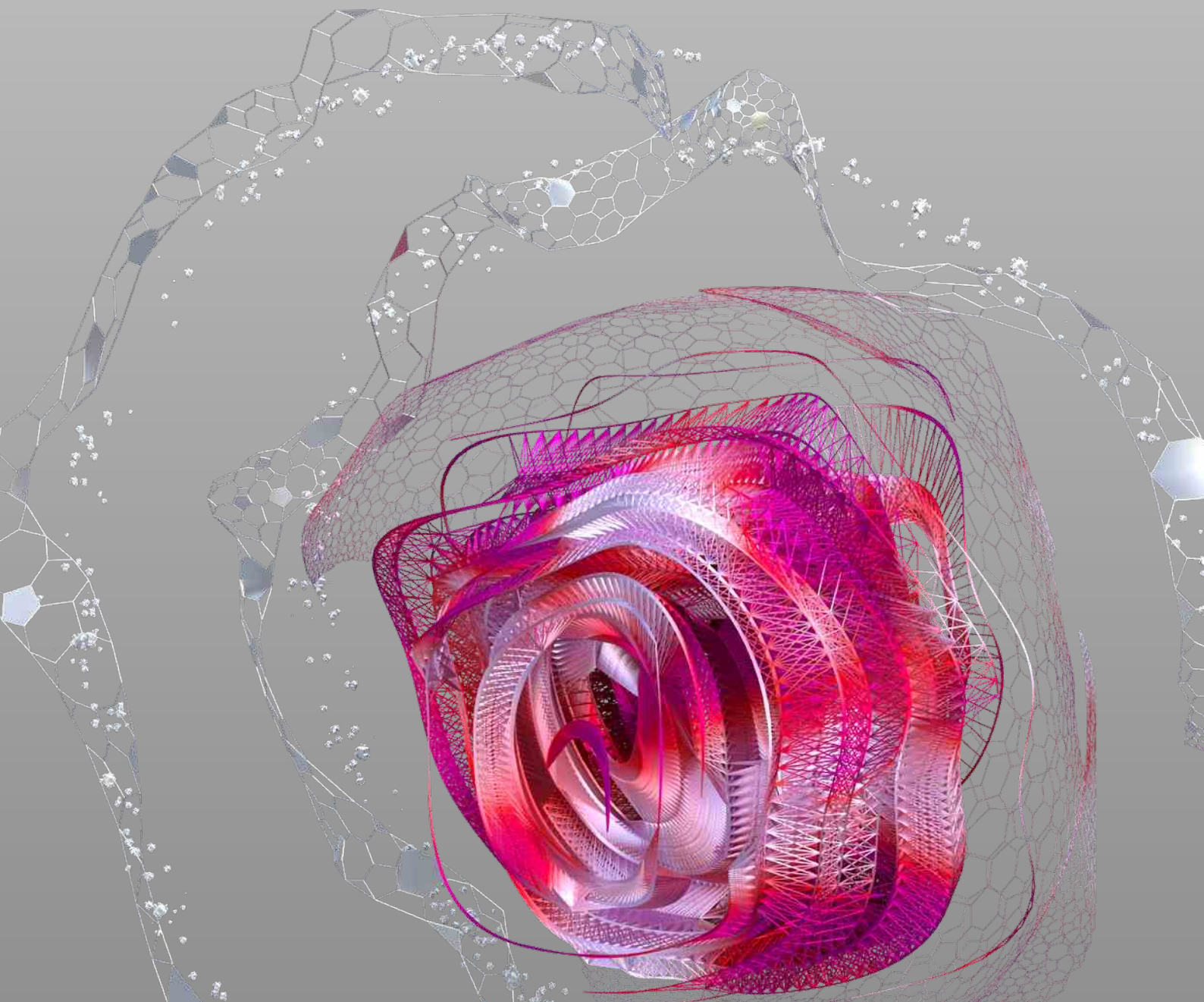
TREND MICRO™

A global study

EVERYTHING IS CONNECTED:

Uncovering the ransomware threat from global supply chains



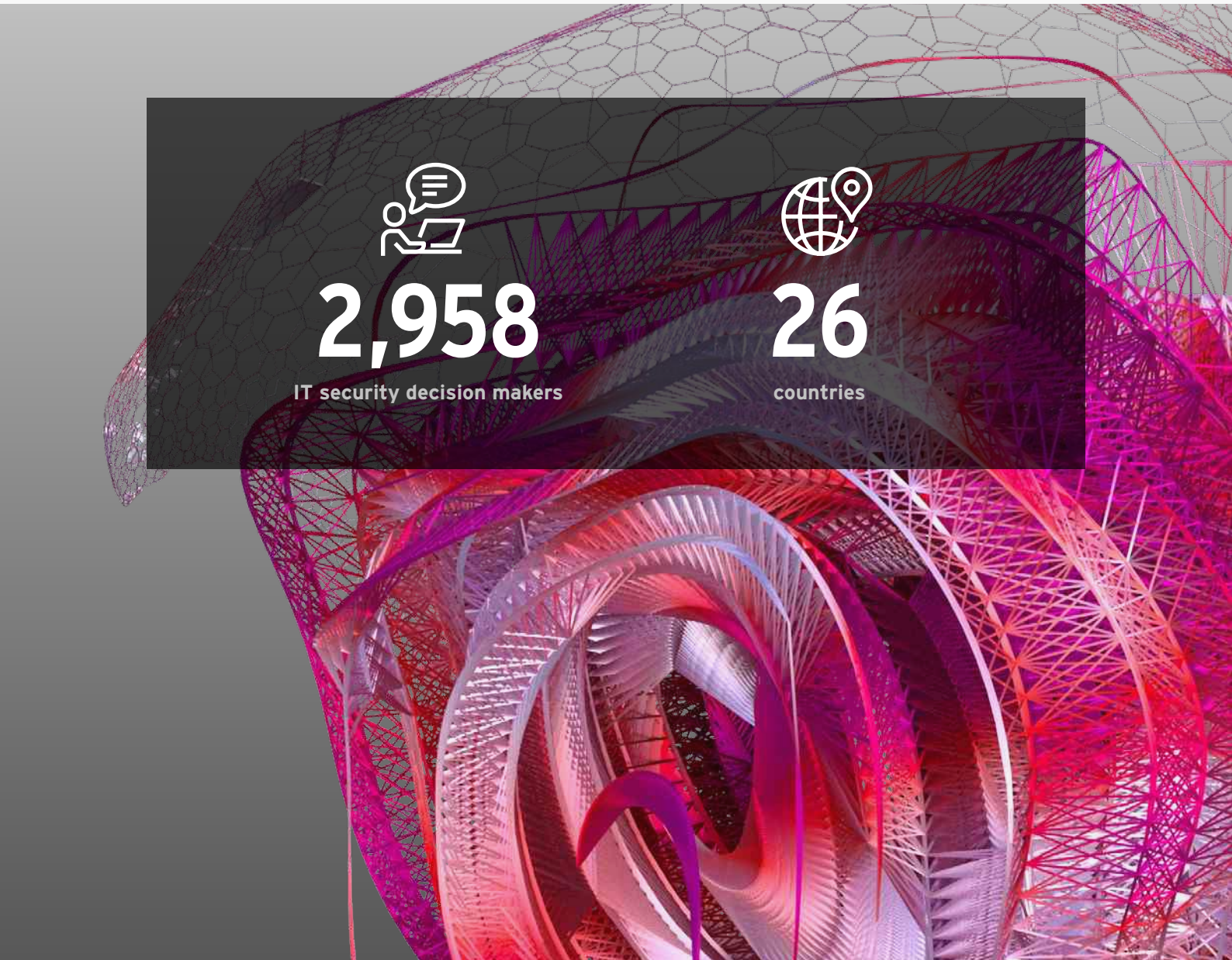
Introduction

Over the past two years, cyber has come to dominate boardroom risk calculations. That makes ransomware unquestionably the pre-eminent concern of IT and business leaders. A vast majority (87%) now view cyber compromise as a bigger threat than an economic downturn, with a fifth admitting that a serious attack in the past nearly sent their business into bankruptcy.

Their concerns are well founded. One analysis reveals a 105% surge in ransomware last year, with hundreds of millions of attacks detected. That's due in no small part to a surge in threats during the pandemic, which capitalised on digital investments and home working. Yet that's only part of the story.

The corporate attack surface is also increasingly distributed – across an extensive supply chain that spans cloud and software providers, professional services firms and other connected entities. Each one of these may have privileged network access or store sensitive information belonging to client organisations. Each one therefore represents a potential security risk which must be addressed. Yet too often supply chains are nebulous and ill-defined, with controls applied in a reactive and haphazard manner, if at all. This must change.

To find out more, Trend Micro commissioned Sapio Research to interview 2958 IT Decision Makers across 26 countries: UK, Belgium, Czech Republic, Netherlands, Spain, Sweden, Norway, Finland, Denmark, France, Germany, Switzerland, Austria, USA, Italy, Canada, Taiwan, Japan, Australia, India, Poland, Hong Kong, Mexico, Colombia, Chile, Brazil.



The ransomware epidemic

Ransomware has been with us for well over a decade. But it reached a nadir during the pandemic. As corporate attack surfaces expanded with digital investments, security controls were often dismissed in favour of productivity gains. Under-protected home workers and remote access infrastructure became an unwitting access point. It didn't help that many engaged in riskier behaviour at home than they would in the office.

At the same time, ransomware-as-a-service offerings attracted a new breed of affiliate groups into the sector, increasing the volume and variety of threats. Initial access brokers (IABs) often provide the entry point – whether via vulnerability exploitation, phishing attack or RDP compromise. Then the affiliates take over, using legitimate tooling to move laterally to find and exfiltrate data and deliver their ransomware payload. Major organisations are singled out in sophisticated "big game hunting" attacks while SMBs suffer in even greater numbers. Double, triple and even quadruple extortion have become commonplace ways to force payment. And some of the most aggressive groups like Conti and REvil make billions.

Ransomware is now present in 25% of data breaches, a 13% year-on-year increase. The volume of reports to the FBI, itself representing just the tip of the iceberg, jumped 109% from 2017 to 2021.

Ransomware is now present in

25%

of data breaches

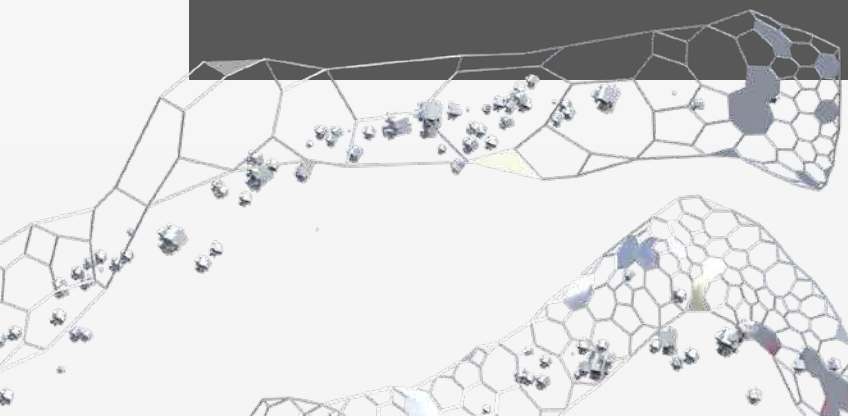
13%

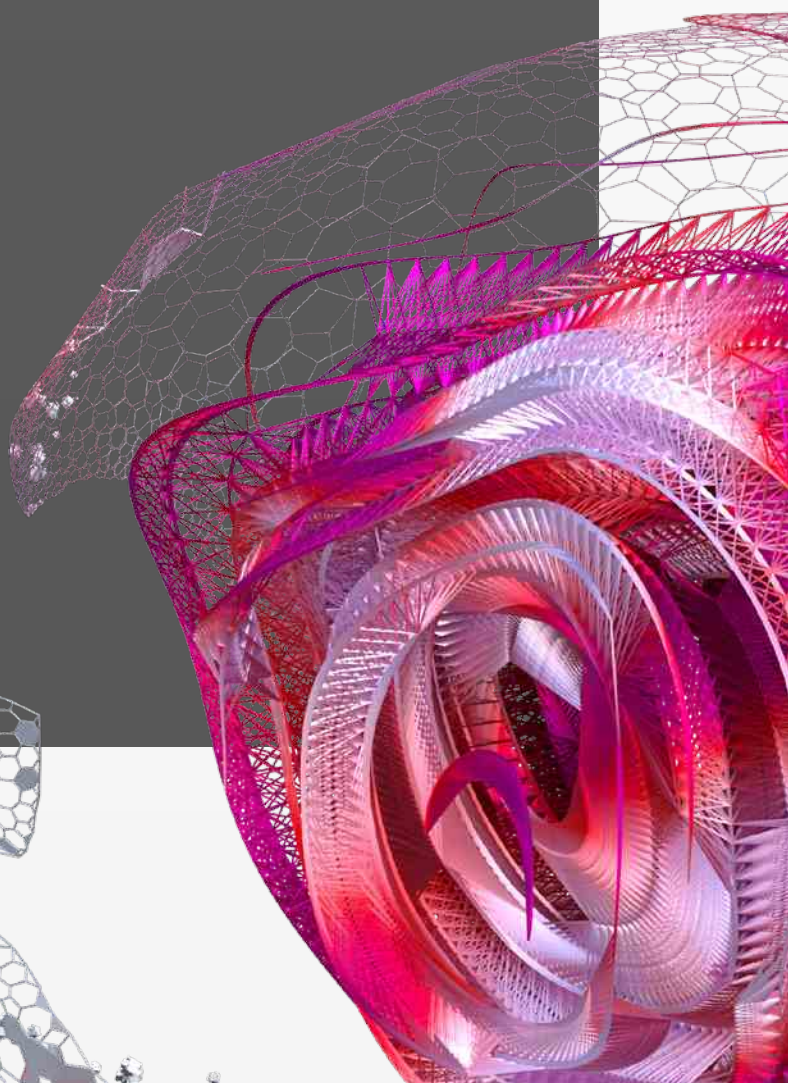
year-on-year increase

Jumped

109%

from 2017 to 2021





How bad is supply chain cyber risk?

This matters, because ransomware actors are always looking for a bigger pay-day. Supply chains are an attractive target because they can offer either a poorly defended access vector and/or an opportunity to multiply illicit profits by infecting many organisations through a single supplier.

Supply chains are a complex web of interdependent organisations. Many participants in these networks probably don't even realise how many suppliers, partners and contractors they have. They could be providers of IT hardware, software and services. They could be open source code repositories. They could even be non-digital suppliers ranging from law firms and accountants to building maintenance providers. Supply chain risk is everywhere.

Some examples of big-name supply chain breaches are instructive:

IT management software provider Kaseya was compromised in 2021. A sophisticated attack saw hackers exploit an internal software vulnerability to push out malicious updates to its MSP customers. They in turn infected downstream customers with ransomware. An estimated 1,500-2,000 organisations were impacted.

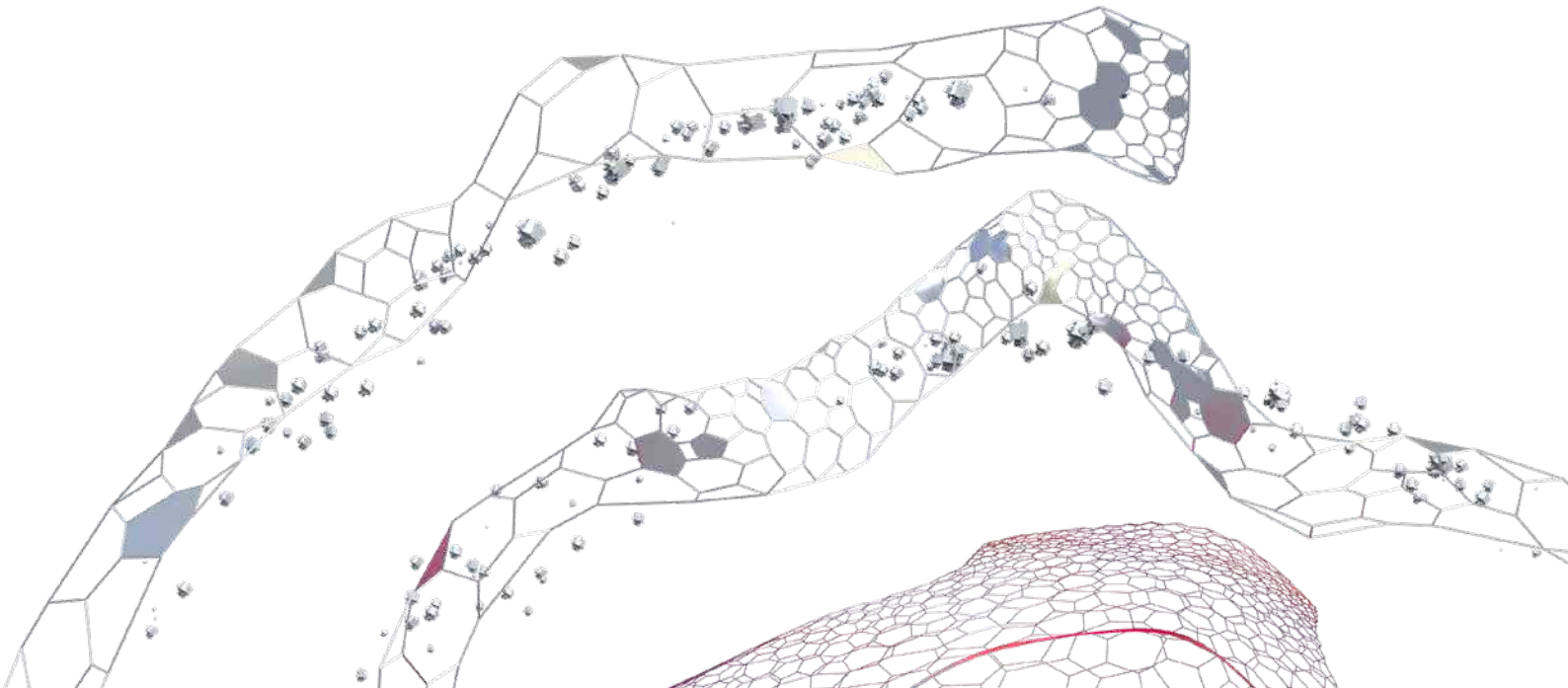
IT management vendor SolarWinds was hacked by state operatives in late 2020. Similar to the Kaseya incident, attackers used the firm's privileged access to customer networks to infect countless customers. Malware inserted into the Orion software was used to compromise at least nine US government departments.

A little-known HVAC company was compromised by a third-party back in 2013. They stole its access credentials for client Target, to access the US retail giant's IT systems and carry out one of the biggest card breaches ever seen.

The Log4Shell exploit highlighted ongoing challenges around the security of open source code and components. It's still causing problems for firms unable to comprehensively locate the presence of Log4j across their systems, due to complex software dependencies. Many DevOps teams use third-party components to accelerate time-to-market for their software. But these often introduce vulnerabilities or deliberately planted malware. According to a recent report, the average application development project contains 49 vulnerabilities spanning 80 direct dependencies, while 40% of bugs are found in indirect dependencies.

Not all of these examples involve ransomware. But they highlight the potential impact of supply chain compromise. The risk is real.

Against this backdrop, Trend Micro found that 79% of global IT leaders believe their partners and customers are making their own organisation a more attractive ransomware target. That's perhaps unsurprising, given that 52% of global organisations have a supply chain partner that has been hit by ransomware.



Sharing knowledge

The first stage to improving supply chain security is transparency around cyber risk. Yet only 47% of organisations we interviewed share knowledge about ransomware attacks with their suppliers. And 25% say they don't share potentially useful threat information with partners.

This could be because security teams don't have information to share in the first place. Detection rates were worryingly low for ransomware activities. Some of them are listed here:

- Ransomware payloads (63%)
- Use of legitimate tooling e.g., PSexec, Cobalt Strike (53%)
- Data exfiltration (49%)
- Initial access (42%)
- Lateral movement (31%)

Mitigating ransomware risk effectively should start at home. This would also help to prevent a scenario in which suppliers are contacted about breaches in order to pressure their partner organisations into paying up. We found that 67% of respondents which had been attacked in the past three years experienced this kind of blackmail to force payment.

So, absolutely start ransomware mitigation inside the firewall. But efforts shouldn't stop there. They must then extend to the wider supply chain to help reduce the risk from the third-party attack surface.

Building a safer supply chain

There's no silver bullet when it comes to reducing ransomware risk in the supply chain. Many of the usual best practices apply here. The key is first to gain a comprehensive understanding of the supply chain itself and corresponding data flows, so that high-risk suppliers can be identified. They should be regularly audited where possible against industry baseline standards. And similar checks should be enforced before onboarding new suppliers.

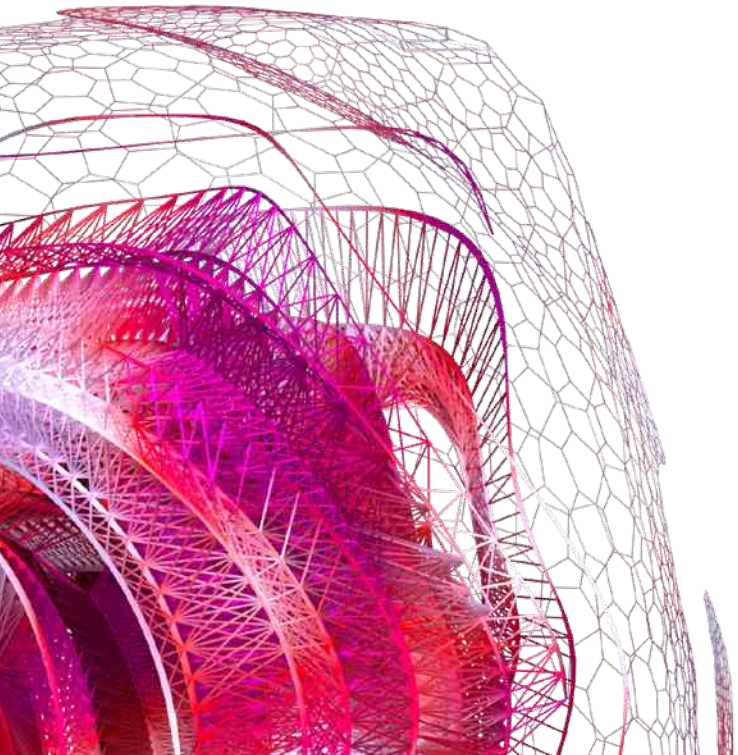
The below steps should ideally be followed by both supplier and client:

- Implement a policy of least privilege for all devices and services
- Use multi-factor authentication to protect sensitive information
- Scan open source components for vulnerabilities/malware before use and build into CI/CD pipelines
- Run XDR to spot and resolve threats before they can make an impact
- Apply comprehensive multi-layered protection at email, server, cloud, network, endpoint
- Run continuous risk-based patching and vulnerability management
- Run continuous user education programmes
- Back up regularly according to 3-2-1 rule
- Run attack surface management (ASM) tools
- Regularly perform penetration and vulnerability testing
- Regularly test incident response plans
- Apply data encryption at rest and in transit

Trend Micro can help with many of these critical security controls. Crucially, we deliver ASM and comprehensive protection, detection and response from a single platform: Trend Micro One. By delivering everything – from open source code scans to XDR – from a unified location, Trend Micro One can:

- Reduce the costs of managing multiple point solutions
- Eliminate the coverage gaps that can grow between siloed products
- Empower security teams to be more productive
- Enable customers to better understand their supply chain risk, and then take concrete steps to mitigate it

To find out more www.trendmicro.com



TREND MICRO™

Extended detection and response across multiple IT layers by Trend Micro. **Created with real data by artist Brendan Dawes**.