splunk> turn data into doing™

CASE STUDY

Cyber Security Software Maker Check Point gains in-depth intelligence with Splunk

Key Challenges

Check Point wanted to derive more meaningful insights from diverse data sets so it could improve operations and effectiveness whilst mitigating threats.

Key Results

Splunk provides real-time insight into business operations and allows Check Point to ensure staff and systems stay one step ahead even for unforeseen events such as remote working during the pandemic.

Check Point SOFTWARE TECHNOLOGIES LTD

Industry: Technology

Solutions: Security

How does a security software company secure its own systems?

Check Point creates cyber security solutions that helps over 100,000 businesses of all sizes. When it comes to safeguarding its own systems and staff of 5,400 employees, Check Point holds itself to the highest standards. It wanted to derive more meaningful insights from the terabytes of data its systems collected daily to better understand its business and ensure the security of its entire operation.

Faster, smarter investigations and effective threat prevention

When Check Point set up a security operations center to improve accountability for protecting the organization, it chose Splunk Enterprise Security. Splunk can ingest all of the many data formats Check Point uses and works with all of the technologies it relies on.

"We're a data-driven company," says Jony Fischbein, global chief information security officer at Check Point. "The main challenge was aggregating the huge amounts of data we collected and converting it into useful information."

Only 17 days after migrating to Splunk, Check Point began to see benefits like increased threat awareness and faster security investigations, compared to its previous security information and events management tool.

Splunk's dashboards help Check Point visualize the current state of its systems, and automated alerts notify them of any malicious activity or network vulnerabilities. Fischbein says Splunk also allows his team to quickly and effectively investigate potential harmful issues — such as developers taking source code out of the office, or a new vulnerability appearing in a product they use — before they can cause any damage.

"We now know what to investigate and whether we've solved the problem. And not just because someone has a gut feeling about it. The data shows us for certain," says Fischbein.

Data-Driven Outcomes

5x
faster security investigations

17
days to migrate to Splunk

100%
of remote workforce compliant with new Covid-19 security policy

Working safely and securely through the pandemic

Splunk's ability to derive meaningful insights from data also helped Check Point work safely and productively during the COVID-19 pandemic.

When an employee tested positive for COVID-19, Check Point's IT team used Splunk to track staff access badges and identify the exposure level and identify which employees had contact with them in the previous 14 days. At-risk workers were notified immediately and told to work from home and self-isolate.

"We couldn't have done this with another solution," says Fischbein.

Splunk also helped Check Point secure remote work during the pandemic. When leadership set new security measures for working from home, Splunk revealed which employees were complying, and within two weeks, Fischbein was able to show the CEO that they had achieved 100% security compliance. "This really drove home the value of using Splunk to the leadership team. The data proved that staff were secure and productive when working from home."

> We're a data-driven company. The main challenge is aggregating the huge amounts of data we collect and converting it into useful information."
>
> **Jony Fischbein,** Global Chief Information Security Officer, Check Point

With staff working remotely, Check Point also used Splunk to discover and mitigate security risks, such as a developer using a BYOD laptop to access the dark web and a finance team member giving another staff member access to their work laptop. Once made aware of these issues, managers instructed staff to follow policies to keep company data and sensitive information protected.

> We know what to investigate now and if we've solved the problem. And not just because someone has a gut feeling about it. The data shows us for certain."
>
> **Jony Fischbein,** Global Chief Information Security Officer, Check Point

Growing for the future with Splunk

Check Point has been pleased with the benefits of Splunk that it's planning to expand its usage.

"We don't want a solution that only helps us with what we need today. We want help with things we don't know we want to do yet, in six months or a year's time," says Fischbein. "We found that with Splunk, it grows with us."

Check Point plans to take advantage of Splunk's ability to automate tasks such as isolating a potentially vulnerable device and improving employees' secrets management. It's also finding ways for staff beyond the SOC to use Splunk like help desk staff learning to identify alerts on which they can take action.

"With Splunk, we have eyes on our whole organization," says Fischbein. "It's also very valuable for everything we do."

21-19735-Splunk-Tier2-Check Point-CS-101