A global study

Mapping the digital attack surface:

Why global organisations are struggling to manage cyber risk

January, 2023
Trend Micro

Introduction

There's a simple but powerful dynamic driving cyber risk for most organisations today. The more they invest in digital infrastructure and tooling to drive sustainable growth, the more they may expose themselves to attack. According to experts, digital transformation during the pandemic pushed many of organisations over a technology "tipping point" from which they will never return. In short, the future of business is digital–from hybrid working to cloud-powered customer experiences. That creates a challenge for CISOs.

This challenge is often articulated in terms of the digital attack surface–that is, the collection of applications, websites, cloud infrastructure, on-premises servers, operational technology (OT) and other elements which are often exposed to remote threat actors. The risks associated with attack can be mitigated if organisations have visibility into all of these assets, calculate their risk exposure accurately and then take steps to secure the attack surface. Yet many struggle to do so.

To find out more, Trend Micro commissioned Sapio Research to carry out a survey in April 2022. It polled 6297 decision makers (3138 IT decision makers and 3159 business decision makers) across 29 countries: the UK, Belgium, Czech Republic, Netherlands, Spain, Sweden, Norway, Finland, Denmark, France, Germany, Switzerland, Austria, USA, Italy, Canada, Taiwan, Japan, Singapore, Australia, India, Poland, Hong Kong, Malaysia, Philippines, Indonesia, Mexico, Colombia, Chile.

6,297

IT security decision makers

29

countries

How malicious actors target the attack surface

As the latest Trend Micro annual cybersecurity report for 2021 highlights, threat actors deploy a range of tactics, techniques and procedures (TTPs) to target various elements of victim organisations' corporate attack surface. These included:

- **Email inboxes**
- **IoT endpoints**
- **Mobile applications**
- **Remote desktop protocol (RDP) endpoints**
- **Virtual private networks (VPNs)**
- **PCs**
- **Websites**
- **Servers**
- **Certificates**
- **Public cloud services**
- **Supply chain infrastructure and services**

They did so via phishing, vulnerability exploits, compromise of misconfigured services and other techniques—to deploy ransomware, banking Trojans, info-stealers, botnets, and much more. And they were astonishingly persistent last year. Trend Micro alone blocked over 94 billion such threats for customers in 2021. Many other organisations were doubtless not so lucky.

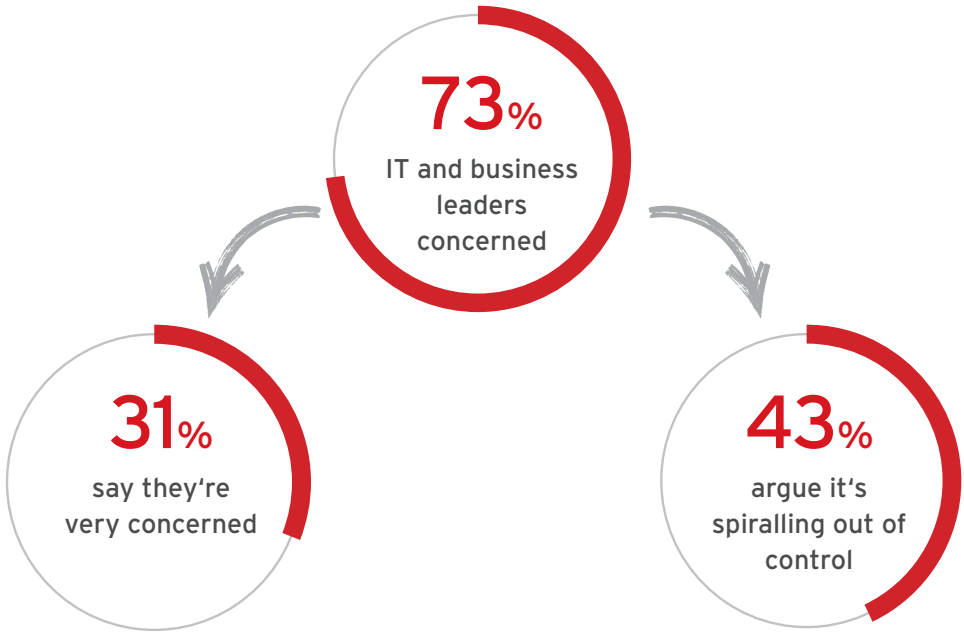
94 billion

threats blocked by Trend Micro in 2021

Organisations are concerned

With stats like these, it's perhaps not surprising that nearly three-quarters (73%) of IT and business leaders we polled are concerned with the size of their digital attack surface. A third (31%) say they're "very concerned". Yet there's more. Some 43% go even further, arguing that the attack surface is spiralling out of control.

There's a sense that major investments in IT modernisation over the past few years have created a momentum that is increasingly difficult to manage. When asked to describe their attack surface, the most popular answer for respondents (37%) was that it is "constantly evolving and messy". This hints at the challenge security teams have: an attack surface that is expanding out of control. In fact, only half (51%) of respondents claim to have completely defined their attack surface. Gaining visibility of this kind is surely the first step towards effectively mitigating risk.



37%

said it is "constantly evolving and messy"

The visibility challenge

Unfortunately, nearly two-thirds (62%) of the IT and business leaders we spoke to admit they have blind spots in trying to secure their attack surface. On average, responding organisations have only an estimated 62% visibility into their total attack surface. Yet even this is only a best guess. The likelihood is that it is even lower.

Cloud assets are understandably considered to be the area where organisations have the least insight (37%), followed by networks (34%) and end user assets (29%). In the cloud, change is the only constant. VMs, containers and other assets appear and disappear with mind-boggling frequency. Business users may bypass IT altogether when setting up new digital initiatives. And continuous innovation from platform providers means the whole edifice is built on constantly shifting sands.

Organisations operating across borders are also impacted. Two-thirds (65%) of respondents claimed that the fact they are global makes managing the attack surface more challenging. Yet a quarter (24%) are still mapping their environments manually, and 29% are doing it regionally, which runs the risk of creating information silos.

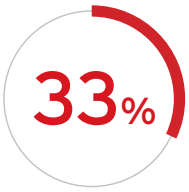
Let's run down some of those key reasons why attack surface visibility is so challenging today:

- **Organisations don't have the right tools to gain visibility into all their assets**
- **CISOs and their teams have too many tools, creating information silos**
- **Opaque supply chains**
- **An environment in constant flux: especially in the cloud where assets are dynamic and ephemeral**
- **The sheer size, complexity and distributed nature of modern IT environments**
- **Constant technology innovation, especially from cloud vendors**
- **Business units investing in new products and services without telling IT (shadow IT)**
- **An explosion in remote working endpoints and shadow IT during the pandemic**

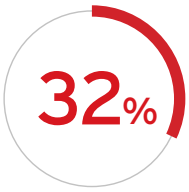
Many of these challenges were borne out by responses to our question: "Why is it so difficult to understand and manage cyber risk?" The largest number of respondents said it is simply hard to quantify (38%). A third (33%) claim they don't have the resources to do so, and a similar number (32%) that they have limited visibility. Complaints of too many tools (30%) and alerts (27%) illustrate the need for a unified platform-based approach. A fifth (21%) spoke of data silos.

Why is it so difficult to understand and manage cyber risk?

said it is simply hard to quantify



claim they don't have the resources to do so



said that they have limited visibility

The problem with managing risk

The end goal of gaining visibility and control of the digital attack surface is ultimately to better understand and manage cyber risk. Yet over half (54%) of organisations we spoke to admit their method of assessing risk exposure isn't sophisticated enough. Less than half (45%) claim to have a completely well-defined process for this.

Part of this is likely down to a lack of investment in the right tools. Yet strategy and process also matter. Over a third (35%) of respondents admit to only reviewing or updating risk exposure every month or less. And less than a quarter (23%) do so daily. Given the pace of technology innovation, the rate of digital investment and the velocity at which the threat landscape is evolving, regular assessments are critical to full visibility and improved control over the attack surface.

It's perhaps not surprising that, when asked what their biggest challenge in managing the digital attack surface is, respondents were most likely to answer: keeping up to date with constant change (39%).

Building a more risk-aware organisation

So how can CISOs build a more risk-aware organisation?

It comes down to three important steps:

1) Gain visibility into all assets and attack vectors

2) Use that data to continuously calculate risk exposure

3) Invest in the right controls to mitigate that risk

The benefit of a platform-based approach here should be clear. If the platform is extensive enough to cover the entire attack surface—from email and endpoints to networks and the cloud—it will help to eliminate data silos and provide comprehensive visibility into assets. That same platform could be configured to deliver continuous protection of those asset via prevention, detection and response tools and techniques, to minimise security gaps and improve decision making.

A platform-based approach will not only reduce expenditure on renewing and managing point products, it also saves stretched IT teams time and effort—freeing them to work on high value proactive security tasks rather than swivel-chair fire-fighting.

To find out more, head to **www.trendmicro.com**