Reduce Your Risk of Being Breached

External Attack Surface Management (EASM) Service

Atos EASM services uncover every internet-facing asset in your environment and give you the tools to close open vulnerabilities, shrink your attack surface, and reduce your risk of an incident

More assets, more vulnerabilities, more risk

Attack surfaces have exploded. Distributed work has flooded organizations with a wealth of new hard-to-find assets. Each of these assets can carry a wealth of exploit-able vulnerabilities like missing patches, weak encryption, insecure authentication mechanisms, misconfigurations, insecure code, and more that attackers can exploit to reach your crown jewels.

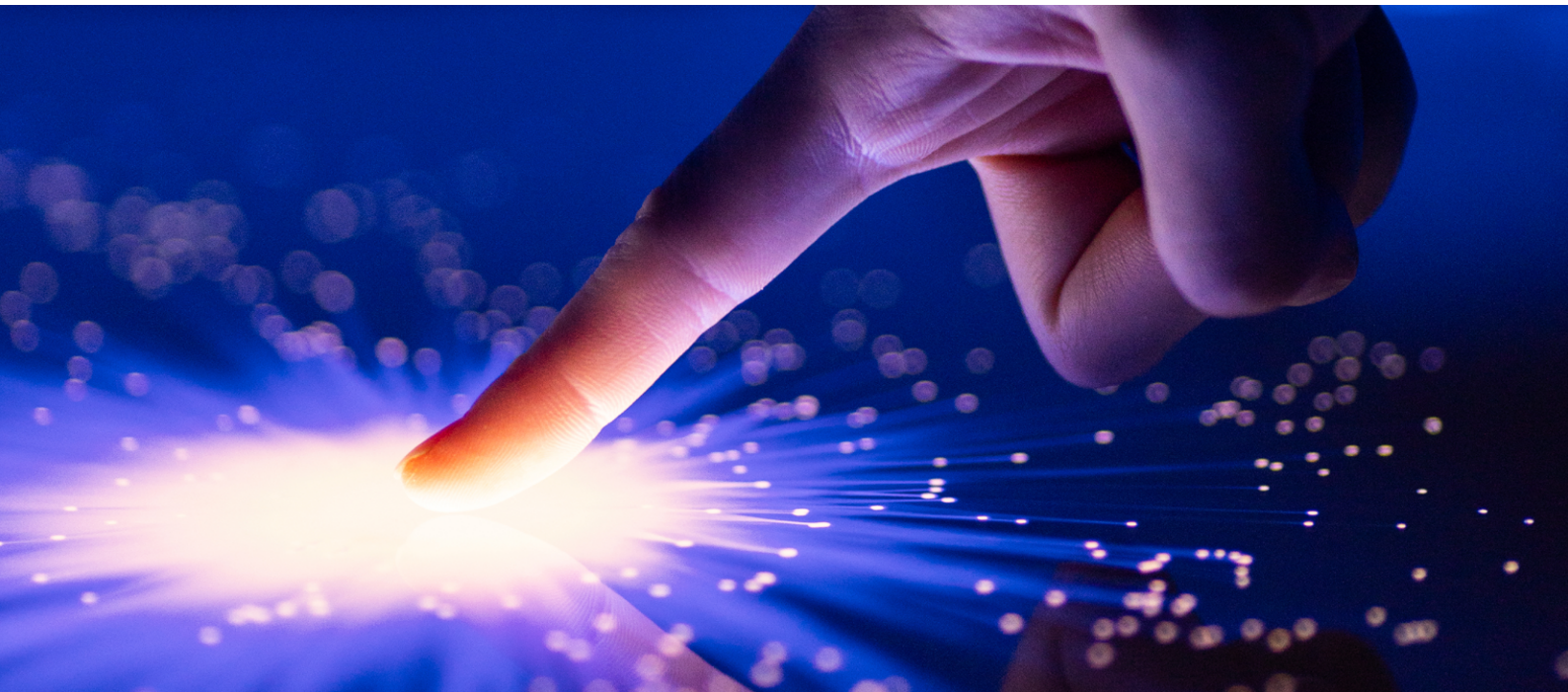
Current risk assessment and monitoring solutions miss the vulnerabilities and threats that originate in Shadow IT. Modern organizations need help to see every asset in their environment, to identify the vulnerabilities those assets carry, and to close those vulnerabilities before attackers exploit them. So, they are caught in a cycle of firefighting incidents and need to take control of their attack surface and reduce their risk.

Atos' EASM services solve this problem.

What is Atos EASM?

Atos External Attack Surface Management (EASM) service help businesses discover and map every inter-net-facing asset in their environment to identify exploit-able vulnerabilities. Atos EASM service covers servers, applications, cloud servers, domains, and more. The ser-vice also extends to the organization's subsidiaries and third parties. And you have the flexibility to set the fre-quency of the scans.

Our certified experts are trained on leading EASM plat-forms and bring years of vulnerability and threat manage-ment experience to clients.



Uncover your shadow risks

Atos EASM services offer a scalable approach to reducing your most significant source of risk. Eliminate your open exploits, and shrink your chances of suffer-ing a breach. Atos EASM services give you a scalable approach to reducing your most significant source of risk.

We offer a complete range of services to reduce risk and proactively improve your fundamental defenses. To do so, we provide visibility and control over the assets that compose your growing attack surface and the vulnera-bilities they carry.

With Atos's EASM services, you get:

Fewer Vulnerabilities:

Identify commonly exploited vulnerabilities like insecure authentication mechanisms, misconfigurations, missing patches, etc. and remediate them.

A Smaller Attack Surface:

Shrink the number of assets an attacker can exploit to breach your network and move laterally within it.

Less Risk:

Reduce the chances of suffering an incident and the damage an attacker can cause if they penetrate your network.

Take a proactive approach to managing your risk

With Atos's EASM services, you will break the cycle of constantly firefighting incidents. Instead, you will proactively eliminate your vulnerabilities, reduce the breaches you suffer, and improve your fundamental security — through three core capabilities:

Asset Visibility

We will identify and map every asset that creates your external attack surface, from endpoints to cloud resources.

Asset Monitoring

We will monitor your environment to see when new assets and asset vulnerabilities appear within your network.

Asset Management

We will prioritize and close your asset vulnerabilities to reduce your exposures to breaches, lateral movement, and compromises.

What's included in every engagement

Our EASM services include every tool and capability you need to map your attack surface, monitor it for changes, and reduce your vulnerabilities. We will:

1. Inventory your assets

Build a catalog of every asset in your environment - including hard-to-find distributed assets.

2. Uncover shadow IT

Identify user-provisioned assets that were never reported yet still connect to your network and create hidden security and operational risks.

3. Alert on exposures

Define the current state of every asset in your network and receive prioritized lists of their vulnerabilities and how to close them.

4. Improve IT security hygiene

Work with your internal teams to apply missing patches and updates, fix misconfigurations, and otherwise bring your assets to a healthy state.

5. Inform risk management

Provide critical intelligence on your attack surface and risk exposures to IT, Security, Red Teams, and Risk Management teams to inform their activities.

6. Protect remote assets

Gain visibility and control over assets outside your security perimeter and allow hybrid work and supply chain dependencies without compromising security.

7. Scale your protection

Automatically fold new assets into your security posture to maintain airtight defenses even as your environment continues to grow and evolve.

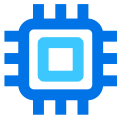
Why Atos, a proven, reliable partner in your cyber defense

Atos has decades of frontline experience managing cybersecurity for leading enterprises worldwide. Unlike com-pe-titors, our dedicated teams are certified, trained, and routinely uncover and remediate significant vulnerabilities and incidents. An extensive network of 16 SOCs supports our CERT experts that manage your EASM service.

By partnering with Atos, you gain:

Human Expertise

Leverage our hundreds of battle-tested frontline analysts and responders.



Dynamic Threat Intelligence

Use our up-to-date lists of vulnerabilities to find new exposures in your assets.

Flexible Engagements

Augment your internal EASM program or gain an entire program out of the box.

Custom Processes

Adapt our proven EASM processes to your specific security needs.

Vertical-Specific Knowledge

Deploy solutions designed for the unique needs of each industry and org structure.

Unified Security

Connect EASM with our fully managed detection and response services.

Global and Local Coverage

Tap into 16 Global SOCs with “boots on the ground” support for most regions.

Bring Atos EASM services to your organization

With Atos’s EASM services, you will:

- Shrink your attack surface, lowering the chances of suffering an incident and reducing the harm you might suffer from a breach
- Allow hybrid work and digital transformation to expand without worrying about the security exposures they can create
- Take a proactive approach to security, lower potential vectors into your network, and sleep better at night
- Create a fundamentally more secure environment that automatically protects against a wide range of modern threats like ransomware

Reach out today to partner with Atos.

Want to learn more? Schedule a consultation to build the EASM program that works best for you.

About Atos

Atos Group is a global leader in digital transformation with c. 70,000 employees and annual revenue of c. € 10 billion, operating in 67 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. 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

251007 - CS + JG