> "Most [employees] are unaware that [Cb Defense] is even running. That's unheard of."
>
> - Grant Stavely, Senior Security Engineer, Evernote

EVERNOTE

INDUSTRY

Mobile and Web Application

COMPANY SIZE

300+ employees

SECURITY CHALLENGES

Required better security on endpoints

Wanted to protect remote users

No impact to developers

PRODUCT

Cb Defense

KEY BENEFITS

Visibility across the whole environment

Lightweight sensor

Zero interference with business operations

SUCCESS STORY

Evernote Replaces Traditional AV with Cb Defense

SUMMARY

Like the elephant portrayed in its gray and green logo, Evernote never forgets.

With more than 100 million users worldwide, the Evernote multi-platform, cloud-based workspace empowers people to collect, store, organize, share, and access all the digital details of their work lives, creative projects and family activities in one place and from any device.

"We encourage customers to capture in Evernote all the content that's important to them," says Grant Stavely, senior security engineer at the company, which is based in Redwood City, California. "And we make some pretty strong promises about how we protect their information from being accessed or compromised."

BEFORE CARBON BLACK

In mid-2014, Evernote recognized that, while its service was secure, the company's endpoint-security capabilities did not offer sufficient visibility and protection for its widely dispersed workforce.

"Roughly two-thirds of our 320 employees are involved in development," says Stavely. "We are very careful about restricting developers' access to production systems and user data. But if an attacker manages to compromise a developer's system and then uses it to inject code into source control–and the tainted code slips through the internal review process–attacker code could end up running on production systems. That's unacceptable."

Evernote also wanted to enhance endpoint security for employees who work remotely, and for its satellite offices in Austin, Zurich, Tokyo and Beijing.

THE RESEARCH

Stavely's team evaluated a number of malware detection products before selecting the Cb Defense solution. First, they looked at network content detonation and decided it wasn't worth the expense. "These solutions require heavy appliances, and with so many employees working at home, we were asking ourselves, 'How do we scale it?' It didn't make sense financially," he says. In addition, the most mature products were Windows-focused. Because Evernote is almost exclusively a Mac shop, the company would have to deploy products in beta, a compromise Stavely was not willing to make.

Next, the team looked at host solutions to complement network security monitoring. They disregarded one widely deployed product because of a negative experience Stavely had with the vendor while working at a different company. “It had so many stoppers, we had to uninstall it,” he said. Evernote tested a different host solution only to discover that employees’ laptops were running hot, the fans were turning on (consuming yet more power), and batteries were quickly being drained.

> “Cb Defense (formerly Confer) is an excellent complement to network security monitoring. It logs executables and other activity in a way that is uniquely able to provide context for other systems.
>
> - Grant Stavely, Senior Security Engineer, Evernote

THE SOLUTION

Undeterred by these disappointments, Evernote next evaluated Cb Defense and found that it had none of these shortcomings. Cb Defense’s cloud-based management solution provides advanced endpoint detection, prevention and incident response with visibility across the whole environment, including remote sites and mobile workers.

“Cb Defense is an excellent complement to network security monitoring,” says Stavely. “It logs executables and other activity in a way that is uniquely able to provide context for other systems. If my network security monitoring system alerts about something that is happening, I can go look at the host and see what process was responsible for that activity, without requiring a level of monitoring that is intrusive or burdensome for employees.”

Cb Defense’s lightweight footprint consumes less than 1% of CPU and collects and transfers far less data than competing solutions. This ensures a non-disruptive experience, even for Evernote developers, who are technically astute and often very demanding. “Most [employees] are unaware that [Cb Defense] is even running, he adds, That’s unheard of.”

THE RESULT

Cb Defense has allowed Stavely to streamline many of his duties. “If I wake up and see an alert on my phone from something that happened overnight, I can pivot directly into Cb Defense and immediately know what happened, with a level of fidelity that didn’t exist before.” Cb Defense also eliminates the constant care and feeding that anti-virus products require. In addition, analysts can “turn up the knob” to more closely track suspect activity, and can quickly identify and discard false positives.

He further cites a pleasant surprise he discovered after deploying the Cb Defense solution. “We are mindful of employee privacy and want to be able to audit whether an analyst is abusing their access to employee activity records in tools like Cb Defense,” said Stavely. “Every security monitoring platform has this problem, but most offer only a basic ‘blame log.’ Carbon Black is the first vendor to demonstrate that they not only understand this requirement but can actually provide the visibility we require.”

Disclaimer: Carbon Black acquired Confer, which is now Cb Defense as part of their endpoint security platform.

ABOUT CARBON BLACK

Carbon Black has designed the most complete next-gen endpoint security platform, enabling organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 600 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute’s Best of 2015 Awards.

CARBON
BLACK
ARM YOUR ENDPOINTS