MIDWEST RUBBER SECURES A GLOBAL SAAS WORKPLACE WITH CHECK POINT

MIDWEST RUBBER

Industry
Manufacturing

Challenge

- Protect customer and internal data and maintain regulatory compliance
- Protect SaaS users from malware, phishing, and malicious attacks
- Simplify management complexity

Solution

- Check Point CloudGuard SaaS
- Check Point SandBlast Agent

Results

- Gained comprehensive protection for public cloud (SaaS) applications
- Ensured compliance for globalmanufacturing sites
- Extended advanced threat protection to endpoint devices

"I feel more comfortable using SaaS applications in the cloud with CloudGuard SaaS, because I know that I can protect them. It's a great piece of technology that we can use—and support a more mobile workforce because of it."

—Brandon Pelinka, I.T. Manager, Midwest Rubber Service & Supply Company

Overview

Midwest Rubber Service & Supply Company

Midwest Rubber Service & Supply Company manufactures, fabricates and distributes high quality rubber products. Founded in 1976, the company provides belting and conveyor products for food, paper, packaging, and distribution industries, as well as the global floor care industry. The firm is based in Plymouth, Minnesota, with additional sites in the Netherlands and China.

Business Challenges

Securing a Global, Cloud-Powered Manufacturing Organization

Despite its name, Midwest Rubber is very much a global organization, with operations spanning three continents and customers worldwide. This innovative manufacturer relies on cloud-based SaaS applications to stay agile and keep costs in line. Midwest Rubber relies on its Microsoft Office 365 applications to help users stay productive, in the office and on the go,as well as Microsoft Dynamics 365 Business Central cloud ERP. Its servers reside on Microsoft Azure, and the company also supports its multinational operations on a Citrix digital workspace environment. With so much data moving between sites, endpoints, and in the cloud, maintaining pervasive security is a top business imperative.

"Check Point SandBlast Agent really helps, because if a user goes to download any malicious document, or a document that they think is not malicious, it downloads it and extracts it in the cloud without requiring the user to do it,"

—Brandon Pelinka, I.T. Manager,

"We strive to protect our customers' data, our proprietary data, and all of our research," said Pelinka. "It's a big security concern. We also have sites in China, which has its own distinct requirements, as well as in the Netherlands, with General Data Protection Regulation (GDPR) compliance concerns that we have to follow."
Pelinka and his IT team needed a security solution that could safeguard its employees SaaS accounts, as well as protect users' endpoints from phishing, malware, and other threats—while ensuring compliance with local regulations.

Solution

Check Point Delivers Purpose-Built SaaS and Endpoint Protection

After considering a variety of options, Pelinka determined that he needed a solution built specifically to protect enterprise SaaS environments. He deployed Check Point CloudGuard SaaS, a cloud service that blocks attacks intended to steal data on SaaS applications and cloud email Much more than a Cloud Access Security Broker (CASB), it provides not only deep visibility, but complete protection against malware and zero-days, sophisticated phishing attacks, as well as hijacking of employee SaaS accounts. CloudGuard SaaS is the only security solution to prevent attacks on enterprise SaaS applications and block cybercriminals from taking over employee' SaaS accounts with a unique Identity Protection technology. "We have had no viruses or other security issues since we've implemented Check Point," said Pelinka. "CloudGuard SaaS really helps us protect our Office 365 environment."

A Layered Approach to Endpoint Security

Check Point SandBlast Agent extends advanced threat prevention to endpoint devices to defend against zero-day and targeted threats. It captures and automatically analyzes complete forensics data, to give Pelinka and his team the actionable insight and context to quickly remediate attacks in the event of a breach. "Check Point SandBlast Agent really helps, because if a user goes to download any malicious document, or a document that they think is not malicious, it downloads it and extracts it in the cloud without requiring the user to do it," said Pelinka. "If the file is malicious, SandBlast Agent will scrub it and send down a clean version. It's great to have another layer of security protection for our endpoints. The rollout was very easy, and the solution is extremely effective." Check Point SandBlast lets Pelinka and his team apply a Zero Trust approach to thwart phishing attacks. "The Zero Trust capability has been really huge," said Pelinka. "When our users are on any Web site and they go to put their credentials in, the phishing capability of SandBlast Agent checks and scans the username and password to make sure that it's not a malicious site, and help ensure they don't put corporate credentials in. That's important for us, because a lot of our users tend to reuse passwords on multiple sites." To provide an additional layer of endpoint protection, Pelinka deployed Check Point Full Disk Encryption (FDE), which delivers transparent security for all information on all endpoint drives, including user data, operating system files, and even temporary and erased files.

"Having the SandBlast Agent on our endpoints has greatly reduced the amount of time we have to spend to clean machines and remove malware or viruses,"

—Brandon Pelinka, I.T. Manager, Midwest Rubber Service & Supply

"Having Check Point's full disk encryption and being able to essentially manage it from one spot made me feel confident about ensuring that all of our devices, including mobile devices, were GDPR and PCI compliant," said Pelinka. "Having Check Point checks all the security boxes that are required for regional compliance."

Results

Empowering a Global Workforce with Secure Cloud Agility

With Check Point CloudGuard SaaS, Midwest Rubber has gained the confidence in knowing that its SaaS users can stay productive, without worrying about account takeovers, unknown logins, or access from unknown regions. Instead of worrying about security, users can focus on their primary job responsibilities. "We've been using CloudGuard SaaS for roughly seven months, and since deploying it I've seen lots of email and shadow IT threats blocked," said Pelinka. "The ability for me to be able to gain visibility into what people are doing with their work accounts, and avoid possible data loss, has been huge."

Secure Endpoints Reduces IT Workload

Check Point SandBlast Agent helps keep employees safe from today's increasingly sophisticated endpoint threats. Its automated, non-intrusive approach protects users against zero-day threats, stopping issues at the point of entry. That means IT have more time to focus on other tasks, instead of troubleshooting laptop or desktop issues. "Having the SandBlast Agent on our endpoints has greatly reduced the amount of time we have to spend to clean machines and remove malware or viruses," said Pelinka. and help ensure they don't put corporate credentials in. That's important for us, because a lot of our users tend to reuse passwords on multiple sites." To provide an additional layer of endpoint protection, Pelinka deployed Check Point Full Disk Encryption (FDE), which delivers transparent security for all information on all endpoint drives, including user data, operating system files, and even temporary and erased files. "Having Check Point's full disk encryption and being able to essentially manage it from one spot made me feel confident about ensuring that all of our devices, including mobile devices, were GDPR and PCI compliant," said Pelinka. "Having Check Point checks all the security boxes that are required for regional compliance."

Providing Relevant, Actionable Management Data

Offered as a cloud service, Check Point CloudGuard SaaS lets Pelinka centralize monitoring via an intuitive web portal that provides instant visibility, presented in a way that's easy to use and understand. "CloudGuard SaaS has helped our IT team reduce alert fatigue by providing alerts that actually mean something to us,"explained Pelinka. "The solution provides a dashboard that presents plenty of good data on a single pane of glass. We can see everything we need to see when we log in. The most important things are in our face right away, so if we need to deal with an issue, we can do it."

A Secure, Flexible Cloud Foundation for the Future

With its CloudGuard SaaS solution in place, Midwest Rubber has gained the pervasive security and management insights it needs to support innovative cloud solutions with confidence. The manufacturer is looking forward to deploying new capabilities as the solution matures in the years ahead. "Check Point is continually enhancing their technology, and the new features they introduce each year make me happy that we made CloudGuard SaaS our security solution of choice," said Pelinka.

For more information, visit: https://www.checkpoint.com/products/