Missing Piece secures a rapidly expanding environment with Cisco Secure

Contents

In an evolving threat landscape where cybercrime has become a big business, any organization, no matter how small, can be a target. For outsourced IT services company Missing Piece, a string of ransomware attacks was a call to action to adopt a comprehensive security approach. With an environment that includes 200 diverse customers at 250 locations across the Netherlands, the company needed an integrated security solution that not only provided robust defenses but also was simple and easy to manage.

Executive Summary	
Customer Name: Missing Piece **Industry:** Information Technology **Location:** Wijk bij Duurstede, Utrecht, the Netherlands **Number of Employees:** 50 serving 6000 users at nearly 250 locations	
Challenges	• Enable a unified approach to defend against evolving cyberthreats • Keep secure data of 200 customers based in 250 different locations across a distributed network • Automates correlation of threat information for faster investigations and scalable response • Improve the speed and efficiency of extended detection and response
Solutions	• Cisco SecureX (includes SecureX threat response) • Cisco Secure Endpoint • Cisco Secure Email • Cisco Secure Malware Analytics (Threat Grid)
Results	• Improved security operations efficiency, reducing workload by 20–30%. • Adopted a holistic approach to security. • Enhanced security posture with better understanding of risks and security priorities. • Blocked 4.6 million email threats in one month. • Stopped 500 endpoint threats and compromises in one month

Malware attacks are a call to action

The team at Missing Piece knew something was wrong when countless customer calls began rolling in. Back in 2016, ransomware was still an emerging threat, but when multiple customers experienced the same problem, the Netherlands-based managed services provider realized it had become a victim of a malware attack.

“We flew into action, even knowing that we were already too late,” recalls a Missing Piece security specialist. Luckily, the attack was low-level. Even so, many of the customers’ end users couldn’t work for several hours while the Missing Piece help desk cleaned up and restored their systems.

Then it happened again, more than once. That’s when Missing Piece understood it was time to find better protection for themselves and their customers. During a ransomware attack, the entire network and security team would be working until 11:00 in the evening or 1:00 in the morning—until they completed all the remediation. But that type of reactive approach was not sustainable.

Martin Kaszuba, information security officer at Missing Piece, calls those ransomware attacks a wake-up call.

With ransomware, cybercrime became a real business, and it’s not just making money off big organizations. There’s also money being made with small and medium businesses. Anyone can be a target, sometimes even by accident “

-Martin Kaszuba, Information Security officer at Missing Piece

The need for a holistic approach

Those ransomware attacks were a call to action for Missing Piece, which offers outsourced IT services to small and medium-sized businesses. An increased focus on security would provide additional value to customers as well as create an opportunity for business growth.

“The time you lose cleaning up and educating users is a huge drain because you’re not spending that time on growing your business, especially because the people you need to do the cleanup are the same people who would otherwise be building your IT and creating new services to provide,” Kaszuba explains.

To implement a comprehensive, robust approach to security, Missing Piece wanted solutions that could be tailored to its environment. The team also had to consider the requirements of customers. One of our challenges is that today, Missing Piece has close to 200 customers, each with different types of environments, policies, and security needs.

Adding to the challenge is that the customer base is primarily in highly regulated sectors such as financial services, accounting, and insurance. “We don’t just need to detect and block malware. We also have to have very deep visibility into everything happening on any device, anything going in and out of the environment, and transferring between servers,” Kaszuba says.

Missing Piece also needed security solutions that would integrate with the company’s existing tools.

"We didn't just want great email security and great endpoint security that didn't work together. We cannot have six different teams managing six different point solutions. We were looking for a holistic approach."

- Martin Kaszuba, Information Security officer at Missing Piece

Building a comprehensive, integrated security ecosystem

When the ransomware attacks hit, Missing Piece already had a longstanding relationship with Cisco, which included networking infrastructure as well as an existing deployment of Cisco Secure Email. Building off their successful partnership, Missing Piece chose Cisco as the preferred vendor for security. In the five years since those incidents foundationally shifted the company's approach to security, Missing Piece has worked to build a comprehensive security ecosystem that checked all those required boxes.

Today, the Missing Piece environment includes about 250 customer sites all around the Netherlands, along with two data centers. The organization relies on integrated Cisco Secure solutions—including Cisco Secure Endpoint and Cisco Secure Email—to protect that infrastructure as well as the emails and files of more than 6,000 users. "Integration, visibility, and all the other things we wanted—that's what we found in Cisco Secure solutions," Kaszuba says.

Cisco SecureX, a cloud-native, built-in platform that connects the Cisco Secure portfolio, offers additional value for Missing Piece's security investments.

"The biggest advantage of Cisco SecureX is that it combines all the separate tooling and monitoring aspects into a centralized platform. It not only simplifies security but also brings more transparency in what solutions you implement in your environment and for what reason, making it easier to provide a management report"

- Martin Kaszuba, Information Security officer at Missing Piece

Improved security, visibility, and efficiency with Cisco SecureX

Cisco SecureX enables organizations to connect their backend security architecture to a consistent front-end experience. With the SecureX platform, the Missing Piece team can quickly visualize threats across the environment, accelerate investigations, and respond to threats faster.

It took the organization less than 15 minutes to activate and configure the first integration in SecureX. In under two hours, the team had email and endpoint security added to the console, as well as the first dashboards.

The security team especially likes that the dashboard collects the data from across thworke customer environments and maps all the events, enabling the team to see lateral movement, exfiltration attacks, privilege escalation attempts, and other suspicious activities from one central location. "I could click on an event and immediately zoom in on what's happening there, instead of getting 40 or 50 different alerts," says one Missing Piece analyst. "With one screen, I can see what's going on anywhere, even with all the endpoints being scattered across the country and many people working from home."

Before deploying SecureX, Missing Piece struggled with event correlation, and gathering contextual information took days. “Now, we can do things in seconds—things we wouldn’t even have thought about doing two years ago. Back then, we didn’t think there would be anyone combining the different sources of information together and making it easy to correlate between what’s happening in the rest of the world and what’s happening in our environments,” the analyst says.

In another first, the Missing Piece team can now hunt for threats proactively, using the SecureX threat response application, rather than waiting for an alert. The security staff don’t have to log in to every server, check all the logs, and execute command lines to capture open ports. They can use a web interface and easily share their casebook with colleagues so they can join the investigation.

The Missing Piece team learned how to perform threat hunting in a workshop with Cisco experts. The workshops, offered globally in local languages, are hands-on sessions based on real-world scenarios. The participants receive a small piece of intelligence to investigate an incident using Cisco Secure solutions, and they have to determine how the incident took place. “The training also positions you to know how to stop the incident from happening again and how to be sure that you found everything that’s happened in your environment,” says one of the workshop participants.

The security team is not the only one using SecureX as a tool. For example, if a compliance officer wants to understand how well security is working, the officer can get those answers directly from SecureX. Without SecureX, the security team would either generate reports and email them, or give the compliance officer read-only access to different systems. With SecureX, they simply need to give the officer access to the dashboard, and all the officer has to do is click a button at the top to get all the information, whether that includes a specific day, week, or month.

The company can also share reports and insights with customers to help them understand their risk and maintain compliance with the ever-tightening regulatory frameworks. “The solutions we offer to customers are connected with our Cisco products, and we can see or track everything in the backend,” Kaszuba says. “We can monitor everything and show them how we’re meeting their needs.”

With the continuous 40 percent growth that Missing Piece has been seeing each year, the scalability of the Cisco solutions is among the key features that Kaszuba finds valuable. “Two of our biggest challenges are the diversity in products used to maintain control of the environment and the rapid growth of the environment. Integrating or building our security solution on top of Cisco infrastructure provides a form of scalability for our company.”

Keeping customers’ data and environments secure

When threats slip past defenses and enter an organization’s IT environment, understanding the scope of the problem is often a challenge. Without an identified root cause, including the method and point of entry, the threat may not be completely remediated, which means an infection may continue to spread. Before deploying Cisco solutions, Missing Piece frequently faced this concern. “I could clean viruses all day, but I want to stop them from coming into my network. If I don’t know how it got in or got on a machine, it’s going to happen again in 10 minutes, or the next day, or next week,” says one analyst.

Now, Cisco Secure Endpoint gives the security team those capabilities. Secure Endpoint offers a robust set of preventive mechanisms to stop threats at their earliest points and the ability to monitor and detect advanced threats. The solution includes features such as forensics, dynamic analysis, and retrospective visibility. “You’re feeling a bit like a private investigator who uses those pins and bits of string to connect all the dots,” Kaszuba says. “You can take a step back and see the exact picture—what came from where,

what goes to where, where it all started, and what endpoints are affected. And with a single click, you can isolate an infected endpoint so you can remediate without the problem getting worse."

Additionally, the Orbital Advanced Search capability in Cisco Secure Endpoint enables the team to run various endpoint queries. They can select the endpoints and choose what kind of information they want—and that baselining helps them understand if suspicious activity is taking place in their environment.

Missing Piece relies on Cisco Secure Endpoint for vulnerability management as well. For example, if someone installs an older version of software, Secure Endpoint sends an alert that the software is running, along with a link to the Common Vulnerability scoring system. In just one month, Missing Piece received alerts about 200 instances of out-of-date software.

Another technology, Cisco Secure Malware Analytics, protects against new malware by automatically analyzing the behavior of unknown, suspect files in a sandbox. "If someone receives a suspicious file via email at 4:00 in the morning or inserts a USB stick, downloading the file and opening it on an endpoint, the automated malware analysis can issue a verdict that the file is malicious and the endpoint will be quarantined," Kaszuba says.

He notes that deploying Cisco Secure Endpoint was easy, and as soon as the connector is installed, the data begins flowing into the dashboard. And the extensive documentation—which comes with every Cisco Secure product—doesn't leave any questions unanswered.

The integration between Cisco Secure Endpoint and Cisco Secure Email also means that when a threat is detected and blocked in one solution, it's automatically blocked everywhere. This is especially important because Missing Piece uses Secure Email to protect both its on-premises and online environments. Kaszuba says, "We use it for outgoing email as well, which protects our customers' name and their brand."

Creating a secure environment that customers can trust

Within just one recent month, Cisco Secure Email blocked 4.6 million threats and Cisco Secure Endpoint stopped 500 threats and compromises in the Missing Piece environment. But it's not just those types of results that prove that the security solutions are working. Before Cisco, some staff would easily spend 10 hours worrying whether they missed anything and double-checking the data. Now they can get the complete picture of their environment in 10 minutes.

The return on investment from implementing SecureX includes streamlined and simplified security operations.

"Cisco SecureX has really increased the efficiency of the organization's security operations. We've reduced our workload by 20–30 percent just from being able to focus on the important things."

– Martin Kaszuba, Information Security officer at Missing Piece

One of the most-important outcomes for Missing Piece after implementing Cisco Secure solutions is the adoption of a more comprehensive security approach. Additionally, the insights that Cisco SecureX and the integrated architecture provide enable the company to better understand its risks. "Based on the output of the dashboards and the reports, we can better prioritize the things we need to change and optimize in our organization," Kaszuba says. "Having these insights gives us better clarity about risk and an additional set

of eyes into the environment to optimize the security posture—perhaps at levels that I initially wouldn't have thought to cover."

Cisco also plays an instrumental role in helping Missing Piece maintain customer assurance. "We can show our customers that we offer a secure environment so that they can trust us with their data," Kaszuba says. "And we can also use all the reports for auditing to show what we're checking and blocking and how we're securing complications with other parties."

Kazsuba notes that Cisco's value doesn't only come from the robust solutions, but from the support and resources that Cisco offers to customers as well—even to smaller companies like Missing Piece. "Our Cisco support team knows the country we're operating in and all the regulations we have. And the tech support is also brilliant. With security especially, being able to dial a number or open a chat 24/7 is very important. You log a case and somebody immediately begins looking out for you and helping you understand the problem."

Added value from the Cisco Secure community and partnership

Cisco's support for customers extends to education and professional development, including a networking community called Cisco Gateway. Through the Gateway, customers can connect both with Cisco internal experts and with peers from other organizations. "You can just fire your questions at someone and get answers back and immediate interaction with someone who really knows the product," according to a Missing Piece lead who participated in the program.

Through the Gateway, community members globally stay abreast of what's happening both within Cisco and throughout the industry. They can also ask the Gateway community about their experience with specific Cisco solutions or security problems. The professionals who participate in the program often face the same challenges, and they freely share their experiences and problem solutions with each other.

Just as important for Missing Piece is to have a security partner who's continuously innovating and looking to the future.

"Cisco is an industry leader and therefore is always on the front line of the ever-evolving threat landscape. Cisco can provide solutions for pending threats, or at least an indication for how to approach possible risk in the future. For me, that is definitely the most beneficial thing to have in a dedicated partnership."

- Martin Kaszuba, Information Security officer at Missing Piece

Product List

Cisco SecureX (includes SecureX threat response)
Cisco Secure Endpoint
Cisco Secure Email
Cisco Secure Malware Analytics (Threat Grid)

Learn More

Achieve simplicity, visibility, and efficiency thanks Cisco SecureX. Visit www.cisco.com/go/securex