External Attack Surface Assessment

Deter and prevent cyber-attacks by identifying and securing your attack surface

The Challenge

Organisations face an expanding digital footprint due to cloud adoption, remote work, and third-party integrations. As a result, two-thirds report an increase in their attack surface.

This growing complexity makes it harder to maintain visibility and control over exposed assets, creating opportunities for attackers. Many breaches begin with a single overlooked vulnerability in an Internet-Facing asset.

Consider this:

- Enterprise attack surfaces are growing by 20–50% annually.[2]
- Only 17% of organisations can confidently inventory 95% or more of their external assets.[2]
- 70% of cyber incidents are linked to unknown, unmanaged, or misconfigured external systems.[3]

Does This Sound Like You?

- You struggle to maintain an accurate, continuous view of your external assets.
- Your attack surface is assessed in siloes – there's no unified view.
- You're exposed through third-party services, and you can't measure that risk.
- Shadow IT and user-created infrastructure are slipping through the cracks.
- You're under pressure to prove control of your digital perimeter to regulators.

Why Act Now?

Regulations such as GDPR, DORA, and the proposed UK Cyber Security and Resilience Bill are making organisations increasingly accountable for securing personal data and critical systems.

Attackers exploit what you can't see, such as outdated portals, unsecured APIs, and forgotten subdomains and unmanaged assets.

An External Attack Surface Assessment enables you to discover, prioritise, and remediate these risks before they're exploited.

The faster you act, the faster you reduce exposure and demonstrate regulatory readiness.

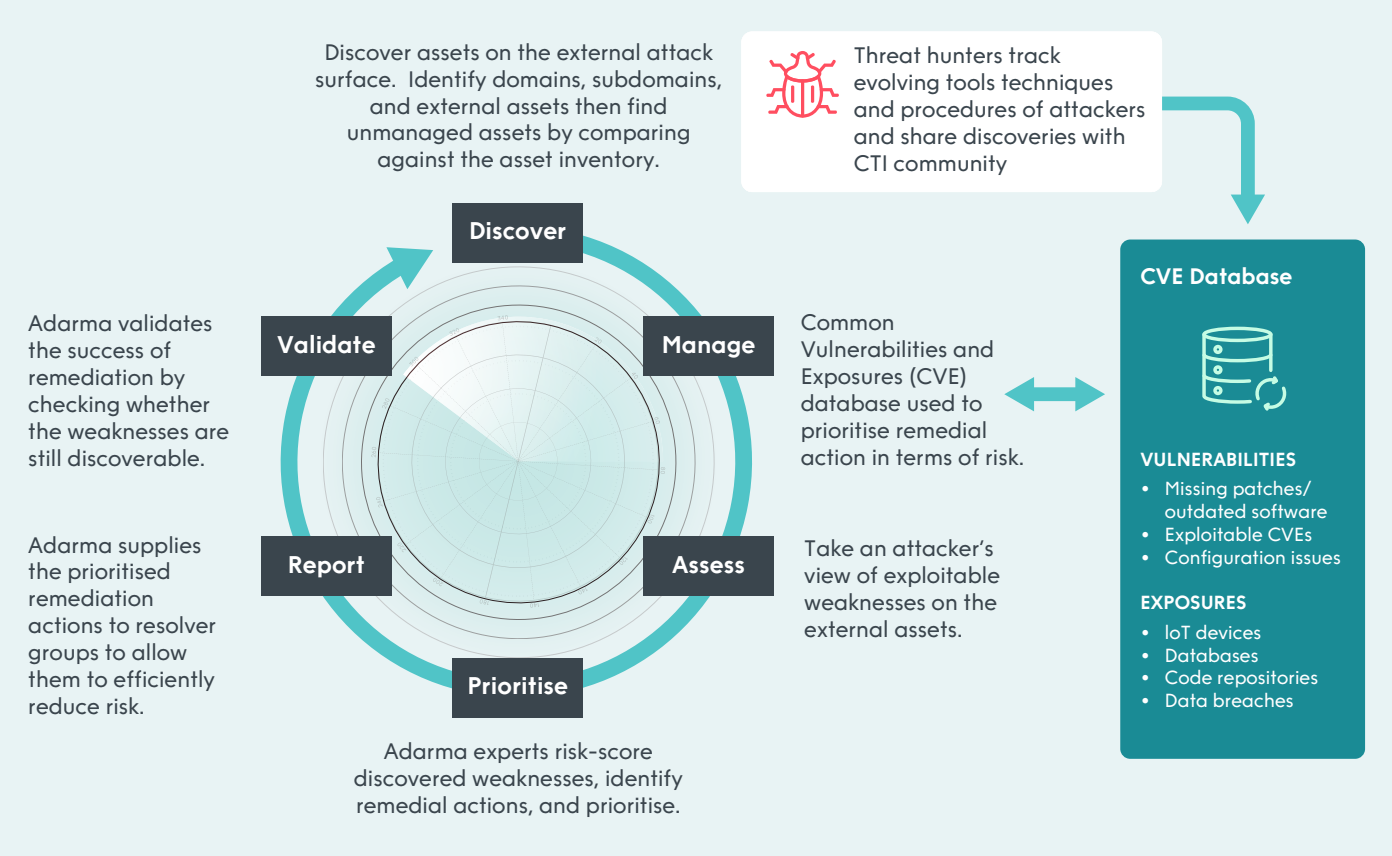
1 https://www.ibm.com/content/dam/connectedassets-adobe-cms/worldwide-content/creative-assets/s-migr/ul/g/fa/6c/codb-2024-leadspace.component.xl.ts=1725649309687.png/content/adobe-cms/us/en/reports/data-breach/jcr:content/root/leadspace

2 https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024

3 Gartner's Innovation Insight: Attack Surface Management, 9 April 2024

Adarma's Solution

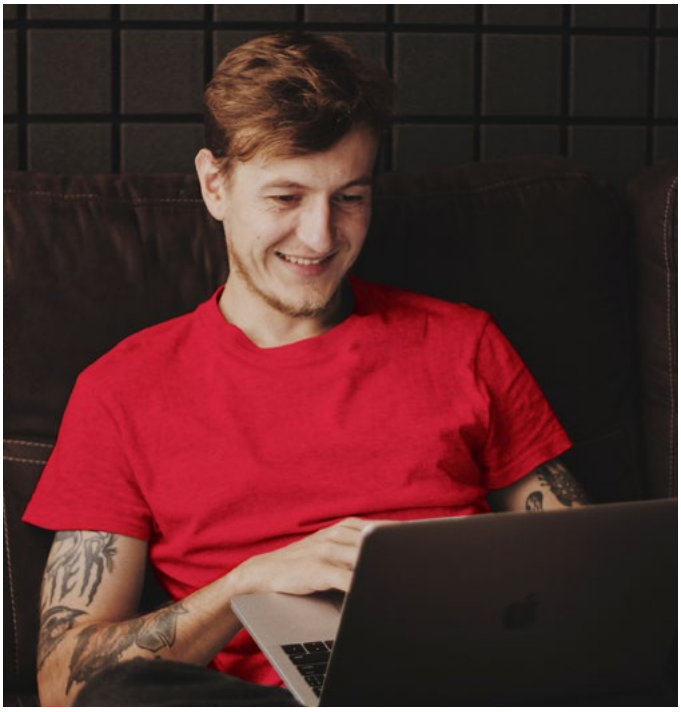
Adarma's External Attack Surface Assessment is a one-off or recurring service that identifies and evaluates exposed assets from an attacker's point of view. The diagram below summarises our approach:



We find all external assets visible to attackers and identify which ones are unmanaged. The unmanaged devices are likely to host vulnerabilities or misconfigurations which compromise your security. We scan discovered assets for weaknesses. Optionally, we also conduct internal scanning and can monitor domain names, logos, or VIP email addresses.

Threat analysts observe how attackers' tactics, techniques, and procedures are evolving. We identify the most likely methods they may use to plan and stage an attack on your organisation.

We take a risk-based approach to prioritise weaknesses and recommend remedial actions. Remedial actions include patching, configuration changes, or removing unnecessary services. Mitigation activities include configuring firewalls and implementing enhanced monitoring.



BENEFITS:

Greater Visibility
Identify and inventory shadow IT and third-party exposures, typically reducing unknown assets by 30–50%.

Regulatory Readiness
Improve audit outcomes and demonstrate compliance with growing regulatory expectations around external risk management.

Risk Reduction
Mitigate up to two-thirds of potential breach vectors by proactively identifying and addressing exposed attack surface points.

Proactive Defence
Support your cyber threat exposure management strategy by shifting from reactive detection to proactive risk reduction.

Success Stories

Adarma has helped organisations across a range of regulated sectors to deter and prevent attacks by minimising their attack surface. Here are some examples:

UK Retail Bank
Adarma delivered an award-winning managed SOC and exposure assessment service, identifying legacy assets and third-party risks that had previously evaded internal controls.

Read the case study

Global Airline
A comprehensive assessment revealed high-risk vulnerabilities in customer-facing systems. Remediation recommendations were integrated into the client's SOC workflow.

Read the case study

Luxury Goods Retailer
We supported proactive threat hunting and remediation across global domains, reducing external risk ahead of peak season trading.

Read the case study

Meet the team

Andy Younie

Managing Consultant – External Attack Surface Specialist

Andy brings extensive experience in vulnerability management, exposure reduction, and threat-led cyber assessments. He partners with customers to simplify their digital perimeter and reduce external risk.

> **“The most effective way to prevent a breach is to understand your exposure as well as an attacker would. That’s where our assessments start.”**

Connect with Andy on LinkedIn

Who We Are

Adarma is a trusted partner in security consulting and co-managed security operations. We work as an extension of your team to help simplify operations, build resilience, and deliver measurable outcomes.

We specialise in 24/7 threat detection, investigation and response, security consulting, and engineering support for large, complex organisations in high-risk sectors. Our platform, Socket, enhances automation, insight, and orchestration – empowering teams to act faster and more decisively.

Technology-independent and customer-led, we integrate with platforms like Microsoft, Splunk, CrowdStrike and Google SecOps to maximise the return on your security investments. Together, we build stronger business resilience and deliver measurable security outcomes that matter.

Ready to see what the attackers see?

Book a discovery session with one of our solution consultants and receive a complimentary Threat Landscape Report tailored to your industry.

Book a consultation