Cybersecurity Tech radar

Tracking innovations for efficient, agile and smart security

Atos

Foreword

Zeina Zakhour

Global Chief Technical Officer, Digital security, Atos

The world is moving at the speed of digital and with new digital technologies, comes new security challenges that must be addressed to secure the digital transformation by design. In fact, this speed of innovation is expanding the 'attack surface' and creating opportunities for threat actors to reach what is one of organizations' most valuable assets: their data. In addition, cybercriminals and state-sponsored actors are innovating at a fast rate, leveraging new technologies to steal data, commit fraud and extort money. For instance, they already adopted Artificial Intelligence to launch stealth attacks and deepfake voice phishing attacks, they are targeting new IoT and edge computing infrastructure as well as focusing on paralyzing critical national infrastructures.

We created the Atos Cyber Tech Radar, to help organizations identify the security technologies that can help them address cyber threats efficiently.

With the Atos Cyber Tech 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 over 100 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
- CERT & GRC services
- Identity & Access Management
- Endpoint and Mobile Security
- Network Security
- Application Security
- Cloud Security
- Data security

Let us take a few figures

70% of organizations with public cloud capabilities experienced a security incident last year. (the State of Cloud Security, 2020).

75% of credential abuse attacks against financial services directly targeted APIs or also. (Information Age).

53% of web-targeted attacks in the first half of 2020 used APIrequests. (Forbes).

94% of organizations have had an identity-related breach, which 99% believe could have been prevented.(Identity Defined Security Alliance).

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.
- 5 years and above: emerging trends will be adopted by the mainstream after approximatively five years or more. Still, Organizations with maturity 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.

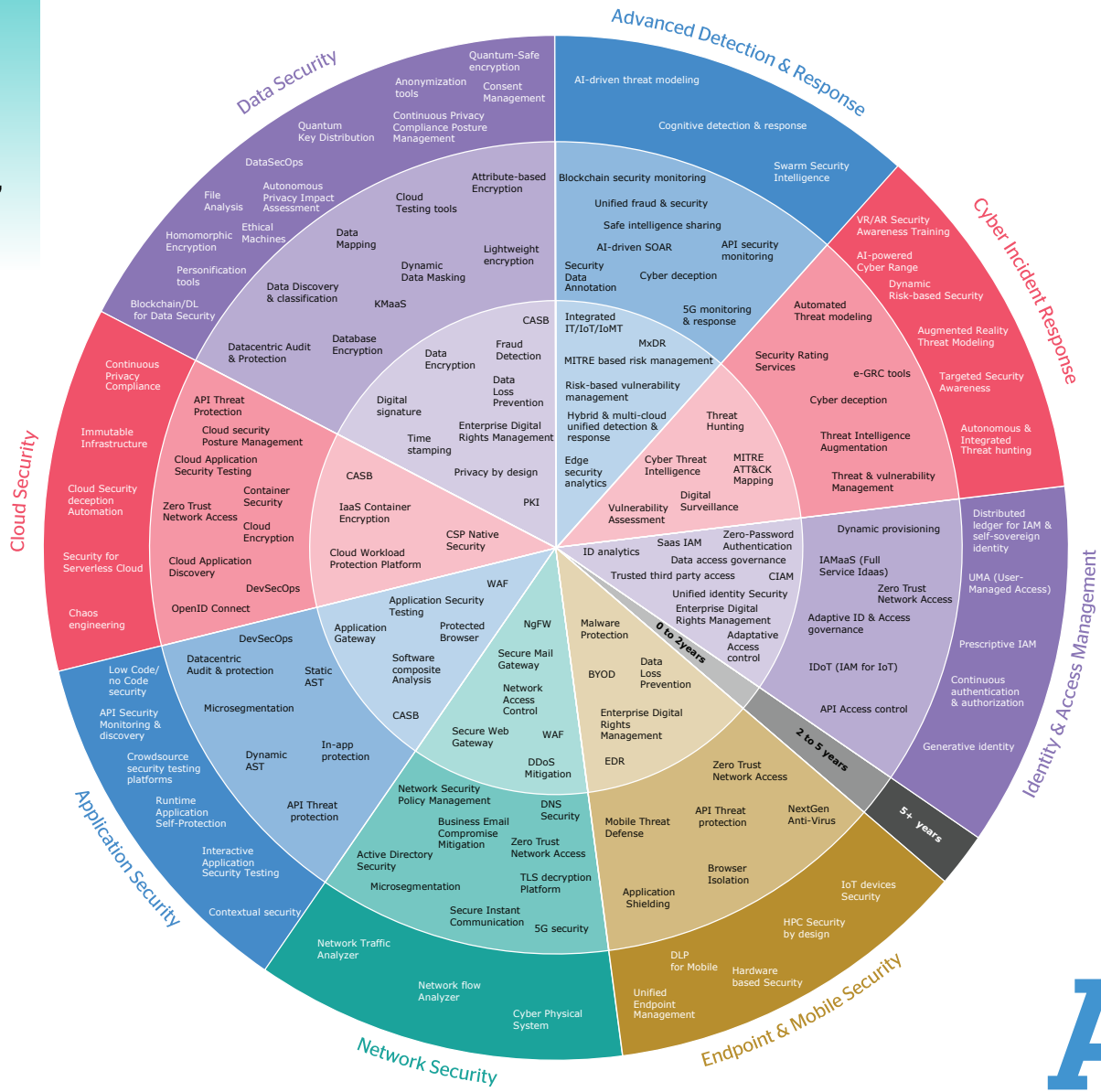
Cybersecurity innovation is a key contributor to the success of the digital revolution as we know it today. And undoubtful, it will continue to be a key foundation for safe and secure adoption of future technology trends such as quantum, edge & swarm computing, Ethical AI, immersive experience.
We hope the Atos Cyber Tech Radar will help you navigate the breadth of cybersecurity technologies and support you in refining the cybersecurity strategy of your organization. To get informed about the full release of the tech radar, follow: https://www.linkedin.com/showcase/atos-digital-security/

Contributors

Adrian Buta, Adrian Ionut Buse, Alexandru Rusandu, Allen Moffett, Anca Isac, Cosmin-Alexandru Radu, Cristian Radu, Dan Schaupner, Dave Bixler, David Bernard, David Smyth, Diego de Felice, Farah Rigal, Geert Fieremans, Jambulingam, Venkatesh, Jesus Lacal, Konstantinos Brokalakis, Laurence B gou, Lyonel Vincent, Marc Llanes Badia, Parag Ghosalkar, Philippe Bodden, Sebastien Blanc, Theo Demoulin, Vasco Gomes, Venkatesh Jambulingam, Vieri Tenuta, Vinod Vasudevan, Zeina Zakhour and Zisis Tsiatsikas.

The Cybersecurity tech radar

Tracking innovations for efficient, agile and smart security



Atos

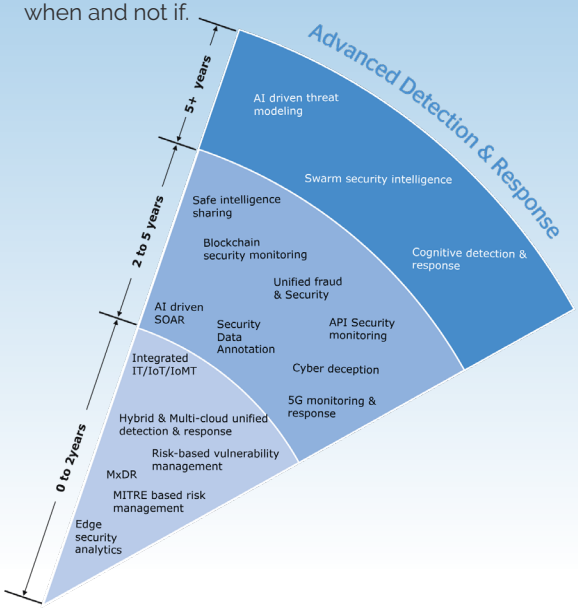
Advanced Detection & response (AD&R)

What is AD&R?

- AD&R is a rapid evolution of traditional detection and response measures hugely challenged by quickly changing attackers' techniques, the growing threat from APTs to the public but also private sectors.
- Modern AD&R has elements in all the five NIST cybersecurity Framework Functions (Identify, Protect, Detect, Respond, Recover).

Why it matters

- The proliferation of digital enterprise has opened up many vectors for cybercriminals to attack, including network, end points, cloud, OT, 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 and not if.



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 more 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 drive 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 & 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

30%

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

45%

of those technologies are expected to be adopted in the next 2 to 5 years cycle.

25%

of those technologies are transformational and wide spread adoption will take over 5 years.

Zoom on
Managed eXtended Detection & Response (MxDR)

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 end points, cloud, OT/IIOT that enable better detection (eg logs, alerts, flows, changes in device configuration and vulnerabilities etc).

Traditional detection & response measures are now hugely challenged by the fast changing attackers techniques

Key figures

- 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/Trend

- 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 skill sets for incident/ breach response.
- Centralized visibility across Hybrid IT environment.
- Better TCO using a combination of technologies, skill sets.

Challenges to Adoption

- Cost could be sometimes a challenge to adoption although MDR is getting widely adopted.

Market Verticals

- All verticals

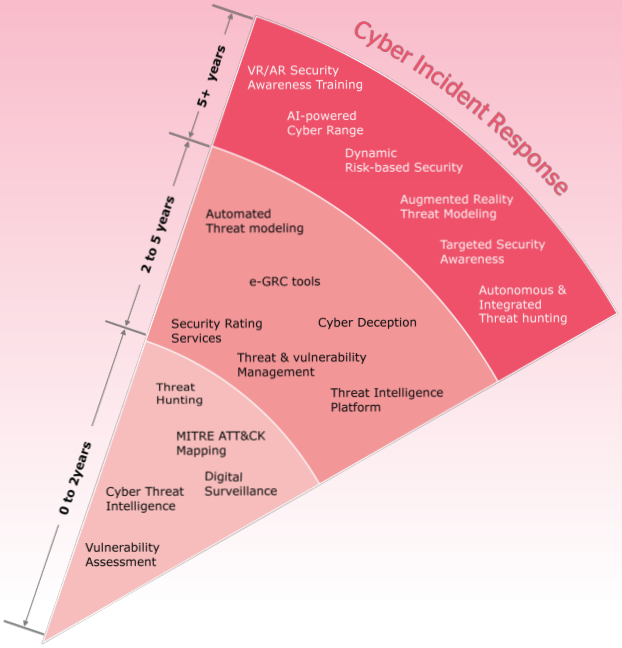
Cyber Incident Response

What is Cyber incident response?

- Cyber Incident Response complements the advanced detection & response domain with a focus on technologies, processes and frameworks aimed at the discovering, eradicating and recovering from cyber attacks 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 modelling, and threat and vulnerability management. when and not if.



The landscape

Adversary profiling with MITRE Att&CK:

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

Threat hunting for proactive protection

With the digital transformation going full speed and the continously 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.

Automation and enrichment

In order to efficiently uncover threats and vulnerabilities in their expanding digital environment, organizations will have to automate their threat hunting activities. This will also enhance and facilitate the job of CERT/CSIRT teams and accelerate threat detection. Organizations will be able to enhance threat hunting by automating and consolidating threat intelligence through different sources, from own-SOC detection, to threat intelligence sharing and cyber deception tools.

Key figures

30%

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 2 to 5 years cycle.

35%

of those technologies are transformational and wide spread adoption will take over 5 years.

Zoom on
Digital Surveillance

Digital Surveillance tools are part of threat intelligence activities, and focus on dark web monitoring and social media monitoring. Such tools and services unveal information exposure (data leakage) and contribute to better protection against reputational damage, credential leakage...

Organizations usually seek Cyber Incident response providers to augment their internal capabilities by subscribing to Incident Response Retainer services.

Key figures

- **Credentials exposure** on the dark web
- **Early Warning of Threats:** To be able to put in place preventive measures against an inevitable threat (such as ransomware attack), you need to identify as quickly as possible if your organization has been mentioned as a target.
- **Vulnerability exposure:** Finding out quickly that there is a known or zero-day vulnerability in your system represents a huge advantage for you to prioritize critical patching and mitigation.
- **Executive protection:** by using customized or targeted phishing campaigns, an attacker can compromise an account of a highlevel executive. Whaling attacks targeting specific individuals, are becoming more common because of the fact that the " Whale" (executive person) has complete access to the sensitive information the threat actor is interested in.
- **Threat actors profiling and TTP alerting:** adversary profiling helps organization understand the TTPs(Tactics, Techniques, & procedures) and the motives of threat actors targeting their organization or their industyr at large. With Digital surveillance organizations can see ahead and prioritize preventive measures to protect from upcoming attacks.

Benefits of the Technology/Trend

- Digital Surveillance tools can give a major advantage to organizations to identify if they are a target, prioritize the patching lists, have better security systems in place
- Time is essential when it comes to an attack : having the knowledge of a vulnerability before an attacker can exploit it gives a change to avoid damaged brand reputation, sensitive data leakage to the public, etc

Challenges to Adoption

- To adopt this solution, a good knowledge of the criminal underground is required.
- Visibility – Even if you have knowledge, monitoring activities in such a specific area is a challenge.
- Some expertise is necessary to identify the potential risk of an attack or interest of threat actors in attacking organizations.

Market Verticals

- Government
- Health care
- Manufacturing
- Retail
- Defense
- Banking
- Information technology

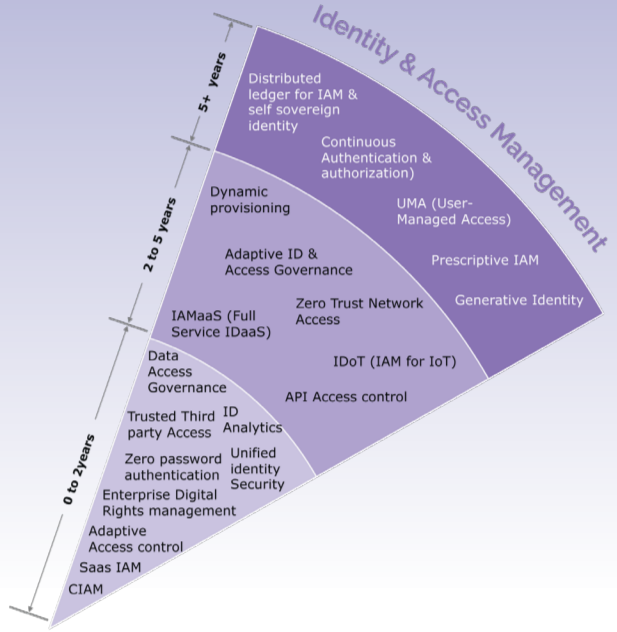
Identity & access management (IAM)

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 organisations 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.



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).

Zero Trust Architecture (ZTA)

Recognition of the insider as a key threat is forcing organizations to rethink the importance of identity and concepts such as the Principle of Least Privilege.

Key figures

40%

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

30%

of those technologies are expected to be adopted in the next 2 to 5 years cycle.

30%

of those technologies are transformational and wide spread adoption will take over 5 years.

Zoom on
ID Analytics

ID Analytics is the introduction of machine learning and behavioral analytics into IAM processes. The analytics will look at not only what a user has access to but how they are using the access to determine real-time risk and use this information in IAM processes such as access governance to deliver business value and improve end-user experience.

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

Key figures

Identity analytics builds on adaptive identity by utilizing machine learning to determine more specific risks based on trends and data patterns.

This could be used in organizations

- to identify behavior that has been unseen in the wild.
- identify an anomaly, report to an analyst, and apply security control to data access depending on the assessed risk.
- in high security organizations, this can provide visibility into zeroday threats and can provide active intelligence to analysts.

Benefits of the Technology/Trend

- It can provide insight into potential threats and identify anomalies in behaviors.
- Based on these analytics, active security controls can be implemented providing faster response to potential threats.
- Enhance Access rights security reviews as well as recertifications and reconciliation of rights over complex infrastructures with thousands of applications, users and objects.

Challenges to Adoption

- Cost
- Scalability
- Potential slowed-down access when risk is being applied to all access requests.

Market Verticals

- Public sector
- Defense
- Technology
- Telecommunications.

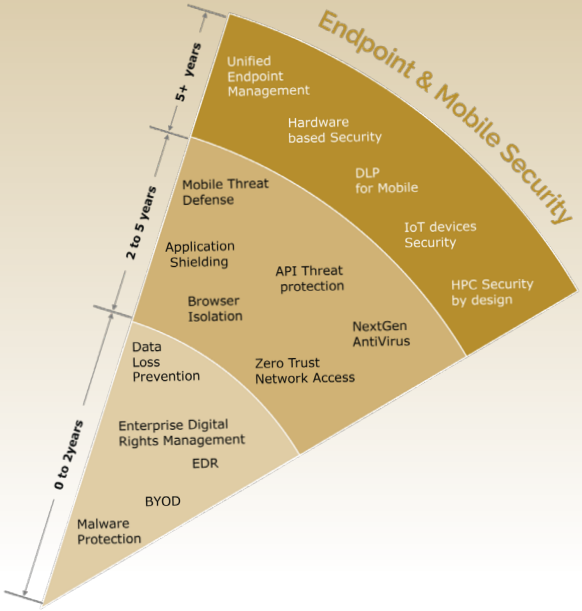
Endpoint & mobile security

What is Endpoint & 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,...
- AI and Edge Computing are expected to challenge most of 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 & Mobility 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 BYOD culture expands and IoT devices are fully adopted by organisations. Among technologies providing improvements in this area :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...). 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 NextGen Antivirus solutions, 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.

38%

of those technologies are expected to be adopted in the next 2 to 5 years cycle.

31%

of those technologies are transformational and wide spread adoption will take over 5 years.

Zoom on
EDR

- The basic principle of EDR is to drastically improve visibility of IT events, by turning endpoints into probes and gathering detailed status and activity information that can be correlated, analyzed and processed before, during, and after an attack
- All these collected bits of data can be fed to local machine-learning models or fetched and sent to a central location for further enrichment and processing, using the whole environment for intelligent detection and protection
- It allows to establish a baseline, assess, contain a situation or recover from the attack

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

Key figures

- **Malicious activity detection and containment:** provide early detection of threats on endpoint, facilitate forensics and accelerate containment of attack.
- **Incident-driven security analytics for SOC analysts:** reducing investigation time and alert volume by leveraging analytics capabilities for root-cause analysis on a compromised system, and group the related alerts into a single incident.
- **Triage:** can be used as a tool for aggregation of data, system monitoring, events detection and alerting.
- **Investigation and training:** can be used as a repository of analyses and information regarding the events. In combination with other technologies (e.g. Threat intelligence) it can bring an added value for alerts investigations, response evaluation ad training for security staff.

Benefits of the Technology/Trend

- **Correlations to accurately assess an organization's security posture and protect it from attacks :** Once centrally consolidated, all elements can be correlated with other "weather reports" like threat intelligence feeds, situational data at other managed customers, etc.
- **Response actions** (such as process kill, containment, user lock-out...) can then be triggered from this central location and pushed to all devices (even the ones that are unaffected) to protect the environment.

Challenges to Adoption

- Complexity of integration
- EDR systems do not work on unmanaged devices, which will soon vastly outnumber managed devices in corporate.
- EDR does not work on unconventional IT devices such as industrial OT environments

Market Verticals

All verticals

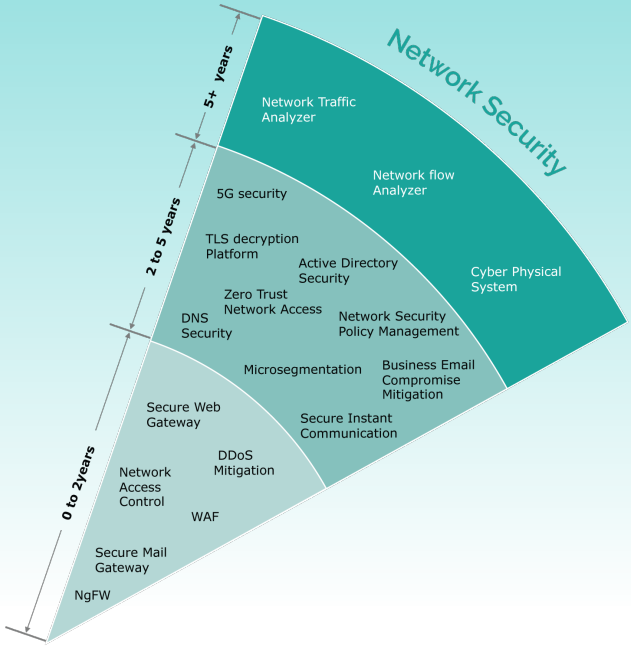
Network security

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,
- seemlessly 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 appliance 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

The uptake of preventive technologies

Preventive network security technologies that are highly agile and compatible with a wide spectrum of enterprises' IT infrastructures will have an increasing adoption rate.

The end of traditional security perimeters

All traditional perimeter controls are being redefined (e.g., Firewalls, VPNs), or virtualized and optimally delivered as a Service from the cloud. Functional consolidation and virtualization of core capabilities (SASE, FWaaS) is taking place.

On the road to Zero trust

With corporate networks, infrastructures, applications and data moving quickly beyond traditional onpremise 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.

Key figures

33%

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 2 to 5 years cycle.

17%

of those technologies are transformational and wide spread adoption will take over 5 years.

Zoom on
Zero trust network Access

- Zero trust implies that no user or device - whether inside or outside the network - will be trusted. In the traditional security paradigm, you trust everything inside the network.
- Zero trust network access solutions require all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously (per request) validated for security configuration and posture before being granted or keeping access to applications and data.

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

Benefits of the Technology/Trend

- Normalizing the user experience for application access & authenticating users on personal devices.
- Carrying encryption all the way to the endpoints for scenarios where you don't trust the carrier or cloud provider.
- Providing application-specific access for IT contractors and remote or mobile employ-ees as an alternative to VPN-based access.
- Extending access to an acquired organization during M&A activities, without having to configure site-to-site VPN and firewall rules.
- Isolating high-value enterprise applications within the network or cloud to reduce in-sider threats.
- Creating secure enclaves of Internet of Things (IoT) devices or a virtual-appliance-based connector on the IoT network segment for connection.
- Cloaking systems on hostile networks, such as systems that would otherwise face the public internet, used for collaboration.
- Dynamic assessment of the access risk, including steppinng up or down the access and/or authentication according to the user and his device security risk and posture evolution.

Challenges to Adoption

- High Time and Effort during Initial Setup.
- Understanding User Access: An organization must have a deep understanding of user access rights from the highest level possible to the bottom of the technology stack.
- Impact on Employee Productivity: A balance will be needed between security enhancement and availability of information to perform tasks.
- Traffic behind the gateway may not be encrypted by the product.
- No vendor currently covers both Identity management & access and network segmentation.

Use cases

Increasing organisation's security posture by:

- Validating users and their devices' security posture.
- Controlling access through granular policy enforcement.
- Protecting and encrypting data transactions.

Market Verticals

All verticals

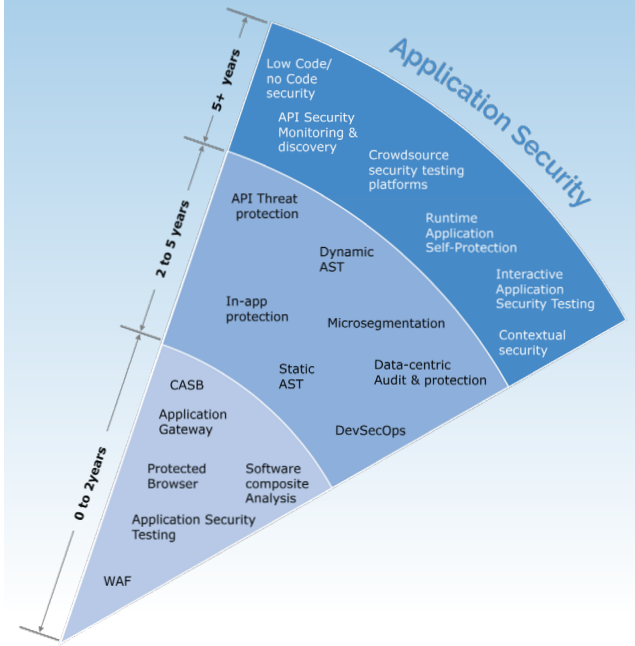
Application security

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 a fertile ground for attackers. 90% of the security incidents is launched by exploiting the software design and/or the code of a software application.



The landscape

Support of mature technologies to the classic application security dimension of critical Internetexposed web portals, with

Static analysis: the source code analysis, performed to identify problems in the software.

Dynamic analysis: the scanning process of an already packed application (i.e., an executable).

Real-time protection: devoted to the scanning process in a real-time fashion, for instance via WAF.

The need to integrate application security into the entire application lifecycle

Evolutions in the application field require the various types of application security testing (Static, Dynamic, Interactive, Mobile, ...) to be embedded into the Application Lifecycle Management tooling. in their environments and will be able to proactively mitigate them.

Heavy influencing 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 containerisation and automation,
- Orientation toward API and microservices end goal of staying in front of the attackers for a change.

Key figures

30%

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 2 to 5 years cycle.

35%

of those technologies are transformational and wide spread adoption will take over 5 years.

Zoom on
Web Application Firewall (WAF)

- WAF is designed to filter & monitor the HTTP traffic between a web application server & the internet. It provides layer 7 protection against attacks on inbound web flows.
- WAF can be seen as the equivalent at upper layers of components like network DDOS protection or network firewalls operating at lower layers.
- At layers 4 to 7, the WAF tends to work on a rather generic infrastructure-wide scope, often combined with other functionalities like TLS termination, application load balancing.
- WAF has contributed to stopping web attacks defined by OWASP in their list of top 10 security risks on web applications.

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.

Use cases

WAF can be provided in various forms

- WAF network appliance (Bespoke physical or virtual software appliances)
- Software-based WAF (WAF modules embedded in various equipment such as Load Balancers)
- Cloud WAF services

Market Verticals

- Mandated by regulators in Financial & insurance sector, at least for critical applications in large systemic financial stakeholders.
- Given the trend toward cloud and API-based architecture, WAF is becoming ever more important in all verticals.

Benefits of the Technology/Trend

- Most of the application level attacks like SQL injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) could be eliminated or minimized by deploying a WAF with strict rule set in front of a vulnerable web application.

Challenges to Adoption

- Configuring a WAF to efficiently detect and block threats can be challenging, since the "legitimate " traffic depends on applications to be protected (and thus on application lifecycles).

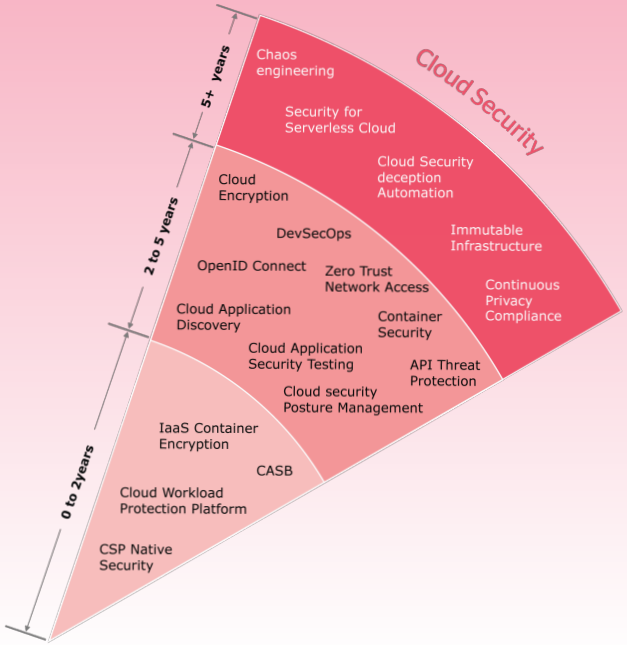
Cloud security

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.



The landscape

Losing track of cloud service & cloud native application

Organizations may have lost track of the Cloud services and Cloud native applications used by employees inside the organization, some of which may not conform to the organization's security requirements.

The growth of shadow Cloud

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 raising

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

Customers need to classify and determine the accountability for their data as

Ultimately the customer remains responsible for their data.

Key figures

22%

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 2 to 5 years cycle.

28%

of those technologies are transformational and wide spread adoption will take over 5 years.

Zoom on
CSPM – Cloud Security Posture Management

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

CSPM offerings continuously manage cloud risk through the prevention, detection, response and prediction of where excessive cloud infrastructure risk resides based on common frameworks, regulatory requirements and enterprise policies.

They proactively and reactively discover and assess risk/trust of cloud services configuration (such as network and storage configuration), and security settings (such as account privileges and encryption). Ideally, if a setting is non compliant or a configuration represents excessive risk, the CSPM offering can take automated action to adapt, including remediation.

Use cases

- Continuously monitoring for gaps between the desired security policy, the intended security posture (by the developer or DevOps team) and the actual security posture observed at runtime.
- Continuously assess for trust/trustworthiness in addition to risk (workload, service and API identities are verified, changes to Cloud infrastructure using a control change process, behavioral baselining and anomaly detection and so on).

Benefits of the Technology/Trend

- Policy visibility and consistent enforcement across multiple cloud providers.
- Continuous discovery and identification of cloud workloads and services.
- Alerting on risky new deployments or changes to the cloud environment, hosts or ser-vices.
- Risk assessment versus frameworks and external standards (ISO, NIST), technical poli-cies and best practices (CIS, CSP).
- Continuous cloud risk management, risk visualization and risk prioritization capabili-ties.
- Verifying operational activities are being performed as expected.

Challenges to Adoption

- Put in the place the correct organization between security and application teams to leverage the output/results of the solution.

Market Verticals

All verticals

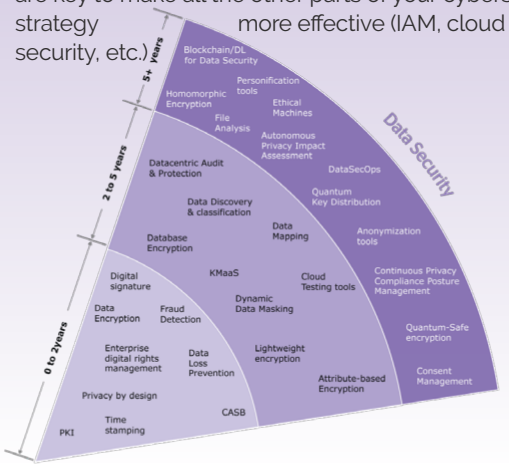
Data security

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 is the CIA (Confidentiality, Integrity, Availability) triad security model, applied to the various phases of the data lifecycle (Create, Store, Use, Share, Archive, Destroy)
- Data Security encompasses very diverse use cases from classic networks based on perimeter security, to cloud-based environments and IOT.
- Since there 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

- Knowing your data (data mapping, discovery & classification, etc) is the first step to prioritise investments and security controls.
- 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

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 Cloud has a significant impact on data security

Technologies like CASB, DLP and EDRM can and provide a good control on unstructured data, particularly in a cloud environment and for personal data protection.

Dealing with the upcoming IoT wave of largely unprotected objects

a specific effort will be required in the field of data security to leverage Lightweight encryption, specifically designed to support objects with limited computational resources.

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 challenges they present (need for quantum safe-encryption).

Key figures

30%

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

30%

of those technologies are expected to be adopted in the next 2 to 5 years cycle.

40%

of those technologies are transformational and wide spread adoption will take over 5 years.

Zoom on
KMaaS (Key Management as a Service)

- KMaaS are KMS (Key Management Server) solutions provided as a service. They tackle some of the drawbacks to adoption of encryption, enhancing robustness, flexibility and simplicity.
- Their underlying security modules can be either hardware or software.
- Most of Cloud Service Providers do have KMaaS natively available but, for regulatory purposes or based on a risk assessment requiring segregation of powers, many organizations choose for some of their data to take key management out of the CSP responsibility.

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

Use cases

- Central view on all encryption policies
- Simplified migration away from an obsolete or deprecated encryption scheme or algorithm.
- Greater control on encryption keys generation and storage.
- Parallel cryptographic operations
  - Hybrid and/or Multi Cloud integration
  - direct integration with various other SaaS to do Bring-Your-Own-Key (GCP, AWS, Azure, Salesforce, O365,...)
  - expose a KMIP interface that allows integration with any application compatible with this standard (VMware vCenter for example)
  - expose specific integration with some big SaaS of the market.

Benefits of the Technology/Trend

- Strong data protection regulatory compliance with low audit reporting costs.
- Cost reduction on encryption policies management
- Enhanced and scalable encryption keys security and resiliency.
- Encryption policy visibility and consistent enforcement across all environments (On Premise and Multi Cloud)
- Centralized traceability of cryptographic operations and access to decryption keys
  - Simplicity (compared to hosting and managing KMS/HSM)
  - Benefit from advanced cryptographic solutions without the need to host & manage them.
  - The price, as the aaS model is more attractive financially.

Challenges to Adoption

- Complexity of the deployment options and lack of clarity from providers.
- Impact on Business Applications performance.
- Dependency on the KMaaS provider.

Market Verticals

All verticals, especially if we consider BYOK usecases and particularly those where a large number of cryptographic operations are required, such as Financial Services, Government with growing importance on Healthcare as well for patient records protection.

About Atos

Atos is a global leader in digital transformation with 107,000 employees and annual revenue of over € 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), listed on Euronext Paris and included in the CAC 40 ESG and Next 20 Paris Stock Indexes.

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