Ebook

WITH secure

Protecting the Supply Chain: **we’re all in this together**

In a complex, non-linear and modern supply chain network, one tiny mistake can have disastrous consequences. In 2021, the Russia-affiliated hacker collective REvil exploited two vulnerabilities to break into more than 50 managed services providers, each of which sat at the center of complex supply-chain networks. The attack then spread out across digital supply chains, using customer trust to breach critical systems.

The late 2021 attack on free, open source, Apache logging utility Log4j allowed attackers to remotely execute code. Log4j is one of the most popular tools for recording and collecting data on users and online behavior, having been downloaded millions of times. The Log4j attack has so far been linked to ransomware, cryptojacking, and numerous other incidents. Its long-term repercussions remain unknown.

“Something like Log4j has this ability to grow exponentially, which means it will take a long time before you're certain that your least risky applications have been checked and patched too, and not just your critical systems. It's something that will keep lurking in the background,” says an EMEA Chief Information Risk Officer at a multinational bank.

The supply chains of the past were relatively simple – raw materials came in, finished products went out; suppliers were upstream and customers were downstream. Today's supply chains are no longer linear. They consist of complex digitized processes and relationships between organizations of all sizes, arranged not like a single line of dominoes but like an interconnected pattern of thousands of them. Knock one of those dominoes over and we all know what happens next.

In effect, we are all downstream from each other in modern supply networks, because a security breach can come from any part of the ecosystem and spread in any direction, with repercussions that become more serious as they spread. That's what we call the butterfly effect.

So, how do we avoid the butterfly effect in today's complex and nonlinear supply chains, where the effects of a seemingly minor lapse in cybersecurity can be both wide-reaching and devastating? The key is to work together with every other organization involved in your supply chain, turning shared vulnerability into shared strength. The Elements cybersecurity platform from WithSecure™ can make this process a lot easier.

Protecting your endpoints

In this new world of remote work and personal devices, every person in your organization will have connections of their own, a network of overlapping networks. Any employee can be compromised at any point in their personal network. The effects of such a compromise can easily impact not only your organization but many others – a classic case of the butterfly effect.

No matter how much cybersecurity training you put in place, and no matter what policies you use, human error is always possible, whether that means opening an infected attachment or simply using a weak password. That's why you need an additional layer of security for endpoints, especially with your remote employees.

WithSecure™ Elements Endpoint Protection provides the extra security you need, protecting against known and zero-day ransomware and malware on all the computers, mobile devices, and servers used by your employees. It can be deployed from your browser and managed easily from a single console. WithSecure™ Elements Endpoint Protection includes automated patch management, keeping you up to date on all necessary patches.

By protecting all the endpoints in your organization, you also protect everyone else your employees are connected with – from suppliers to customers, both upstream and downstream. It's a clear example of shared strength rather than shared vulnerability.

Detecting and responding to threats

Everyone has heard of organized criminals, hacker collectives, and hostile states, and we are all familiar with phishing attacks, ransomware, trojans, viruses, malware, and data theft. These are words we hear every day, both at work and home.

However, opportunistic cybercriminals are increasingly looking for ways to exploit normal functionality or poorly configured systems – in other words, to be the butterfly on the sole of your shoe that goes unnoticed but changes everything.

That's why threat detection is a must for supply chain security.

"What something like EDR [endpoint detection and response] does is shine a flashlight on potential vectors of attack. It allows you to, as quickly as possible, detect and respond to a supply chain attack. EDR can be the difference between sinking and swimming in an incident scenario because it buys you the time to catch up," according to Jordan, Director of Consulting & Incident Response, WithSecure™.

Cloud platforms, shared services, remote working, and mobile devices have all expanded the IT perimeter far beyond the head office. This process had already begun before the pandemic, but definitely accelerated as a result of it.

As difficult as it is, it remains essential to map the perimeter if you want to stay on top of cyber threats, whether internal or external. According to IBM X-Force Threat Intelligence Index 2021, scanning for vulnerabilities has overtaken phishing as the most common attack vector for cybercriminals. This process can be automated, a fact that explains the soaring attack volumes on open-source and other code repositories. It also makes it even more important to understand what's happening on your perimeter.

Endpoint detection and response systems are no longer optional, but essential. WithSecure™ Elements Endpoint Detection and Response gives you instant visibility into your IT environment, allowing you to accurately assess your security status through a single pane of glass – and giving you expert guidance on how to effectively tackle threats as they arise.

WithSecure™ Elements Endpoint Detection and Response detects real threats accurately and quickly, allowing you to easily spot the difference between misuse and proper use, so you can respond effectively without the distractions of alert fatigue.

What does this mean for your supply chain network? If an attacker slips in, you'll be able to spot the incursion quickly and deal with it immediately. This not only protects you from threats that come to you from suppliers or customers, it also protects your suppliers and customers from being infected through you.

Managing vulnerability

It's common for IT and DevOps teams to reuse trusted code from outside sources, such as open-source code repositories. Unfortunately, attacks against popular code repositories have become extremely common since 2020. This type of attack is a direct assault on trust and collaboration between developers, because it can result in the contamination of trusted code. Cloud platforms, managed services, and utility applications are also under increasing attack.

How can you guard against this type of threat? First, you should only do business with suppliers who are vigilant about their cyber security. To determine whether a supplier is truly vigilant, you need to establish what permissions and policies they use. You need to know ahead of time how much of your organization's intellectual property and personally identifiable information they could potentially expose. You need to know whether your supplier employs their own security teams and consultants and whether they reward white-hat hackers for finding new vulnerabilities and exploits.

It's not enough to ask tough questions of your suppliers. You need to ask them of your own organization as well. Today's supply networks are thoroughly interconnected, so there's a constant risk of deploying a supplier's flawed code in your own products.

You need to know what open-source components your products contain, and you need to be sure that externally sourced code is secure before you use it. You also need to know whether your organization is good at patching vulnerabilities rapidly.

To remain secure, you have to extend your threat-modelling process to your own organization, asking yourself whether you might be part of the security problem.

Essentially, laying the groundwork is essential. "Some of the more sophisticated attacks in recent years have come from basic control weaknesses. Most successful attacks have been easy for the attacker to implement. People are doing lots of flash stuff, but not getting the basics right. You're making criminals' lives a hell of a lot easier if you haven't done the basics," says an EMEA Chief Information Risk Officer at a multinational bank.

WithSecure™ Elements Vulnerability Management minimizes your attack surface and your risk by scanning networks, endpoints, and systems to determine exactly where the most critical weak points are. It gives you a risk-based view of your whole attack surface, allowing you to find, prioritize, and fix vulnerabilities before they're exploited.

By proactively looking for weak points before you're attacked, you can make your organization a much harder target for cyber attackers. That's good news for you – and everyone else in your supply chain.

Protecting Collaboration

The more interconnected organizations are, the more they are exposed to collective risk. This includes companies with many subsidiaries, as well those that function within massive and complex supply networks.

This interconnectedness can mean shared weakness unless you make it into a shared strength. The more interconnected a supply chain is, the more its members must collaborate with each other to fight off security threats.

When you use collaboration platforms like Microsoft 365, it is your responsibility to protect the platform against advanced attacks. WithSecure™ Elements Collaboration Protection goes beyond Microsoft 365's native security features, keeping you and your supply chain protected against the most sophisticated phishing, malicious content, and targeted attacks.

Help and Guidance

The sooner you catch a cyberattack, the better off you are. Still, some situations are too challenging to be handled alone. This is where elite threat hunter investigation and response guidance is critical. Elevate to WithSecure™ is a 24/7 pay-as-you-go service that gives you the expert assistance you need to cope with the most challenging cybersecurity situations.

Conclusion

According to Jordan LaRose, WithSecure™'s Director of Consulting and Incident Response, "We are all more distributed these days, so it's harder for companies to enforce proper segmentation and proper network access. In technology terms, so many teams are moving to cloud-hosted platforms and weaker authentication solutions."

As companies and their supply chains become more distributed and more reliant on cloud platforms, cyber attackers will continue to look for weaknesses wherever they find them. From breaching an employee's personal laptop to compromising entire code repositories, cyber attackers are always looking for an opportunity.

Today's supply chain can be a confusing and often frightening place. The biggest danger isn't always from the loudest and most frightening attacker. In this environment, the safest course of action is to work together as a team. It is very much a case of 'all for one and one for all', and WithSecure™ Elements provides that platform to make sure the good guys always end up on the winning side.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.