Risk Management and Attack Surface

Manage Assets, Minimise Vulnerabilities and Reduce Risks

Cyber security is an increasingly pressing concern for businesses. As organisations are becoming more reliant on their IT, their number of exploitable assets is growing. Every technology investment brings with it a potential new attack surface. As a result, businesses are now looking for a multi-layered, proactive defence that will protect their entire IT infrastructure.

As an MSP, it is your responsibility to understand how best to manage and mitigate risks across your clients' attack surfaces.

What is the Attack Surface?

A business' attack surface is made up of the network of connected IT assets that could potentially be targeted during a cyber attack and therefore pose a risk to the business.

An organisation's attack surface is typically made up of four key elements:

On-premises IT assets

(e.g. servers, hardware and endpoints.)

Cloud assets

(e.g. Cloud servers and workloads, SaaS applications and Cloud-hosted databases.)

External assets

(e.g. services purchased from external vendors or partners that house company data.)

Subsidiary networks

(e.g. networks that are shared by more than one organisation.)

What is Attack Surface Risk Management?

Attack surface risk management refers to the proactive management of all risks and threats associated with the assets that make up the attack surface.

Why Do Organisations Need Attack Surface Risk Management?

As businesses have adopted new IT and Cloud solutions, their digital footprint has increased, and their attack surfaces have become larger.

67%
of organisations have seen their attack surfaces expand in the last 12 months.

69%
of organisations have been compromised an unknown or poorly managed assets in the last 12 months.

73%
of IT security decision makers are concerned about the digital attack surface.

(Source:IBM)

Legacy asset discovery, risk assessment and vulnerability management processes can no longer keep pace with the speed at which new threat vectors are arising. Your customers now need security solutions, such as attack surface risk management, which are designed for the more devolved, multi-layered attack surfaces of modern businesses.

The Value of Attack Surface Risk Exposure for MSPs

Increased demands upon the MSP warrant an extended reach and proactive visibility into today's popular Cloud platforms. Fast integration into well-known collaboration Cloud-based services is required, as these are more uncontrolled growth areas in terms of attack surface expansion:

Ensure your services can respond to customer demand.

Remain competitive in the MSP space.

Centrally deliver security services across multi-vendor platforms and customer sites.

Streamline MSP security solution delivery and automate email and endpoint response.

How to Carry Out Attack Surface Risk Management

Effective attack surface management should include:

- Automating asset discovery, review and remediation
- Eliminating known vulnerabilities, including misconfigurations, unpatched software and weak passwords
- Continually mapping all client assets
- Efficiently identifying and disabling unknown assets and shadow IT assetspasswords

To achieve this, you should follow five key phases:

Phase One: Discovery	Phase Two: Testing	
First, identify and map all digital assets across the internal and external attack surface to enhance visibility across the client's IT infrastructure.	As the attack surface is always changing, you must carry out proactive, continual monitoring and testing to analyse assets, prevent new vulnerabilities and close any security gaps.	
Phase Three: Context	**Phase Four: Prioritisation**	**Phase Five: Remediation**
Not all IT assets within the attack surface pose the same risk to a business. You should analyse the assets within an attack surface and consider key factors such as how the assets are used, who uses it and its network connection to help contextualise the threat and determine the severity of the risk an asset poses.	Next, prioritise your remediation efforts for any identified vulnerabilities. You should do this using objective, data-backed criteria including threat visibility and history of exploitation.	Using the information gathered in the first five phases, you can now begin to remediate any potential threats across the attack surface.

More Than a Solution: Trend Micro One

Seamlessly integrates into your existing security stack.

Automated cross platform and cross customer analysis chains.

Root cause automation for faster response and remediation.

Benefit from cost-effective security. Scale with confidence and achieve more with less.

Centralised and simplified security for the decentralised workforce.

Accelerates detection and response and helps you to maintain compliance for your customers.

Tighten the ever-expanding, non-definable modern security perimeter.

Unify asset management and billing across multiple tenancies from a single console.

Trend Micro One Results

Over 94 billion threats blocked.

Helps protect over 500,000 organisations globally.

Managed over 5 trillion threat queries.

Monitor, Mitigate, Manage: Trend Micro

As the attack surface continues to grow for your clients, you need to modernise your approach to cyber security. To start transforming your MSPs approach to risk management with Trend Micro today, get in touch with one of our expert representatives.

GET IN TOUCH