Cybersecurity Tech Radar

Tracking innovations for efficient, agile and smart security

2022 edition

Foreword

Zeina Zakhour

Global Chief Technical Officer, Digital Security, Atos

The only constant in our cybersecurity industry is change, leaving organizations with a myriad of emerging cybersecurity technological trends that can secure their digital transformational journey and thwart looming cyberthreats. However, innovation in cybersecurity is not only focused on improving the security of the digital environments, but also to provide an agile architectural blueprint adapted to the increasingly distributed, decentralized and complex organizational environment.

Those challenges are heightened by the cybercriminals' speed of innovation. Cybercriminals and state-sponsored actors keep innovating at a fast rate, leveraging new technologies to steal data, commit fraud and extort money. Now, not only do they try to paralyze critical national infrastructures, but also local and regional authorities, which realize they have become a target. Nobody is exempt from being attacked.

Concepts like the cybersecurity mesh are presenting a modern conceptual approach to security architecture. Emerging trends such as the metaverse change the creation, use and consumption of digital services, and raise new concerns and challenges in terms of security. When identity is the new perimeter and data the new oil, solutions such as Privacy Enhancing Cryptography (PEC), applied to concrete use cases protect data in use.

To top it all, artificial intelligence is infused to all cybersecurity areas. Deep learning and machine learning are already in use, but AI use cases and usability in the cybersecurity field goes beyond. Cognitive AI (CAI) and frugal AI are a few examples of emerging trends that will shape the evolution of cybersecurity.

Consequently, in order to help organizations keep an eye on the latest cybersecurity tech trends and identify the security technologies that can help them address cyberthreats efficiently, we created the Atos Cybersecurity Tech Radar.

With this yearly updated radar, organizations can keep abreast of the emerging cybersecurity innovations, and adopt an agile cybersecurity strategy that can adapt to the changing digital environments.

Our Atos security experts are tracking more than 150 cybersecurity technological trends that are shaping and transforming the industry as we speak. We built our radar around eight major cybersecurity domains, because we believe those are the most critical for the end-to-end management of your security posture and security of your digital transformation.

- Advanced Detection & Response
- Cyber Incident Response
- Identity & Access Management
- Endpoint and Mobile Security
- Network Security
- Application Security
- Cloud Security
- Data Security

Let us take a few figures

74% of companies experienced a security incident in 2021. (Security Leaders Research Report, Vectra)

79% of organizations suffered an identity-related breach in the last two years. (Identity Defined Secury Alliance)

64% increase in the costs of cybercrimes, whereas those cybercrimes only grew by 7% in volume (Internet Crime Report 2021, FBI)

61% of all SMBs have reported at least one cyber-attack during the previous year. (Verizon)

For each cybersecurity domain, we have grouped the cybersecurity technological trends in terms of speed of adoption:

- Zero to two years: Mature technologies are either already adopted by most organizations or will be in the next two years In other words, these technologies have become an integral part of the security strategies of most companies.
- Two to five years: Proven technologies are usually adopted in the next two to five years cycle as organizations improve in maturity.
- Five years and above: emerging trends will be adopted by the mainstream after approximatively five years or more. Still, organizations with a mature cybersecurity level can adopt such emerging trends earlier.

For each technology trend captured in our radar, we have worked on:

- The main business use cases it addresses.
- The benefits it brings with a focus, when applicable, on the specific market verticals.
- The main challenges to adoption that organizations must take into consideration when deploying any of those cybersecurity technology trends.

Cybersecurity innovation is a key contributor to the success of the digital revolution as we know it today. Undoubtedly, it will continue to be a key foundation for safe and secure adoption of future technology trends such as quantum, edge and swarm computing, ethical AI and immersive experience.

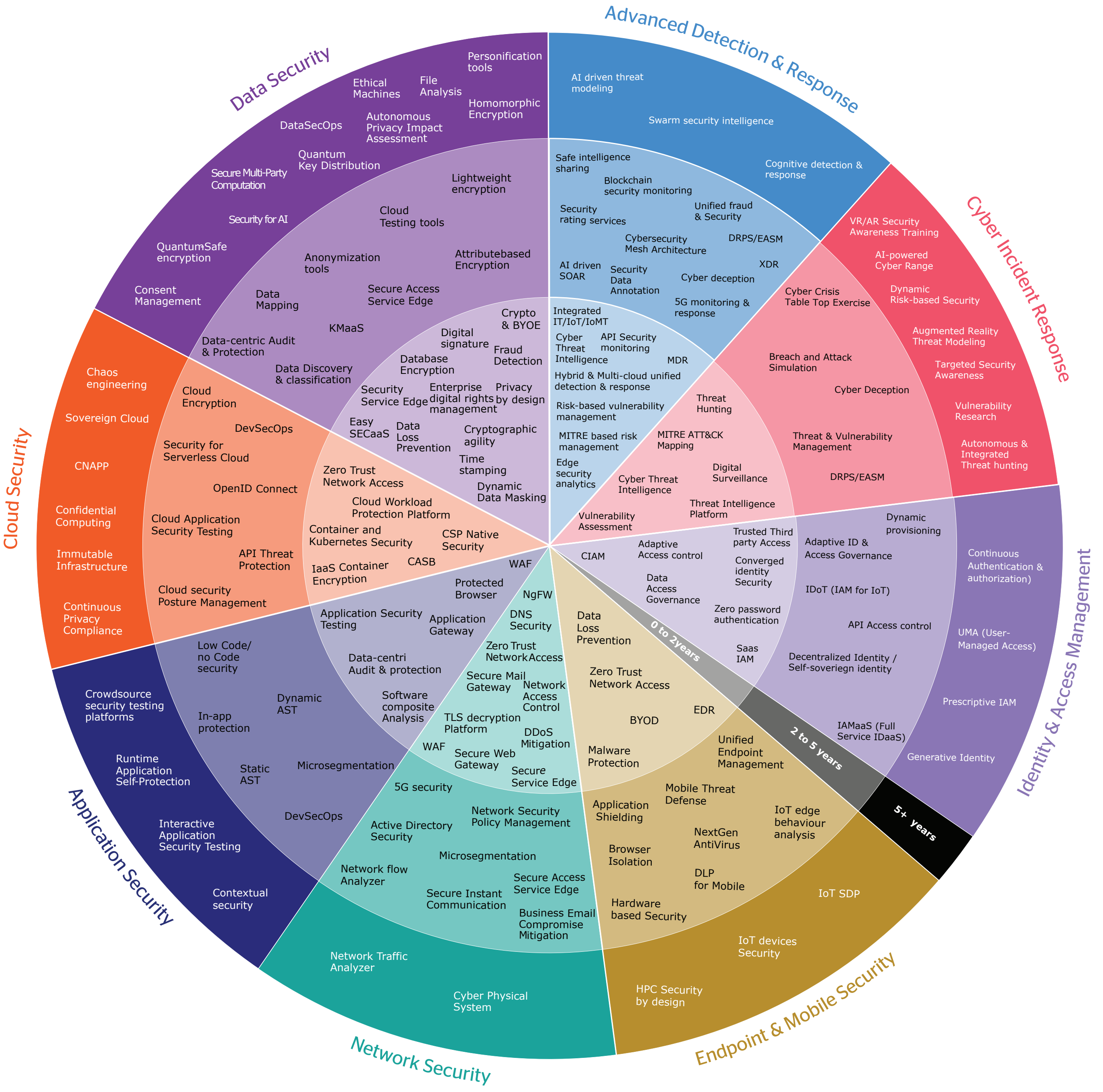
Our Cyber Tech Radar aims to help you navigate the breadth of cybersecurity technologies and support you in refining the cybersecurity strategy of your organization. To stay informed about the latest cybersecurity news and updates to the radar, follow: https://www.linkedin.com/showcase/atos-digital-security/

Contributors

Aleksander Pawlicki, Allen Moffett, Amalia Lin, Ana Bura, Andrei Chipaila, Andrei Dumbrava, Angel Polamaro, Boubacar Camara, Christian Radu Cleiton Lenkiu, Dan Schaupner, Dragos Pelian-Popa, Ernesto Parodi, Farah Rigal, Gabriel Priceputu, Gabriela Gorzycka, Geert Fieremans, Ivana Getia, Laurence Begou, Lia Predut, Marc Llanes, Marcin Krysinski, Marco Gruber, Marcus Lahm, Mihai Belu, Mircea Avram, Mohan Ayare, Nitin Kulkarni, Philippe Bodden, Raul Salagean, Reli Arras, Thierry Winter, Vali Pop, Vasco Gomes, Vinod Vasudevan, Wojciech Bohatyrewicz, Zeina Zakhour.

The Cybersecurity Tech Radar

Tracking innovations for efficient, agile and smart security


Advanced Detection & Response
AI driven threat modeling
Swarm security intelligence
Cognitive detection & response
Safe intelligence sharing
Blockchain security monitoring
Security rating services
Unified fraud & Security
Cybersecurity Mesh Architecture
DRPS/EASM
AI driven SOAR
Security Data Annotation
XDR
Cyber deception
5G monitoring & response
Integrated IT/IoT/IoMT
Cyber Threat Intelligence
API Security monitoring
MDR
Hybrid & Multi-cloud unified detection & response
Risk-based vulnerability management
MITRE based risk management
Edge security analytics
Vulnerability Assessment
Cyber Incident Response
VR/AR Security Awareness Training
AI-powered Cyber Range
Dynamic Risk-based Security
Augmented Reality Threat Modeling
Targeted Security Awareness
Vulnerability Research
Autonomous & Integrated Threat hunting
Cyber Crisis Table Top Exercise
Breach and Attack Simulation
Cyber Deception
Threat & Vulnerability Management
DRPS/EASM
Threat Hunting
MITRE ATT&CK Mapping
Cyber Threat Intelligence
Digital Surveillance
Threat Intelligence Platform
Identity & Access Management
Continuous Authentication & authorization)
UMA (User-Managed Access)
Prescriptive IAM
Generative Identity
Dynamic provisioning
Adaptive ID & Access Governance
IDoT (IAM for IoT)
API Access control
Decentralized Identity / Self-soveriegn identity
IAMaaS (Full Service IDaaS)
CIAM
Adaptive Access control
Trusted Third party Access
Converged identity Security
Data Access Governance
Zero password authentication
Saas IAM
0 to 2years
2 to 5 years
5+ years
Endpoint & Mobile Security
IoT SDP
IoT devices Security
HPC Security by design
Unified Endpoint Management
Mobile Threat Defense
IoT edge behaviour analysis
Application Shielding
NextGen AntiVirus
Browser Isolation
DLP for Mobile
Hardware based Security
Data Loss Prevention
Zero Trust Network Access
BYOD
EDR
Malware Protection
Network Security
Network Traffic Analyzer
Cyber Physical System
5G security
Network Security Policy Management
Active Directory Security
Microsegmentation
Network flow Analyzer
Secure Access Service Edge
Secure Instant Communication
Business Email Compromise Mitigation
NgFW
DNS Security
Zero Trust NetworkAccess
Secure Mail Gateway
Network Access Control
TLS decryption Platform
DDoS Mitigation
WAF
Secure Web Gateway
Secure Service Edge
Application Security
Crowdsource security testing platforms
Runtime Application Self-Protection
Interactive Application Security Testing
Contextual security
Low Code/ no Code security
Dynamic AST
In-app protection
Static AST
Microsegmentation
DevSecOps
WAF
Protected Browser
Application Security Testing
Application Gateway
Data-centri Audit & protection
Software composite Analysis
Cloud Security
Chaos engineering
Sovereign Cloud
CNAPP
Confidential Computing
Immutable Infrastructure
Continuous Privacy Compliance
Cloud Encryption
DevSecOps
Security for Serverless Cloud
OpenID Connect
Cloud Application Security Testing
API Threat Protection
Cloud security Posture Management
Zero Trust Network Access
Cloud Workload Protection Platform
Container and Kubernetes Security
CSP Native Security
IaaS Container Encryption
CASB
Data Security
Personification tools
Ethical Machines
File Analysis
Homomorphic Encryption
DataSecOps
Autonomous Privacy Impact Assessment
Quantum Key Distribution
Secure Multi-Party Computation
Security for AI
QuantumSafe encryption
Consent Management
Lightweight encryption
Cloud Testing tools
Anonymization tools
Attributebased Encryption
Data Mapping
Secure Access Service Edge
KMaaS
Data-centric Audit & Protection
Data Discovery & classification
Crypto & BYOE
Digital signature
Fraud Detection
Database Encryption
Security Service Edge
Enterprise digital rights management
Privacy by design
Easy SECaaS
Data Loss Prevention
Cryptographic agility
Time stamping
Dynamic Data Masking

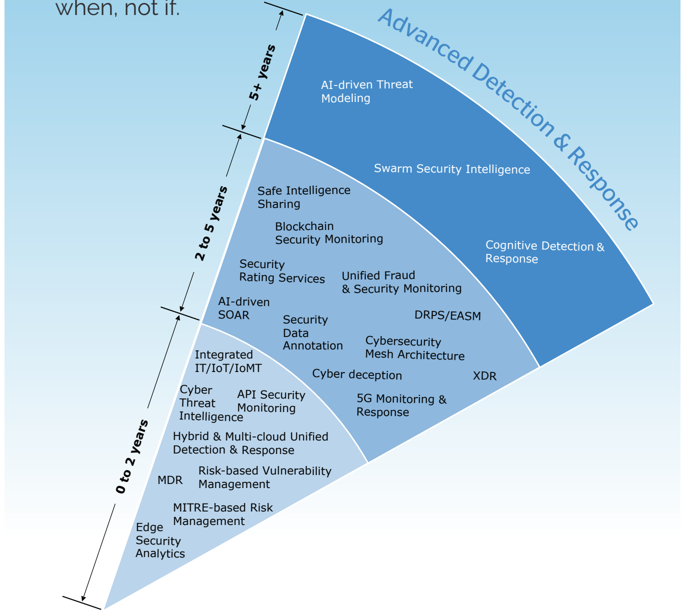
Advanced detection & response (AD&R)

What is AD&R?

- AD&R is a rapid evolution of traditional detection and response measures hugely challenged by quickly changing attacker techniques, and the growing threat from APTs to the public and private sectors.
- Modern AD&R has elements in all five of the NIST cybersecurity framework functions (Identify, Protect, Detect, Respond, Recover), while classic AD&R has elements only in the last three NIST functions (Detect, Respond, Recover).

Why it matters

- The proliferation of digital enterprise has opened up many vectors for cybercriminals to attack, including network, endpoints, cloud, OT and IoT.
- Fast growth of e-crime and the advancement of attacker tooling has made it easy to launch advanced attacks. Successful evasion of preventive controls is a matter of when, not if.


Advanced Detection & Response
5+ years
2 to 5 years
0 to 2 years
AI-driven Threat Modeling
Swarm Security Intelligence
Cognitive Detection & Response
Safe Intelligence Sharing
Blockchain Security Monitoring
Security Rating Services
Unified Fraud & Security Monitoring
AI-driven SOAR
Security Data Annotation
DRPS/EASM
Cybersecurity Mesh Architecture
Cyber deception
XDR
5G Monitoring & Response
Integrated IT/IoT/IoMT
Cyber Threat Intelligence
API Security Monitoring
Hybrid & Multi-cloud Unified Detection & Response
MDR
Risk-based Vulnerability Management
MITRE-based Risk Management
Edge Security Analytics

The Landscape

Convergence of multiple monitoring technologies into overarching platforms

It enables extended multi-vector visibility and control, including endpoint-based detection and response (EDR), network traffic analysis (NTA), cloud analytics and more. On the functional side, use case-based correlation or behavioral analysis are no longer separate functions in the SOC, but rather one of multiple ways a single platform or service mines every dataset to capture maximum indicators of threat.

AI is currently being proven on single modules and functions before envisaging a full AI-driven autonomous/cognitive monitoring and response.

AI will also bring intuitiveness to the way the SOC platform is interacted with by the analysts, threat hunters and security managers. AI is expected to enable cognitive detection and response using developments in Artificial General Intelligence before the end of this decade.

The future has much more to bring, mainly in the area of:

Data analytics tooling "commoditization": Expertise development in this area will continue to enable situational awareness far beyond the one offered by legacy logic-based rules and signatures combined with low volume and not scalable monitoring solutions.
Growing maturity in Red Teaming, threat simulation programs, use of deception technologies, threat hunting: All combined, will further drive AD&R development with the end goal of staying in front of the attackers for a change.

Key Figures

36%

of those technologies are either already adopted by most organizations or will be in the next two years.

50%

of those technologies are expected to be adopted in the next two to five-year cycle.

14%

of those technologies are transformational and widespread adoption will take over five years.

Zoom on
Managed Detection & Response (MDR)

Traditional detection and response measures are now hugely challenged by the fast changing attacker techniques

Managed Extended Detection & Response combines technology and skills to deliver

- Advanced threat detection
- Deep threat analytics
- Global threat intelligence
- Enhanced threat hunting
- Faster incident analysis
- Collaborative incident response on a 24x7 basis

In other words, MxDR provides:

- Detection of deep attacks using AI/ML vs. using only rules
- Response to threats vs. only alerting from traditional MSSPs
- Collects data from all vectors – security devices, users, server endpoints, cloud, OT/IIoT that enable better detection (e.g. logs, alerts, flows, changes in device configuration and vulnerabilities, etc.)

Key Features

- Threat Intelligence: Going beyond the generic data of threat intelligence providers, a mature MDR service converts threat intelligence data into actionable tasks, anticipating what could happen and how to stop it if it happens.
- Threat Hunting: AI models are applied on security, user and IT data to enable the detection of unknown and hidden threats.
- Security Monitoring: The application of rules to logs and security events to detect known attacks. MDR offering has a SIEM module for detecting known threats, policy and compliance violations.
- Incident Analysis: This MDR module triages alerts to focus on the most relevant threats and then investigating them to identify potential impact to assets and spread of attack. The alerts are investigated for who, what, when, and how to determine the extent of the impact.
- Threat Containment: It provides automated containment of threats and prevents threats from becoming incidents or breaches.
- Response Orchestration: It enables carrying out rapid, coordinated activities for containment, remediation and recovery. It provides the basis for collaboration between key teams responding to an attack, including end user teams and MDR specialized responders.

Benefits of the Technology

- Deep detection of threats coming from any vector
- Minimize response tasks with automation
- Increased threat containment speed, limiting threats from leading to incidents or breaches
- Get specialized skillsets for incident/ breach response
- Centralized visibility across hybrid IT environment
- Better TCO using a combination of technologies, skillsets

Challenges to Adoption

Cost could be sometimes a challenge to adoption, although MDR is being widely adopted.

Market Verticals

- All verticals

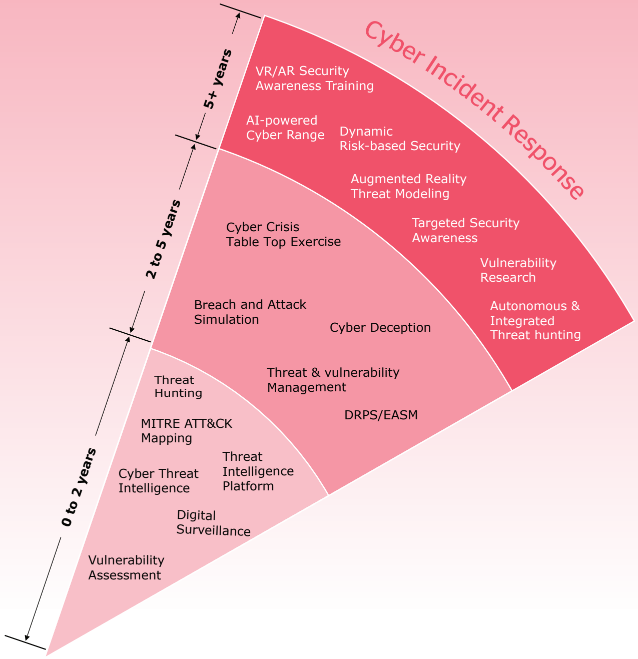
Cyber incident response

What is cyber incident response?

- Cyber incident response complements the advanced detection & response domain with a focus on technologies, processes and frameworks aimed at discovering, eradicating and recovering from cyberattacks and exploited vulnerabilities within an organization.
- It covers the key functions and operations expected by CERT/CSIRT teams and is increasingly important to a mature cybersecurity strategy in many organizations.

Why it matters

- Identifying technological trends will help outline and prescribe threat discovery, attack mapping, threat modeling, and threat and vulnerability management.


Cyber Incident Response
5+ years
2 to 5 years
0 to 2 years
VR/AR Security Awareness Training
AI-powered Cyber Range
Dynamic Risk-based Security
Augmented Reality Threat Modeling
Targeted Security Awareness
Vulnerability Research
Autonomous & Integrated Threat hunting
Cyber Crisis Table Top Exercise
Breach and Attack Simulation
Cyber Deception
Threat & vulnerability Management
DRPS/EASM
Threat Hunting
MITRE ATT&CK Mapping
Cyber Threat Intelligence
Threat Intelligence Platform
Digital Surveillance
Vulnerability Assessment

The Landscape

Adversary profiling with MITRE ATT&CK
Organizations are increasingly adopting the MITRE ATT&CK framework and moving to a threat informed defense strategy. Such a framework will help organizations understand the behavior and tactics of threat actors and proactively tailor their protection strategies.

Threat hunting for proactive protection
With digital transformation going full speed and a continuously expanding attack surface, the old school approach of "building the defenses and waiting in the trenches" is no longer sustainable. Neither is the static approach of waiting for the published IoCs and running unitary searches. Organizations will have to adopt threat hunting (especially red teaming activities) to proactively identify vulnerabilities in their environments before they are exploited by threat actors. With them, organizations will get better insight on the weaknesses in their environments and will be able to proactively mitigate them.

Automated threat modeling provides the means to build secure systems in a repeatable and methodical approach with little to no human intervention, and greatly decreases the success chances of an attack. It also reduces the time and human effort needed for the implementation. The challenge is that it relies heavily on a very good understanding of the business infrastructure and processes. Any error or missing information can have a negative impact or even lead to improper security response. Thus, risks must be identified first, by leveraging the SOC detection, threat intelligence sharing and cyber deception tools.

Key Figures

33%
of those technologies are either already adopted by most organizations or will be in the next two years.

28%
of those technologies are expected to be adopted in the next two to five-year cycle.

39%
of those technologies are transformational and widespread adoption will take over five years.

Zoom on
External Attack Surface Management (EASM)

This trend can be seen as a push from the market for consolidating together a set of similar outcomes, most of which are already in use. Existing threat intelligence (TI) services, digital risk protection (DRP), scoring provide an element of the external estate exposed. Other existing technical services, like web, network and cloud penetration testing / red teaming services operate discovery, external reconnaissance and other steps with the same kind of output. It is also questioned if the pure players in this trend / technology all observe strict legal diligence before offering.

Organizations usually seek cyber incident response providers to augment their internal capabilities by subscribing to incident response retainer services.

Key Features

These solutions rely on external integrations with other service providers such as Shodan, DomainTools, internet service providers and internet registrars to acquire data. Once acquired, it is correlated, analyzed and enriched to provide insight to organizations regarding their public-facing assets and their exposure.

The insights provided include:

- Attack surface management: Identify all the attack-exposed assets
- Prioritization of external-facing attack vectors: With a continuous and updated view of current attack vectors existing in the environment
- Asset mapping
- Monitoring subsidiary risk (visibility of the security posture of subsidiaries and organizations that are evaluated for merging or acquiring)
- Global bot network (attacker-like reconnaissance techniques)
- Multi-vector attack simulator (identification of risks per asset and discovery of potential attack vectors)
- Easy deployment model

Benefits of the Technology

EASM is a holistic approach to understand how threat actors are viewing your organization when compared to penetration tests or red teaming, which have a more technical but narrow-minded approach.

The holistic approach enabled by EASM covers:

- Asset discovery of unmanaged and unknown devices, cloud-based assets, third-party components and other client environments
- Deep risk analysis like software misconfiguration, authentication and encryption weaknesses, sensitive data exposure
- Business context of assets and their relationship to customer environment
- Critical risk prioritization increasing operational efficiency, adding risk scoring system based on attacker priorities such as discoverability, exploitation complexity and potential impact
- Cloud-based efficiency, since no integration is needed and it's 100% external
- Autonomous and continuous analysis that is neither manual nor periodic
- Besides providing a comprehensive and complete inventory of internet-exposed assets, the solution may also provide remediation guidance of penetrable vulnerabilities, security gaps or misconfigurations

Challenges to Adoption

- Integrating the solution with the incident response process.
- Generates a large amount of alerts which organizations need to act upon in order to get value from the technology and reduce their visible external attack surface.

Market Verticals

EASM applies to all markets as long as the organizations own internet-facing assets and that the IT infrastructure is involved.

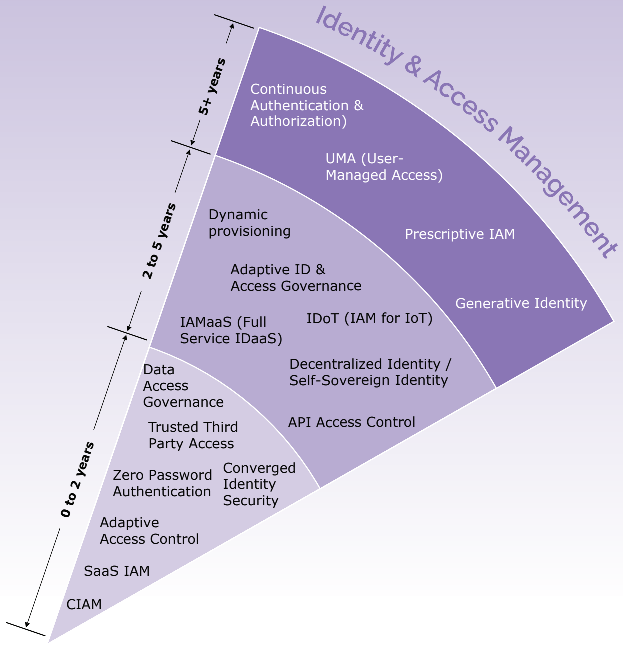
Identity & access management (IAM)

What is IAM?

- A set of business process and tools for providing access to the right resources at the right time for the right reasons.
- Providing visibility into who has access to what and why, along with how the access is being used.
- IAM is not just about protecting organizations against main threats such as insider threats and credential theft, it is also about business enablement and improving the end-user experience.

Why it matters

- According to a survey from The Identity Defined Security Alliance, 94% of organizations have had an identity-related breach, which 99% believe could have been prevented.



Identity & Access Management
5+ years
2 to 5 years
0 to 2 years
Continuous Authentication & Authorization)
UMA (User-Managed Access)
Prescriptive IAM
Generative Identity
Dynamic provisioning
Adaptive ID & Access Governance
IAMaaS (Full Service IDaaS)
IDoT (IAM for IoT)
Decentralized Identity / Self-Sovereign Identity
API Access Control
Data Access Governance
Trusted Third Party Access
Zero Password Authentication
Converged Identity Security
Adaptive Access Control
SaaS IAM
CIAM

The Landscape

The move to the cloud and "as a service models"

This will continue to evolve as tools become cloud-native and are true SaaS tools.

The use of machine learning and behavioral analytics

for a more dynamic or adaptive way of working where decisions are made in near real time.

Extending the role of identities and access beyond people and traditional roles and entitlements

Identities are no longer limited to carbon-based units and are taking the form of devices (e.g. IoT) and applications (e.g. RPA).

Convergence and Cybersecurity Mesh Architecture

Defined by Gartner for centralized security operations, this architecture brings together a flexible architecture to encompass major technologies including SIEM, XDR, Identity and ZTNA to enable better integration and harmonizing output between different products in the detection and response space. It can also drive central intelligence, analytics and policy across different technologies, leading to better ROI.

Key Figures

41%

of those technologies are either already adopted by most organizations or will be in the next two years.

35%

of those technologies are expected to be adopted in the next two to five-year cycle.

24%

of those technologies are transformational and widespread adoption will take over five years.

Zoom on
Customer Identity and Access Management (CIAM)

As identity has become the new perimeter, IAM is needed to protect against cyberthreats, but also to improve end-user experience

Customer identity and access management (CIAM) manages the authentication and authorization for customer identities. CIAM is necessary for public-facing applications that require users to register identities for access to applications that provide data, goods or services.

Key Features

- Self-service for registration
- ID proofing
- Privacy and consent management
- Fraud detection
- Profile generation and management
- Authentication and authorization into applications
- Identity repositories, reporting and analytics
- APIs and SDKs for mobile applications
- Social identity registration and login

Use cases

- Online storefronts purchase products
- Government websites used to take advantage of services such as renewing a driver's license or collecting unemployment benefits.

Challenges to Adoption

- Most organizations have something in place today to interact with their customers, and replacing something that is "working" can be a difficult decision.

Benefits of the Technology

Improved user experience

- The user experience for registration and authentication can be designed with little or no code using graphical orchestration features
- Provides flexible and adaptive authentication methods to require the right level of authentication for the action the user is requesting, based on the real-time risk associated with the action. For example, a user may be able to browse a catalog with a very simple authentication, but making a purchase may require a stronger authentication before spending the user's money.
- Supports the linking of social media accounts, such as Facebook or LinkedIn, to allow the use of these existing authentication mechanisms for access to lower risk services as a convenience for the user.

Improved security

- Provides a secure way for consumers to register with an organization, including ID proofing as part of the process, so the organization can have confidence the person registering is who they say they are.
- Analytics of behavior and input from other data sources can detect fraudulent activities

Compliance

- Supports privacy and consent management to protect the consumer's personal information, including features such as the right to be forgotten for compliance with regulations such as GDPR

Reduced operational costs

- Since the necessary features are provided out of the box and can be implemented with little or no code (except in the most complex scenarios), the system is simpler and less costly to support and maintain than a heavily customized or bespoke solution

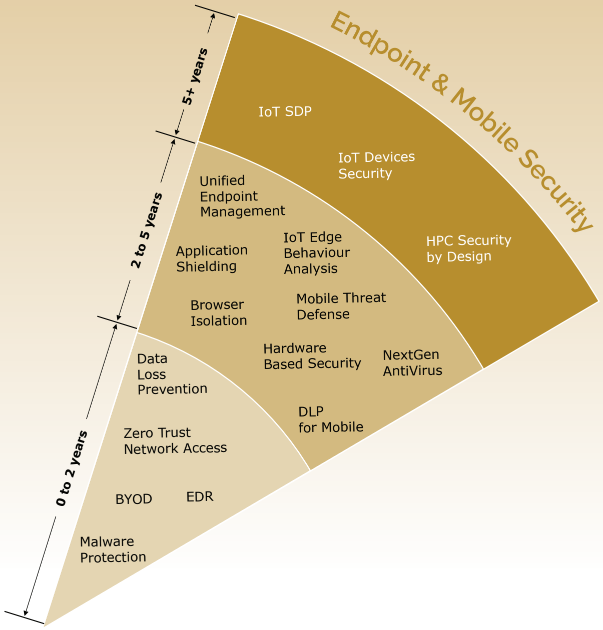
Endpoint & mobile security

What is endpoint and mobile security?

- It combines all solutions, practices and methodologies adopted to protect corporate assets accessed remotely via wireless devices such as laptops, tablets, mobiles, smart watches, etc.
- AI and edge computing are expected to challenge most endpoint implementations and architectures with the switch to an architecture where:
  - “client components” become more intelligent and autonomous to react faster to threats.
  - the “central control component” moves to the edge.

Why it matters

- Endpoint and mobile security plays a major role in the overall security ecosystem, as each remote device accessing the corporate network is a potential security hazard and entry point for attacks. The risk is getting worse with the rising deployment of edge and IoT.



The Landscape

Improved visibility

You cannot protect what you do not see. A proactive approach to visibility will be a key requirement for any endpoint security solution, especially as the bring your own device (BYOD) culture expands and IoT devices are fully adopted by organizations.

Emerging technologies are breaking the silos to improve visibility and security, such as XDR, Zero Trust Network Access, new Unified Endpoint Management solutions and other BYOD solutions.

Security by design

The more data management is moving towards the edge, the more there is a need to better protect the data itself.

Data must be protected wherever it sits, and whenever it moves, with proper encryption, access control and any other suitable controls according to the data status (processing, storage, transport, etc.). Many technologies are evolving today to meet that need, such as DLP technologies, hardware-based security, digital rights management and application shielding.

Intelligent protection

AI is especially useful in endpoint security, as it helps improve detection capabilities and automates response to threats in real time, reducing the time span of the attackers’ cyber kill chain.

Examples of AI applied to endpoint security are present in new developments for next-gen antivirus solutions, endpoint detection and response, API threat protection systems or new malware protection technologies based on machine learning techniques

Key Figures

31%

of those technologies are either already adopted by most organizations or will be in the next two years.

50%

of those technologies are expected to be adopted in the next two to five-year cycle.

19%

of those technologies are transformational and widespread adoption will take over five years.

Zoom on
Mobile Threat Defense

Mobile threat defense (MTD) solutions protect organizations from threats on iOS and Android mobile devices. In particular, they protect against known vulnerabilities and avenues of attack.

Each remote device accessing the corporate network is a potential security hazard and entry point for attacks.

Key Features

Protection against the below known vulnerabilities or avenues of attack:

- Signature-based malware
- Mobile application vetting
- Network-based risks (MITM, host certificate hijacking, SSLStrip, TLS downgrade)
- Vulnerability assessment of applications and OS versions
- OS-level vulnerabilities caused by user actions such as rooting and jailbreaking

MTD solutions are key in numerous use cases, including the following:

- Counter threats
- Content filtering
- Mobile phishing
- Mobile endpoint detection response (EDR)
- App vetting
- Device vulnerability management
- Protect from malicious URLs without having to perform traffic redirection

Benefits of the Technology

- MTD solutions have reached a level of maturity that makes them suitable for wide enterprise adoption.
- In addition to innovation to counter the evolving mobile malware, innovation also focuses on improving the MTD user experience on the device — for example, when providing phishing protection.
- Certain MTD tools integrate with Microsoft Outlook, Microsoft Office 365 suite, as well as other popular enterprise suites and managed enterprise apps to provide ZTNA functionality on unmanaged devices.
- MTD solutions can identify apps that conflict with an enterprise's security and privacy policies, even when these applications are not malicious.

Challenges to Adoption

- MTD adoption has been slower than predictions, as the industry has waited for highly visible or publicized mobile breaches that did not occur. As mobile security issues have rarely led to spectacular breaches, enterprises adopting MTD sometimes have difficulty in identifying positive impact.
- Customers are focused on consolidating their cybersecurity assets. Therefore sometimes overlook MTD and prefer to go with Unified Endpoint Management Solutions that cover some mobile security use cases.
- Poorly implemented MTD could get in the user's way or consume too many resources (e.g. battery)

Market Verticals

- Financial Services and Insurance
- Healthcare
- Government
- Energy
- Enterprises with high security requirements

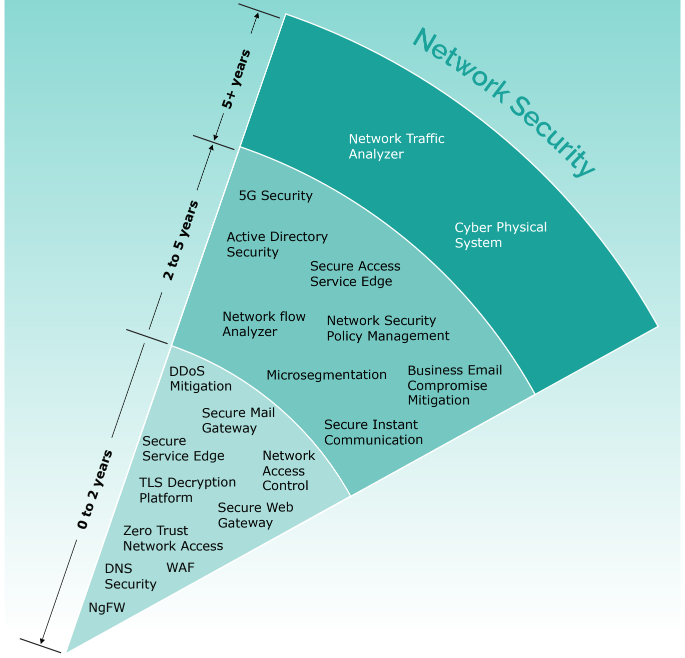
Network security

What is network security?

- The maintenance of authorized access to internal and external connectivity between systems,
- Protection against denial-of-service to network functions that support interconnectivity,
- Seamlessly secure hybrid and complex network architectures where traditional network boundaries are eroding with cloud acceleration, edge integration and 5G adoption.

Why it matters

- Most network security controls are a combination of hardware appliances purpose-built for high throughput of traffic and advanced software that are essential to identify malicious activity and respond in near real time.



The Landscape

On the road to zero trust

With corporate networks, infrastructures, applications and data moving quickly beyond traditional on-premises profiles (e.g. to the cloud, edge, mobile devices, value-chain partners, etc.), the increasing adoption of zero trust architectures and solutions to secure networks is expected.

The end of traditional security perimeters

All traditional perimeter controls are being redefined, consolidated into as-a-service model. SASE services are transforming the consolidation of network and security capabilities with functional consolidation and virtualization of core capabilities.

The uptake of preventive technologies

Preventive network security technologies that are highly agile and compatible with a wide spectrum of enterprise IT infrastructures will have an increasing adoption rate. Innovation will bring together the SASE and XDR worlds to integrate threat anticipation in the fabric of network security.

Key Figures

50%

of those technologies are either already adopted by most organizations or will be in the next two years.

40%

of those technologies are expected to be adopted in the next two to five-year cycle.

10%

of those technologies are transformational and widespread adoption will take over five years.

Zoom on
Secure Access Service Edge (SASE)

Secure Access Service Edge (SASE) combines the functionality of an SD-WAN with network security technologies like firewall, secure web gateways, cloud access security broker (CASB) and network access identity.

Zero trust implies that no user or device — whether inside or outside the network — will be trusted.

Key Features

- Increased data protection by preventing unauthorized access to sensitive data regardless where the endpoint or data is based
- Flexibility because of its cloud based infrastructure
- Reduced complexity by unifying or at least minimizing the number of separate security products

Benefits of the Technology

Bringing several technologies under one umbrella into one solution will reduce the amount of management environments and required resources, compared to the resources required for today's heterogenous best-of-breed approach.

Challenges to Adoption

- Technical and organizational challenges that come with the migration of single products into one single SASE solution
- Updating the investments in security and network technologies to move to SASE solution

Market Verticals

All verticals

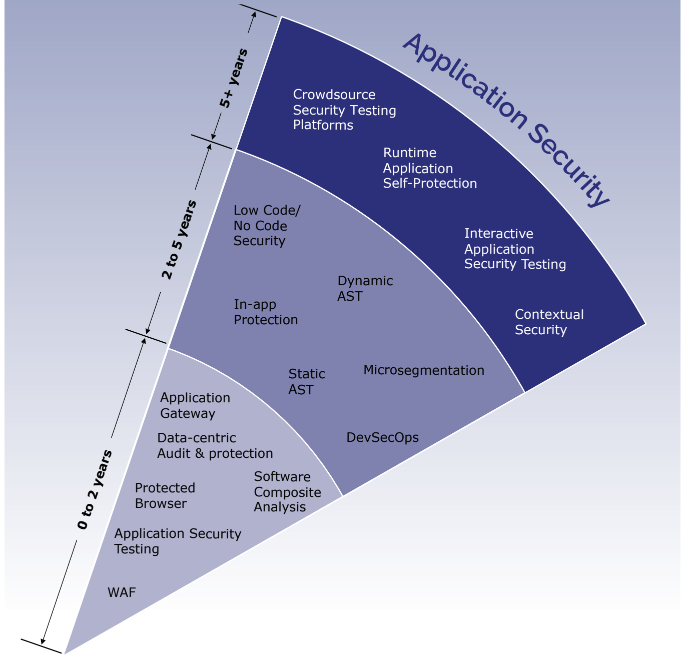
Application security

What is application security?

- Critical web applications have been subject for some time to an overall process of tracking, reporting and fixing security flaws at application level, inspired by initiatives like OWASP Top 10.
- Application security is a very critical area to be incorporated in a complete cybersecurity strategy, so that the vast amount of application errors are reported on time, thus reducing the software application attack surface.

Why it matters

- Exploiting vulnerabilities in the application layer is fertile ground for attackers. 90% of security incidents are launched by exploiting the software design and/or the code of a software application.



Application Security
5+ years
2 to 5 years
0 to 2 years
Crowdsource Security Testing Platforms
Runtime Application Self-Protection
Interactive Application Security Testing
Contextual Security
Low Code/ No Code Security
Dynamic AST
In-app Protection
Static AST
Microsegmentation
Application Gateway
Data-centric Audit & protection
DevSecOps
Software Composite Analysis
Protected Browser
Application Security Testing
WAF

The Landscape

Heavy influence of the most recent evolutions in application security on tooling to be used in the context of

- Integrated ALM with DevOps and DevSecOps
- Cloudification combined with containerization and automation
- Orientation toward API and microservices, with the end goal of staying in front of the attackers for a change

Supply chain attacks are a key driver in the integration of application security in the entire application lifecycle

Evolutions in the application field require the various types of application security testing (static, dynamic, interactive, mobile, etc.) to be embedded into the application lifecycle management (ALM) tooling in their environments, and will be able to proactively mitigate them.

Emerging new trends transforming application security

Modern applications and the Agile development lifecycle are among the driving forces in the fundamental changes and emerging application security trends.

Crowdsourced security testing, no-code security and cloud-native application security are just a few of the fast adopted new tech trends in application security.

Key Figures

37.5%

of those technologies are either already adopted by most organizations or will be in the next two years.

37.5%

of those technologies are expected to be adopted in the next two to five-year cycle.

25%

of those technologies are transformational and widespread adoption will take over five years.

Zoom on
Crowdsourced security testing platforms

A crowdsourced security platform makes use of a group of people registered in their platform to test an application for vulnerabilities. The number of people can range from less than a dozen to several hundred testing concurrently. The skillset of the crowd involved can also vary heavily. These platforms offer incentives to high skilled people or high performers to stay in their platform.

> Application security is a very critical area to be incorporated in a complete cybersecurity strategy so that the vast amount of application errors are reported on time.

Key Features

Crowdsourcing is best suited for B2C-type software applications like web applications, mobile applications, firmware in smart devices, smart cars, etc. Many large corporations are running crowdsourced programs on an ongoing basis to continuously improve the security of their applications:

- Bug bounty programs
- Vulnerability disclosure programs
- Responsible disclosure programs

Benefits of the Technology

- Eliminate overhead and maximize risk reduction
- Provide open-ended campaigns with no time limit, leading to equal opportunity for anyone to contribute
- Ensure watchful eyes over all versions of the software if the incentives are high enough
- Identify critical and zero-day vulnerabilities faster, simply due to sheer size and diversity of crowd skillset
- Crowdsourced penetration testing often yields exploitable vulnerabilities with proof of exploit, enabling organizations to stop chasing phantom vulnerabilities

Challenges to Adoption

- The mainstream adoption of this technology, which we believe will occur within 5 to 10 years, will depend on the willingness of organizations to open their B2C applications to crowdsourced security testing platforms. This relies on their maturity of adoption of the Agile and DevOps models that help accelerate the pace of software release, moving towards continuous delivery.

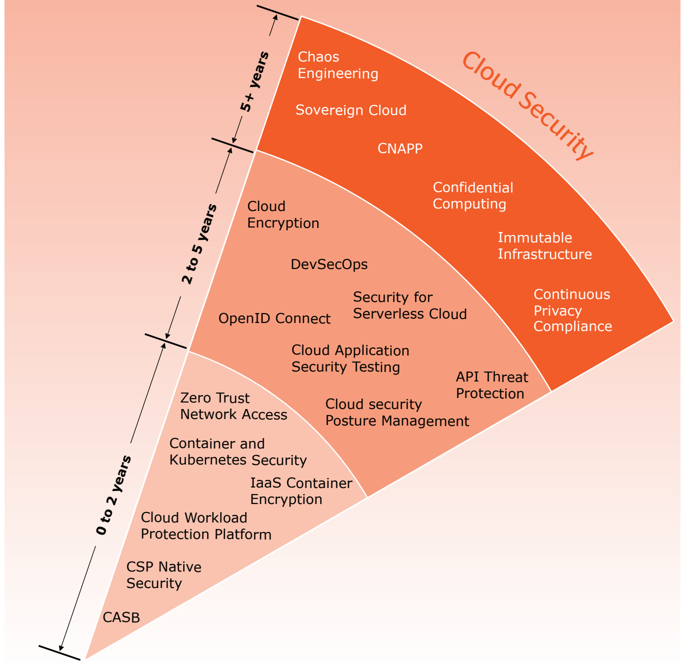
Cloud security

What is cloud security?

- Solutions vary from simple usage monitoring and security exposure rating to very specific enterprise security policy enforcement.

Why it matters

- As cloud adoption and multi-cloud deployments spread exponentially, organizations are faced with unmanaged security risks and data exposure.
- Organizations will need solutions for a single pane of glass security operation in their cloud and hybrid environment.
- Compliance with data privacy regulations and other legal rules will also require better cloud security testing and continuous compliance monitoring/control.


Cloud Security
5+ years
2 to 5 years
0 to 2 years
Chaos Engineering
Sovereign Cloud
CNAPP
Confidential Computing
Immutable Infrastructure
Continuous Privacy Compliance
Cloud Encryption
DevSecOps
Security for Serverless Cloud
OpenID Connect
Cloud Application Security Testing
API Threat Protection
Cloud security Posture Management
Zero Trust Network Access
Container and Kubernetes Security
IaaS Container Encryption
Cloud Workload Protection Platform
CSP Native Security
CASB

The Landscape

Losing track of cloud services and cloud native applications

Some employees inside the organization may not conform to the organization's security requirements.

The growth of shadow IT

is a security vulnerability which may lead to data leakage or data breaches. The result? loss of trust of customers, legal complications, and even loss of quality in the product offering through an employee run-off.

Awareness is rising

due to more frequent occurrence of data breaches and the legal consequences thereof, leading to monitoring and closer management of cloud applications and growing attention to cloud legal compliance,

Customers need to classify and determine the accountability for their data

as visibility of the data classification allows appropriate security measures to be applied.

Key Figures

31.5%

of those technologies are either already adopted by most organizations or will be in the next two years.

37%

of those technologies are expected to be adopted in the next two to five-year cycle.

31.5%

of those technologies are transformational and widespread adoption will take over five years.

Zoom on

Cloud Native Application Protection Platform (CNAPP)

Cloud native applications are applications which are developed with a cloud deployment in mind. As such, they tend to integrate many of the cloud providers' native offerings, virtual machines, Kubernetes container services, and serverless functions.

Cloud native application protection platforms (CNAPPs) are an integrated set of security and compliance capabilities designed to help secure and protect these cloud-native applications from development to production runtime.

CNAPPs consolidate many previously siloed capabilities such as network micro/nano segmentation, container scanning, Infrastructure as Code (IaC) scanning, Cloud Infrastructure Entitlement Management (CIEM), Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPPs)

As cloud adoption and multi-cloud deployments spread exponentially, organizations are faced with unmanaged security risks and data exposure.

Key Features

Deploy CNAPPs to:

- Reduce the number of tools and vendors involved in the lifecycle of a cloud-native application. This reduction in tools will reduce the complexity and costs associated with developing and deploying cloud-native applications.
- Help develop secure solutions rather than secure developed solutions. CNAPPs come with scanning capabilities that seamlessly integrate into development's IDE platforms, CI/CD pipelines and security test tooling. Shift the security scanning to development and rely less on runtime protection, which is well-suited for container as-a-service and serverless function environments.
- Visualize and control security gaps. The micro-segmentation inherent to cloud-native applications opens a multitude of attack vectors. CNAPPs allow security departments to understand attack path analysis based on relationships — identities, roles, permissions, networking and infrastructure configuration.
- Consistent management and continuous compliance scanning from a single control point for organizations that have a multi-cloud strategy.

Benefits of the Technology

- Better visibility, monitoring capabilities, and control over total cost, since CNAPPs consolidate an ever-growing, disparate number of independent security testing and protection tools.
- Using a CNAPP offering will improve developer and security professional effectiveness and reduce complexity and costs while maintaining development agility.

Challenges to Adoption

- As new categories arise, they are getting consumed into CNAPP.
    - o CIEM and IaC scanning are two recent examples.
- Reorganization may be necessary, as Dev, Sec and Ops may have already made siloed purchases of application security testing tooling.
- CSPs are continually growing their native toolset – features and capabilities may be offered natively.

Market Verticals

All verticals

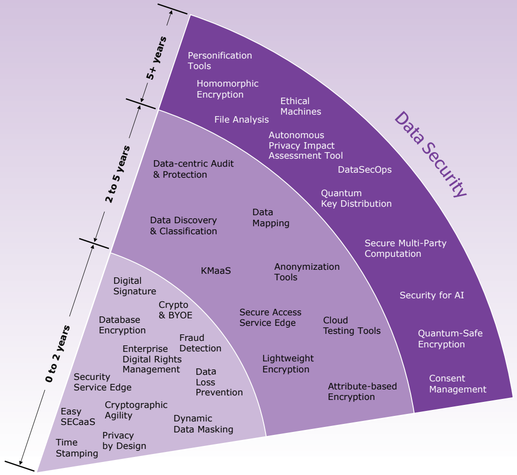
Data security

What is data security?

- Data security includes the process and associated tools that protect sensitive information assets, be they in transit, at rest or in use (while processing).
- Core element of data security goes now beyond the CIA (....) triad to also include effective access control and privacy protection mechanisms
- Data security encompasses very diverse use cases, from classic networks based on perimeter security to cloud-based environments and IoT.
- Since there is no single-pane-of-glass solution for data security, this creates the challenge of orchestrating policies and controls across all tools and consoles for data security, IAM, etc.

Why it matters

- As data becomes pervasive, data security is vital to protect sensitive data, protect the business and ensure compliance with data protection and privacy regulations
- Adaptive controls that evolve based on the data lifecycle are key to make all the other parts of your cybersecurity strategy more effective (IAM, cloud security, etc.)



The Landscape

You cannot protect what you cannot see

Rising changes to identify, discover and track data across the new decentralized and distributed digital environments. Yet, to properly protect sensitive data, organizations will need to adopt emerging technologies that improve discovery and classification of structured and unstructured data.

Adapt to the regulatory landscape

Data security and privacy laws, such as GDPR in the EU, continue to impact choices in technologies to implement those legislations. In particular, Privacy by Design is now a must for all new implementations, both for structured and unstructured data.

The increased use of public and hybrid c loud has a significant impact on data security

Organizations must secure a decentralized hybrid cloud environment where data control is fleeting and an increasing volume of unprotected IoT objects will require data security to leverage lightweight encryption as well as advanced privacy enhancing computation tools and data security governance tools.

Anticipation

Over the long term, it is vital to align data security (and encryption methods in particular) with upcoming technological trends like the rise of quantum technologies, with both the new capabilities (e.g. QKD) and the challenges they present (like the need for quantum-safe encryption).

Key Figures

38%

of those technologies are either already adopted by most organizations or will be in the next two years.

28%

of those technologies are expected to be adopted in the next two to five-year cycle.

34%

of those technologies are transformational and widespread adoption will take over five years.

Zoom on
Quantum-safe encryption

Data security includes the process and associated tools that protect sensitive information assets, be they in transit, at rest or in use.

Quantum-safe cryptography (QSC) – also referred to as post-quantum cryptography — aims to solve the threat to asymmetric or public key cryptography caused by the rise of quantum computing, because it relies on hard-to-solve mathematical problems that can be easily solved with a full-fledged quantum computer.

This being said, quantum computers are still a new technology that requires a high degree of knowledge and understanding around other scientific fields, such as mathematics and physics. They are still far from providing the capability to break asymmetric cryptography. However, the threat they can represent to cryptography will arise much before the first full-fledged quantum computer can break current standard cryptography, since future quantum computers will be able to break past data that would have been recorded.

Key Features

- Use cases of quantum-safe cryptography revolve mainly around replacing current standard cryptographic protocols with new quantum-safe ones that are still in a standardization process. Depending on use cases, plug-in replacement can be required for some protocols in complex cryptographic systems.
- Similarly, the point at which current cryptographic protocols must be replaced depends on the potential short- or middle-term impact of future quantum computers on stored data.

Benefits of the Technology

Replacing standard cryptographic methods with quantum-safe methods will mitigate the future threat posed by quantum computers and provide an opportunity to enhance communication and encryption security.

Challenges to Adoption

- Although several QSC ciphers already exist, the standardization process is still underway with NIST.
- Moreover, extensive crypto analysis will be required before QSC ciphers reach a significant level of maturity.
- From a performance perspective, increase in key length and in signature volumes can represent a serious obstacle, particularly for drop-in replacements in complex protocols like TLS.

Market Verticals

Virtually any industry that relies on standard cryptographic methods will be vulnerable once full-fledged quantum computers are available. The adoption will come first in the telecom vertical, then move outwards to other sensitive industries, such as:

- Governments and defense institutions
- Banking and finance
- Healthcare

About Atos

Atos is a global leader in digital transformation with 112,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together