OFS Prevents Breaches with Expert Threat Validation

Family-owned, community-driven company OFS provides contract furniture and logistical solutions to various markets worldwide. Rooted in a strong foundation of sustainability and craftsmanship, each department within the company takes those values seriously in their day-to-day operations, especially Security Technology Administrator Jeremy Wilkins. With the help of VMware Carbon Black Cloud™, Wilkins has been able to transform and improve OFS' back-end technology with a security-centric focus, enabling the company to confidently and swiftly deliver their products and services.

A complete replacement

The OFS team needed a solution that would help Wilkins do his job, not add more effort to it. OFS previously used Symantec Endpoint Protection, which constantly ran scans and hindered performance. With a solution that bogged down the network whenever virus updates needed to be pushed, Wilkins determined it was time to take aggressive action in evaluating a new security solution. With the help of partner CDW Logistics and research from the Gartner's Magic Quadrant, OFS found three vendors to test, considering deployment, time to value, interface and ease of use. VMware Carbon Black performed top of the tier in every category.

After evaluating VMware Carbon Black, Wilkins realized that with Symantec, "a full on-premises legacy AV solution, it was a nightmare to deploy, update, maintain and act on alerts. But a lot of the struggle was it just didn't do what VMware Carbon Black does." As a result, OFS fully replaced Symantec with VMware Carbon Black Cloud.

Significant time savings

Since using VMware Carbon Black, the time spent responding to alerts and malware has decreased significantly. "Our time to value with your product was almost instantaneous. I'm spending less time tracking down false positives, and spending more time triaging and acting on legitimate threats. We don't bog down our internal network with legacy virus updates," says Wilkins on the value of VMware Carbon Black.

INDUSTRY
Retail

COMPANY SIZE
1,001–5,000 employees

SECURITY CHALLENGES
- Traditional antivirus (AV) bogged down the network
- Solution difficult to maintain and act on alerts

PRODUCT
- VMware Carbon Black Cloud Endpoint™ Standard
- VMware Carbon Black® Cloud Managed Detection™

KEY BENEFITS
- Better alignment with executives through clear reports
- Reduced remediation time

vmware® Carbon Black

Expert threat validation

VMware Carbon Black Cloud Managed Detection provides OFS with the expert threat validation their leadership team needs. Carbon Black Cloud Managed Detection reports provide valuable information that Wilkins and team are able to easily comb over, prioritize and forward to their security executives. "Our leadership team loves all of the Carbon Black Cloud Managed Detection content. They love seeing the different OS versions on the report and top trending users who were hitting the report," says Wilkins. Carbon Black Cloud Managed Detection has been very valuable as Wilkins is able to determine what exactly he needs to focus on, and not waste time or resources on less important alerts and tasks.

Remediation in 30 minutes or Less

Recently, the team had an incident with a weaponized Microsoft Word document. A file was received via email and shared internally with another user. Both users extracted the weaponized document and allowed macros, prompting the document to attempt to open a command interpreter. VMware Carbon Black immediately terminated the process, saved both endpoints and alerted Wilkins on the incident. As Wilkins recalls, it was 30 minutes or less from incident to closure. "I was able to blacklist the file hash and delete the file from both endpoints from the VMware Carbon Black dashboard. I got the alert, I triaged it and I called both users. I didn't get out of my chair… and I slept like a baby that night."

Conclusion

With VMware Carbon Black following his lead, Wilkins can now dedicate more time on legitimate threats and less on the false positives, and feel confident knowing VMware Carbon Black has his back in protecting the OFS environment.

"Our leadership team loves all the Carbon Black Cloud Managed Detection content. They love seeing the different OS versions on the report and top trending users who were hitting the report."

JEREMY WILKINS
SECURITY TECHNOLOGY ADMINISTRATOR, OFS

Discover more companies who have partnered with VMware Carbon Black. Visit:

https://www.carbonblack.com/why-cb/customer-success/

vmware® Carbon Black