

ATTACK PATH MAPPING

Gain unparalleled visibility into the most likely attack vectors malicious intruders will seek to exploit within your network.



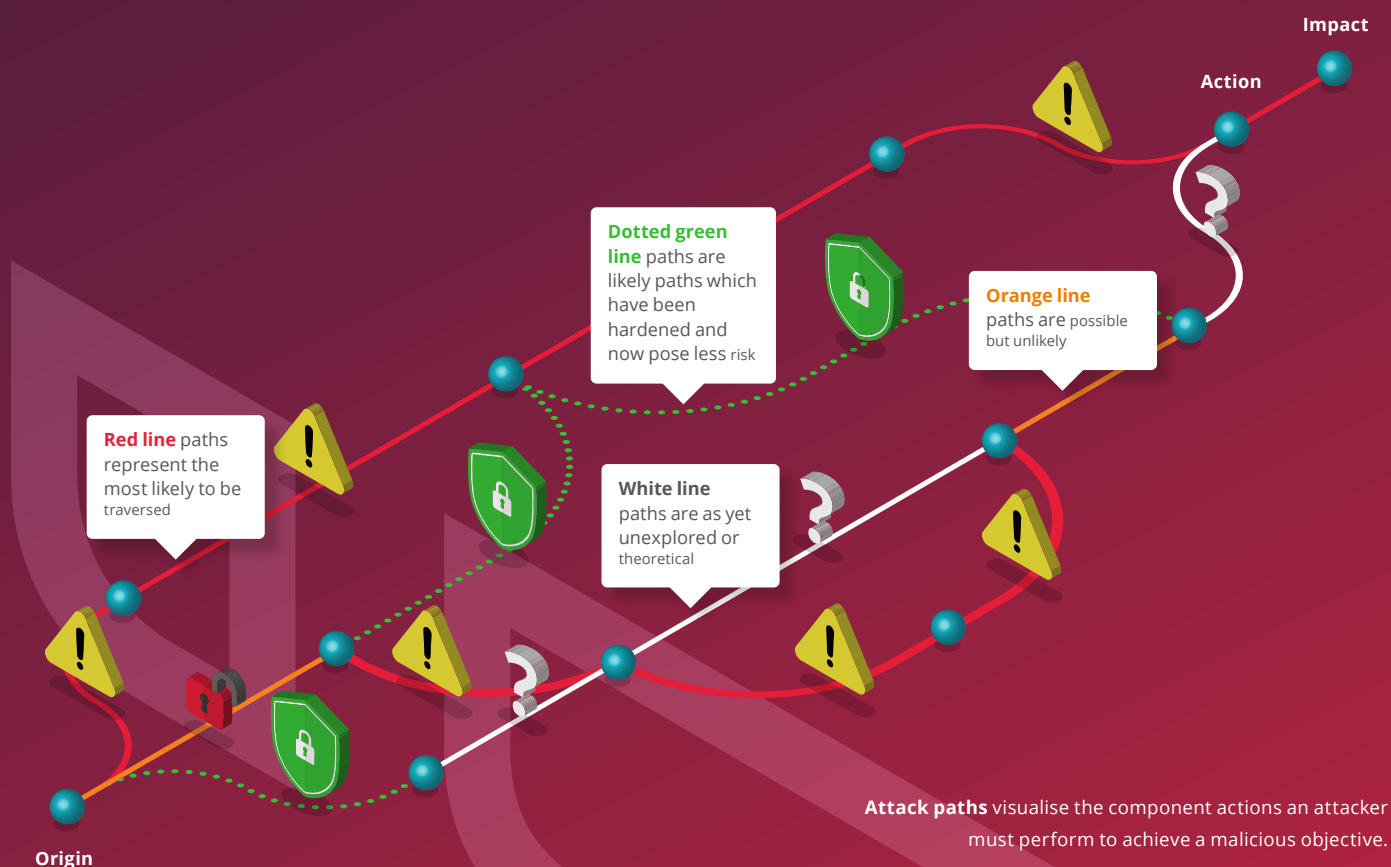
Security teams today are inundated with a backlog of vulnerabilities and false positives, overwhelming defenders and preventing decisive and effective action. Conventional threat and vulnerability management solutions, in combination with manual methods, present thousands of theoretical attack vectors that cannot be prioritised, meaning crucial vulnerabilities are frequently overlooked.

As backlogs continue to expand and adversaries enhance their speed and accuracy, the timeframe for addressing and resolving security issues is reaching critical levels, thus elevating the risks for organisations.

Attack path mapping alleviates defenders and enables you to visualise and focus on the most pertinent threats to your business.

JUMPSEC's Solution

We specialise in identifying and mapping the potential paths attackers exploit to gain access, escalate privileges, and move through your network to achieve specific malicious objectives. This allows you to eliminate inconclusive results and reduce time-consuming distractions and ultimately prioritise the right remediation efforts in the most critical areas.



Attack path mapping is highly tailored and context-dependent. By establishing a deep understanding of your business, high value assets, and relevant threat intelligence, JUMPSEC only identifies and investigates the paths that pose the most realistic and critical risks to your business.

WHY JUMPSEC?



Our human driven approach overcomes the limitations of typical penetration testing and red team exercises. Typically, these approaches follow the path of least resistance, taking the shortest and narrowest possible route to achieve the objective, meaning fewer attack paths are explored, fewer controls tested, and ultimately fewer improvements can be identified.



Unlike a product only solution, JUMPSEC doesn't overwhelm your security teams by revealing 1000s of vulns and theoretical paths that you cannot prioritise.



In contrast, JUMPSEC offers collaborative attack path mapping exercises that enable the scalable assessment of large environments. Instead of achieving a limited objective as quickly as possible, JUMPSEC maintains the demonstrable impact of each attack simulation across the entire network, thus delivering more improvement opportunities in areas where attackers can feasibly seek to exploit your organisation.

Benefits and outcomes

Attack Path Mapping represents a significant step in an organisation's progression towards long-term strategic success in cyber security.

By building targeted controls against the most pivotal attacker actions, JUMPSEC maximises the value of your investment in key strategic security controls. **Key benefits include:**



Understand how well your network tolerates real world-style attack patterns.



Gain insight to the level of sophistication an attacker needs to successfully compromise your systems.



Visibility of the environment and its susceptibility to compromise as part of a real-world attack.



Identify additional prevention and detection controls to close or restrict the attacker's ability to traverse attack paths, controlling the risk of the end-goal being achieved.



Demonstrate how effectively the network meets the specific stated security objectives.

JUMPSEC Attack Path Mapping (APM) focuses on truly exploitable issues which enable an attacker to progress toward their objective, meaning you can generate real cyber security improvement because you are not simply repeating the same tick-box activities each year.

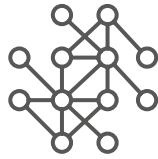
Key Features

JUMPSEC's Attack Path Mapping encompasses the following key features:



Threat Modelling

Review your environment's threat profile and identify key services, functionality, and infrastructure that can be leveraged, abused, or targeted by attackers.



Network Visibility

Gain a holistic view of your network, discover and map all interconnected devices, systems, and dependencies, providing a clear visualisation of your network architecture.



Flexibility and Scalability

Align with your unique network infrastructure, business processes, and security objectives. As new attack vectors and techniques emerge, JUMPSEC ATM can flex over time to address emerging threats and provide you with the latest tools and insights to stay ahead of attackers.



Attack Path Validation

Test to validate attack paths can be traversed to achieve in-scope objectives, demonstrating whether key technical milestones can be achieved to escalate privileges, traverse the environment, and perform actions with a tangible business impact.

Customer Success Story



"JUMPSEC consistently provides high quality and reliable support, demonstrating expert knowledge in their field and composure in challenging situations, which gives us full confidence that they are the right security partner for the job!"

Groupe Atlantic