CUSTOMER STORY

COFENSE UNIFIES AND IMPROVES ENDPOINT MANAGEMENT IN THE CLOUD

COFENSE
Power of the Collective

INDUSTRY

TECHNOLOGY

LOCATION

LEESBURG, VIRGINIA

KEY CHALLENGES

- Support cloud-only services, with no traditional on-premises services
- Provide an excellent user experience for more than 500 remote workers
- Eliminate high-touch deployment and maintenance for IT
- Manage Windows 10 and macOS devices with a single platform

SOLUTION

To improve IT efficiency and user experiences for its mostly remote workforce, Cofense deployed VMware Workspace ONE, an integrated platform powered by VMware AirWatch unified endpoint management technology. By managing Windows 10 and macOS devices with a single platform, the company reduces costs, improves security, and reclaims hundreds of hours a year in productivity.

According to Cofense, more than 90 percent of data breaches can be attributed to successful phishing campaigns—targeted attacks that fool an otherwise trustworthy employee into revealing sensitive information. Rather than blaming employees as the root cause, Cofense's philosophy is that employees can be empowered to strengthen an organization's defenses and gather real-time intelligence to stop attacks as they happen.

To source top-notch global security talent, Cofense's workforce is primarily remote—in fact, most of the company's 550 employees, consultants, and contractors work remotely. To improve efficiency and security, and provide an excellent user experience, Cofense unifies endpoint management across Windows 10 and Mac devices with VMware Workspace ONE™ powered by VMware AirWatch® technology.

Cofense saw a real opportunity in leveraging the everyday employee in the fight against phishing. Today, Cofense is the leading provider of phishing threat management for organizations concerned about human susceptibility and response to advanced targeted attacks.

The Challenge

All Cofense employees receive a company-owned laptop so they can be productive on the go. About half of the users receive HP Windows 10–based machines for business productivity. The other half use Macs for software development and creative work.

Until recently, Cofense's device deployment and management processes varied by platform. Building Windows-based machines took the IT department up to three days, after which the laptop was shipped out to the user. Mac users configured and updated their own machines, giving IT limited control. In addition, Cofense's Simulator and Triage services require employees' workstations to follow SOC 2 Type 1 controls, which requires the enforcement and auditing of cross-platform security policies.

"We needed a tool that would allow us to deploy new systems and software quickly, and enforce policies across both Windows 10 and macOS platforms," says Mark Zigadlo, vice president of IT at Cofense. "We're a cloud-only company, so we needed a cloud-based solution."

BUSINESS BENEFITS

- Delivering an out-of-box experience to users with zero IT involvement
- Reclaiming weeks of user productivity and hundreds of hours for IT in just one year
- Improving security and compliance with patching and policy enforcement
- Reducing endpoint management costs with a unified system

The Solution

Cofense evaluated several endpoint management solutions, including IBM MaaS360, Panorama9, and Workspace ONE. Early on, it was clear that Workspace ONE provided the best cross-platform support.

"We ran into quirks and limitations with other endpoint management tools that we just didn't experience with VMware," says Zigadlo. "Workspace ONE is easy to get started with, and provides all the functionality we need to manage our mixed fleet of Windows 10 and macOS workstations. In our experience, Workspace ONE works equally well with both platforms."

Workspace ONE works with Microsoft Azure Active Directory's mobile device management enrollment and Apple's Device Enrollment Program to streamline setup. New devices get automatically enrolled into Workspace ONE when Windows-based devices are joined to Azure Active Directory. Once the laptops are deployed, it's easy for Cofense to verify and enforce the use of hard drive encryption policies, screen lock timeouts with password re-entry, and malware protection software.

Although most of Cofense's data center infrastructure is in the public cloud, the company uses on-premises VMware vSphere® data center virtualization for product development. They can replicate customer environments for testing, quality assurance (QA), and malware analysis. Cofense relies heavily on VMware Fusion® and VMware Workstation Pro™ for research and development. To stay current and enhance manageability, Cofense upgraded to vSphere 6.5 Enterprise and uses VMware vRealize® Operations™ for capacity optimization. Cofense also uses vSphere to build and QA its Cofense Triage solution as a virtual appliance, offering customers faster deployment.

"Most of our customers use VMware, so it makes sense for us to use the latest version of vSphere in our testing," says Zigadlo. "We also appreciate the new vCenter Server Appliance and HTML5-based vSphere client included in vSphere 6.5. We have a large population of macOS users, so having a web-based client is very helpful."

Business Results and Benefits

Cofense nearly doubled its workforce in just one year, onboarding approximately 250 new employees. Having Workspace ONE in place saved approximately 625 hours for IT in configuration time alone, significantly reducing endpoint management costs. New employees can be productive immediately upon hire instead of waiting days for a computer with needed applications and data access.

"With Workspace ONE, we can have a laptop ready with all security policies in less than half a day. It can be shipped off to an employee, who can start using it as early as the next day," says Zigadlo. "That capability will be even more valuable as we continue to globalize our workforce and continue to refine a true out-of-the-box service delivery model."

In situations where an employee experiences laptop issues without physically damaged hardware, Cofense's IT staff can connect to end-user devices remotely to aid in troubleshooting and perform maintenance. IT staff can even remotely reimage a machine, if required. By putting employees back to work faster and minimizing long periods of end-user downtime, Cofense reclaims weeks of productivity every year.

> "VMware Workspace ONE is easy to use and provides all the functionality we need to manage our mixed fleet of Windows 10 and macOS workstations. In our experience, Workspace ONE works equally well with both platforms."

MARK ZIGADLO
VICE PRESIDENT OF IT
COFENSE

VMWARE FOOTPRINT

- VMware Workspace ONE
- VMware vSphere with Operations Management™ 6.5
- VMware Fusion 10
- VMware Workstation Pro 12

APPLICATIONS VIRTUALIZED

- Test/QA environment

PLATFORM

- Windows 10
- macOS

Workspace ONE also improves security, allowing Cofense to verify that needed patches have been applied, proactively push out patches faster, and verify that the company's control objectives are being met. "As a security company, we take endpoint security and compliance very seriously, and AirWatch technology helps us keep our laptops healthy and compliant," says Zigadlo.

Looking Ahead

As Cofense identifies new ways of empowering its global remote workforce, it is considering using Workspace ONE for enterprise mobility management to support secure BYOD. The company's goals for Workspace ONE include integrating Simple Certificate Enrollment Protocol (SCEP) with a third-party certificate authority to strengthen email security and machine and device authentication. Windows AutoPilot will enable easy onboarding of Windows devices, managed by Workspace ONE. Cofense also intends to implement conditional access and compliance policies with Workspace ONE, providing more granular security policies.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com