TREND MICRO™

The MSP Guide to Attack Surface Risk Management

Manage Assets, Minimise Vulnerabilities and Reduce Risks

The Future of Cyber Security

Cyber security is an increasingly pressing concern for businesses of all sizes. New cyber threats are always developing rapidly and, as organisations become more reliant on their IT, the number of exploitable assets is growing. Every technology investment brings with it a potential new threat vector. 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 in the modern, mature cyber environment. The solution? Attack surface risk management.

To help you get started, we have created a comprehensive guide to this new security strategy. We explore everything you could need to know, including:

- What is the attack surface?
- What is attack surface risk management?
- Why do organisations need attack surface risk management?
- Why attack surface risk management is valuable for MSPs
- How Trend Micro solutions can help
- And much more

C++ - main/Level01.cpp - Moonlight SDK
Outline
Make Target
No consoles to display at this time...

```
EXPORT_SYMBOL(groups_alloc);

void groups_free(struct group_info *group_info)
{
 if (group_info->blocks[0] != group_info->small_block) {
  int i;
  for (i = 0; i < group_info->nblocks; i++)
   free_page((unsigned long)group_info->blocks[i]);
 }

 kfree(group_info);
}

EXPORT_SYMBOL(groups_free);


 nblocks = n
```

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. Simply by being connected to a corporate network, any of these assets could pose a risk to the business in question. An organisation's attack surface is typically made up of four key elements:

- **On-premises IT assets** - including servers, hardware and endpoints.
- **Cloud assets** - including Cloud servers and workloads, SaaS applications or Cloud-hosted databases
- **External assets** - including services purchased from external vendors or partners that house company data or are incorporated in the connected network
- **Subsidiary networks** - networks that are shared by more than one organisation

As your clients' businesses scale and they deepen their IT investments, their attack surfaces will continue to grow. Therefore, it is extremely important that you have the tools, strategies and solutions in place to manage their assets effectively, so you can reduce their overall risk.

What is Attack Surface Risk Management?

As the name suggests, attack surface risk management refers to the proactive management of all risks and threats associated with the assets that make up the attack surface. To manage these risks effectively for your customers, you should continually monitor existing and new threat vectors within an organisation's IT infrastructure. This allows you to evaluate and prioritise the potential risks and implement an effective remediation strategy.

When conducting attack surface risk management, you should adopt the perspective of an attacker, and look for potential vulnerabilities and risks in both known and unknown assets. This will help you to implement a more comprehensive defence for your customers, across their entire IT infrastructure and attack surface.

Why Do Organisations Need
Attack Surface Risk Management?

In recent years, as technology has become more integral to business operations, most organisations have undergone significant digital transformations. To facilitate remote working models, businesses have adopted new IT and Cloud solutions, which in turn have increased their digital footprint and made their attack surface larger.

As a result, the number of threats on businesses' attack surfaces has risen.

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. This is because traditional solutions were designed to secure more stable, centralised corporate networks, rather than the more devolved, multi-layered attack surfaces of modern businesses. For instance, penetration testing can only identify vulnerabilities in known assets and cannot test for new cyber risks. To keep their data and valuable assets safe, businesses are now looking for security solutions that can keep up with the rapidly evolving cyber threat landscape.

The Value of Attack Surface Risk Management for MSPs

As businesses become more reliant on their technology, there is naturally a higher demand for solutions that map directly onto their continually developing attack surface. As a result, offering attack surface risk management as an MSP will help you to remain competitive and ensure that your services directly respond to consumer demand.

Through attack surface risk management, your MSP will gain much-needed visibility across all potential attack vectors. This will streamline the process of providing cyber security support to clients. You will have clear, targeted actions to take that will help to mitigate risk and reduce the attack surface.

As an MSP, effective attack surface management should include:

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

The Value of Attack Surface Risk Management for MSPs

To achieve this and create an effective attack surface risk management strategy, you should follow five key phases:

Phase One: Discovery

First, identify and map all digital assets across the internal and external attack surface to enhance visibility across the client's IT infrastructure.

Phase Two: Testing

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

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.

Phase Four: Prioritisation

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.

Phase Five: Remediation

Using the information gathered in the first five phases, you can now begin to remediate any potential threats across the attack surface.

Proactively containing threats across the attack surface in this manner will help to improve your MSP's reputation, strengthen client satisfaction and establish your business as a figure of authority in the cyber security space.

More Than a Solution: Trend Micro One

At Trend Micro, we provide so much more than just security solutions, we provide the means by which you can effectively manage and mitigate cyber risks. With so many clients to manage and so many IT environments to monitor, consistently containing threats and vulnerabilities can be challenging for MSPs. At Trend Micro, we proactively adopt this burden for you and eliminate the ongoing stress of risk management.

We know that effective attack surface risk management simply would not be possible without the right tools. That's why we have created Trend Micro One: a unified security platform with broad third-party integrations. Seamlessly integrating into your existing security stack, the platform continuously discovers your dynamic attack surface, assesses and prioritises your risk, and helps you respond with the right security at the right time. Supported by innovative security capabilities such as XDR, continuous threat monitoring, risk assessments, and automation, Trend Micro One accelerates detection and response and helps you to maintain compliance for your customers.

Over 94 billion threats blocked.

Helps protect over 500,000 organisations globally.

Managed over 5 trillion threat queries.

TREND MICRO™

Monitor, Mitigate, Manage: Trend Micro

As the attack surface continues to grow for your clients, you need to modernise your approach to cyber security. As global cyber security leaders, Trend Micro can help you to eliminate vulnerabilities and proactively manage threats across all your clients' IT environments.

To start transforming your MSP's approach to risk management, get in touch with one of our expert representatives today.

Get in touch