Control Southern Engineers Cyber Protection Across All Fronts with Check Point

Check Point Infinity architecture protects the company everywhere against next-generation mega-cyber attacks

CONTROL SOUTHERN

Customer Profile

Control Southern sells and supports industrial controls and safety systems

Challenge

- Prevent ransomware, zero-day and phishing attacks via network, endpoint and SaaS applications
- Keep endpoints updated correctly
- Reduce manual steps and increase visibility

Solution

- Check Point Infinity architecture, including CloudGuard SaaS, CloudGuard IaaS, Next Generation Security Gateways, SandBlast Network, SandBlast Agent, and R80.20 Security Management

Benefits

- Stopped thousands of previously undetected phishing emails
- Identified instances of anomalous logins, spoofed emails, and shadow IT
- Accelerated log monitoring and simplified management

> "What we've been able to secure with Check Point Infinity is fantastic. It's the best cyber security architecture and protection I've ever worked with, hands down."
>
> — David Severcool, Manager, IT Infrastructure and Security, Control Southern

Overview

Control Southern

Control Southern has been a trusted automation partner for process industries in the Southeastern United States for more than 50 years. It is an Emerson Impact Partner, providing local access to global Emerson engineering services and expertise. Industrial customers across market segments rely on Control Southern automation, engineering, monitoring, valve and instrumentation, and training services to maximize production performance and efficiency.

Business Challenge

Fighting Back Against Gen V Threats

As the company's firewalls were reaching end of life, the Control Southern IT team began seeing a growing number of multi-vector attacks targeting its network and endpoints. Malware, phishing, and larger-scale infections had outstripped the capabilities of the company's existing Sophos platform, and it needed costly hardware upgrades. When Control Southern moved to Office 365, it experienced a tremendous influx of phishing attacks on its endpoints. Then, ransomware gained access through malware on a web browser, infecting servers and spreading to connected client computers. In just a few minutes, gigabytes of data were encrypted and inaccessible.

David Severcool, Manager of IT Infrastructure and Security for Control Southern, and his team removed and remediated the infected computers and restored files from backup, but ransomware hit two more times during the same week. The team discovered that the McAfee software on endpoints was not updating systems correctly. Now they had the additional burden of manually pushing updates to endpoints almost every day.

"As we began looking for better protection, we wanted the best platform out there," said Severcool. "We wanted a next-generation firewall, unified threat management, management capabilities from a single pane of glass, and logging. It was a tall order."

> "No one else could match the logging, visibility, or protection that the Check Point Infinity architecture provided."
>
> — David Severcool, Manager, IT Infrastructure and Security, Control Southern

Solution

Far Above and Beyond

The Control Southern team evaluated Barracuda, Check Point, Cisco, and Sophos solutions. However, Severcool knew that Control Southern needed next-generation protection across all attack surfaces—network, endpoints, and cloud deployments. The team also wanted unified threat intelligence to detect Gen V threats and single-pane-of-glass visibility to preempt them. As they evaluated Check Point CloudGuard SaaS, they immediately found several infections in SharePoint and OneDrive, and Office 365 email. The findings made their choice easy. The team chose Check Point Infinity and its unifying architecture.

"We needed more protection for Office 365," said Severcool. "The company had experienced serious email phishing campaigns after moving to Office 365. When an attacker gained access to our email address list through one of our partner companies, phishing emails spread like wildfire. Check Point CloudGuard SaaS solved that problem, protecting Office 365 as well as our SharePoint and OneDrive environments."

CloudGuard SaaS provides Threat Emulation capabilities to sandbox and analyze suspicious emails and files, as well as Threat Extraction to ensure that clean files are delivered to end users. Control Southern also deployed Check Point Security Appliances with threat prevention and SandBlast Zero-Day Protection across its locations. The company replaced the McAfee endpoint solution with the Check Point SandBlast Agent endpoint suite for comprehensive protection against bots, exploits, ransomware, and malware. SandBlast Agent also provides application control, endpoint compliance, endpoint firewall, and remote access VPN capabilities.

Deployment was fast and easy. Check Point Infinity Architecture enables Check Point CloudGuard SaaS and all other Check Point solutions to work in harmony, delivering Gen V cybersecurity defense. Check Point R80.20 Cyber Security Management gave Severcool and his team complete visibility into their infrastructure and policies. With all management capabilities and logging in one place, they have up-to-the-minute full threat visibility.

"No one else could match the logging, visibility, or protection that the Check Point Infinity architecture provided," said Severcool. "Check Point was far above and beyond everything else we evaluated."

"In the first three months of using Check Point CloudGuard SaaS, we prevented and recorded more than 1,100 incidents."

— David Severcool, Manager, IT Infrastructure and Security, Control Southern

Benefits

Proactive Prevention

Check Point CloudGuard SaaS not only stops targeted attacks, it also enables the team to see exactly what's going on so that they can take action. Even before Control Southern fully deployed Check Point CloudGuard SaaS in prevention mode, it found phishing emails that otherwise would have been undetected. It found infected files on SharePoint and OneDrive, and it identified users whose email addresses had been compromised and were being spoofed.

For example, the "anomalies" feature of Check Point CloudGuard SaaS alerted the team to an odd login from a user who doesn't leave the state of Georgia. It appeared that he had logged in from Nigeria. The team knew that his account had been breached and quickly reset his password, avoiding any repercussions.

Check Point CloudGuard SaaS also identified instances of "shadow IT"—applications that users had installed for sharing files. Now the team knows which third-party applications are deployed on users' systems and how they are being used. If Check Point alerts the team to large file transfers being downloaded or uploaded, they can investigate and identify any potential insider threats from succeeding.

"In the first three months of using Check Point CloudGuard SaaS, we prevented and recorded more than 1,100 incidents," said Severcool. "We can immediately remediate infections and we've seen Check Point CloudGuard SaaS block attacks that prey on application vulnerabilities that we didn't know we had."

Keeping An Eye on Everything

Control Southern gained unprecedented control and visibility into activity and policy in a single console with Check Point R80.20 Cyber Security Management. SmartEvent correlates millions of logs for a single view into security risks, enabling the team to see significant events easily and understand security status and trends.

"Check Point R80.20 is clean and easy to navigate," said Severcool. "I can see everything in a single pane of glass and don't have to bounce around between applications. The logging is fantastic—nothing else we looked at even came close."

Next Step: Up

Control Southern is rolling out Check Point CloudGuard Public IaaS for Azure to protect applications as they are migrated to the public cloud. It will enable the team to automatically keep assets and data protected across cloud and on premises environments.

"I was a big fan of other solutions in the past," said Severcool, "but what we've been able to secure with Check Point Infinity is fantastic. It's the best cyber security architecture and protection I've ever worked with, hands down."

For more information, visit:
www.checkpoint.com/architecture/infinity/