized Information for Enhanced Business Insights and Decision-Making, Data Dynamics.
- Dwight Davis, AI Unleashes the Power of Unstructured Data, CIO, 9 July 2019.
- Alexis Porter, What Is Dark Data? Uncovering Vulnerable Data, BigID, 1 October 2022.

[4] Executive Order on Improving the Nation's Cybersecurity, The White House, 12 May 2021.

Note 1: Out-of-Scope Areas for This Research

Not all aspects of security and risk management can be addressed in this Planning Guide. The focus is on advising security and risk management technical professionals about security architecture and technical practices in particular. The following areas are beyond the scope of this document:

- Industry-specific security and risk management practices and technologies, such as those used for operational technology and electronic payments.
- Audit and compliance practices and technologies, as well as integrated risk management platforms and tools.
- Business continuity and disaster recovery practices and technologies. For more information on these topics, see 2023 Planning Guide for IT Operations and Cloud Management.

Document Revision History

2023 Planning Guide for Security - 10 October 2022

2022 Planning Guide for Security and Risk Management - 11 October 2021

2021 Planning Guide for Security and Risk Management - 9 October 2020

2020 Planning Guide for Security and Risk Management - 7 October 2019

2019 Planning Guide for Security and Risk Management - 5 October 2018

2018 Planning Guide for Security and Risk Management - 29 September 2017

2017 Planning Guide for Security and Risk Management - 13 October 2016

2016 Planning Guide for Security and Risk Management - 2 October 2015

2015 Planning Guide for Security and Risk Management - 2 October 2014

2014 Planning Guide for Security and Risk Management - 3 October 2013

2013 Planning Guide: Security and Risk Management - 1 November 2012

2012 Planning Guide: Security and Risk Management - 1 November 2011

Recommended by the Authors

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

Guide to Network Security Concepts

Guide to Data Security Concepts

Guide to Cloud Security Concepts

Guide to Application Security Concepts

Guide to Infrastructure Security Concepts

Guide to Endpoint Security Concepts
