Attack Path Reduction

DATASHEET

The acceleration of digital transformation has led to the proliferation of assets and services introducing cloud misconfigurations, exposure to third-party vulnerabilities and changes in configurations, permissions and risky user behaviour.

These constant changes to your networks, be it managed and unmanaged endpoints, cloud services and applications or new employees, vendors, and customers, expand the attack surface and introduce potential new risk to your organisation. A new approach is needed to identify, measure and reduce the risks of a growing attack surface – we refer to this as Attack Path Reduction.

However, before we get on to Attack Path Reduction it is first important to understand Attack Vectors and Attack Paths.

Attack Vectors

Attack vectors are the methods leveraged by adversaries to gain unauthorised access to systems and data. Such methods are extremely varied but could include system misconfigurations, exploitable vulnerabilities, user privileges, or risky user behaviours.

Attack Paths

Attack paths are created when multiple attack vectors are chained together. The process of chaining attack vectors together is how threat actors move laterally across an organisation, escalate privileges and achieve their objectives.

The Attack Path Reduction Service

Adarma's Attack Path Reduction service combines leading technologies with Adarma expertise to effectively discover, validate, and prioritise remediation of cyber risk across your environment. We take an "assume breach" view of the attack surface, meaning we focus on identifying immediate risk to an organisation's critical assets once an adversary has already breached the perimeter.

Attack Path Reduction is the process of identifying attack vectors which can be combined to form validated attack paths to compromise critical assets. Often multiple attack paths will share a single attack vector along the path, which is known as a choke point. Identifying and eliminating such choke points will significantly increase the value of remediation efforts performed by the organisation's limited security resources.

How does it work?

Our Attack Path Reduction service follows **4 critical steps:**

1. **Threat Landscape Assessment**: We work with you to understand your threat, what are you trying to protect and why, and finally who threatens it and how.
2. **Attack Path Analysis**: We analyse your attack surface, identify and validate attack paths that could be leveraged by threat actors to reach their objectives. Our analysis enables us to determine your true footprint and the likelihood and impact of a threat actor exploiting the identified attack paths. We continuously run attack scenarios to give you validation that attack paths no longer exist.
3. **Remediation Planning**: We provide you with a concise and prioritised remediation plan to efficiently reduce risk to your critical assets.
4. **Recommendations**: We deliver actionable recommendations regarding change and investment/rationalisation decisions.

How Attack Path Analysis works

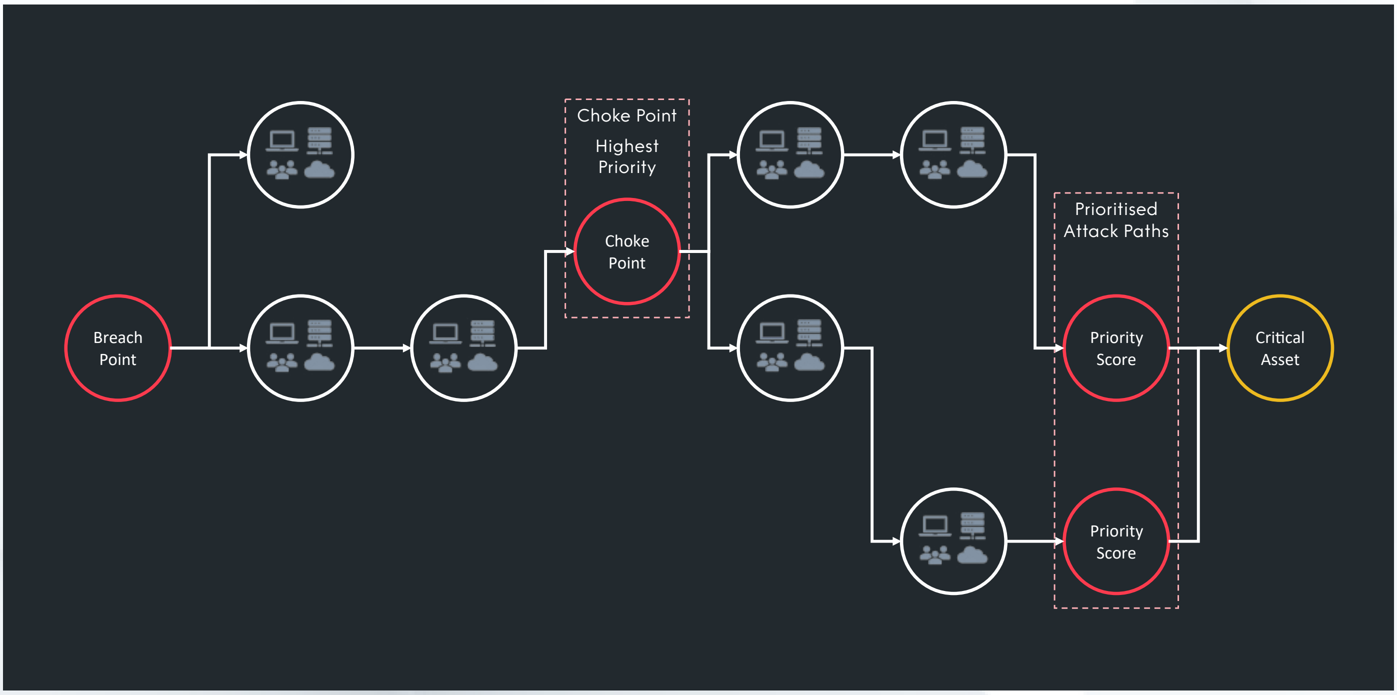

Fig 1: Attack Path Analysis highlights the controls in place and allows you add or change controls and re-run the analysis to validate if you have eliminated the attack path.

ATTACK SURFACE REDUCTION BENEFITS

We provide visual mapping of all attack paths across on-premise and cloud networks chaining together vulnerabilities, misconfigurations, user privileges, and user actions just like an attacker would to reach your critical assets.

We help you understand, discover, prioritise, and eliminate risk with reports and risk metrics that can be quantified and presented easily to the board.

We model attack scenarios to align with business goals and leverage the widest coverage of attack techniques to proactively secure databases, EC2 instances, virtual machines and more.

We deliver high impact risks first with full visibility into all vulnerabilities, affected devices, and patches with prioritisation of critical assets at risk, for swift mobilisation and prioritised fix.

We deliver, real-time, security scores which are easily understood and designed to help drive business decisions. As you remediate exposure, the security score improves, indicating and documenting IT hygiene improvement.

We are Adarma

Adarma is the UK's largest independent cyber threat management company. We deliver trusted and transparent security solutions that protect organisations against an increasingly complex and harmful threat landscape. Founded and led by industry experts, we provide cybersecurity consulting, technology and managed security services tailored to your unique requirements. Day or night we stand by your side, helping detect and respond to threats, protecting the promise of cyber resilience and helping you to build a more sustainable digital future.

Together we've got this.

How to Engage

Start your journey to active attack surface reduction today with Adarma.

For more details visit adarma.com, email **hello@adarma.com** or call us on **+44 333 0058535**.

ADARMA

ISO 27001 CERTIFICATION EUROPE™

FSQS REGISTERED