Customer
Case Study

Rentokil Initial Launches Hybrid Security Operations Center to Support Workforce

Rentokil Initial is a leading pest control and commercial hygiene and wellbeing services provider. The company has more than 36,000 employees working in 1,800 teams across more than 80 countries.

Industry

Business Services

Strategic priorities

- Anywhere Workspace

VMware footprint

- VMware® Carbon Black Cloud™
  - Endpoint™ Standard
  - Vulnerability Management™
  - Audit and Remediation™
  - Enterprise EDR™
  - Managed Detection™
- VMware Workspace ONE®
  - Workspace ONE Intelligence™
- VMware Professional Services

Rentokil Initial is a leading global hygiene and pest control company with a large mobile workforce and a distributed IT estate. To enable both office staff and field employees to work securely from anywhere, the company turned to VMware to deploy VMware Workspace ONE and VMware Carbon Black Cloud in its hybrid security operations center. This enabled the company to gain greater control over its devices, reducing the threat of cyberattacks while working toward a Zero Trust security model.

"Work from anywhere" increases flexibility

At Rentokil Initial, the FTSE 100 company's office-based staff organizes mobile teams to visit customer workplaces and perform services such as specialist disinfection following an outbreak of illness. It also offers commercial fumigation to eliminate pests from holding containers, public transport or premises, and LED light technology to protect offices from flying insects.

To support its "work from anywhere" strategy, field staff use mobile devices, including printers, so they can update records and print paperwork for customers on location. Locating logistics in the field helps employees operate more efficiently, reduces vehicle emissions and eliminates paper processes.

> "The VMware security model perfectly aligns with our requirements and VMware Carbon Black Cloud has all the functionality needed to combat the ever-increasing sophistication of modern cyberthreats."
>
> Pete Shorney, Global Head of Information Security, Rentokil Initial

Strengthening security through consistent device management

With a large global workforce and a history of growth by acquisition, Rentokil had a widely dispersed IT estate. The company lacked an enterprise approach to device management and endpoint security. Approximately 60 percent of staff operate remotely, but when the COVID-19 pandemic forced Rentokil office staff to work from home, the IT team needed to provide highly available, secure access to technology quickly.

Although the company uses Google Workspace technology almost exclusively, company-owned devices run on a variety of operating systems on both fixed and mobile technologies. This complex environment includes approximately 13,500 Microsoft Windows desktops, 25,000 Microsoft Windows laptops, 6,000 Google Chromebooks and more than 30,000 Android devices, with 3,500 servers keeping systems running behind the scenes.

The greatest security threat to any business is human error. Every device needs to be actively protected to reduce the risk of a security breach, so users need comprehensive training in enterprise security. Companies that fail to provide adequate protection face a storm of negative media attention and fines if customer data is compromised, not to mention the painful process of rebuilding trust in their brand.

"Complex environments aren't just time-consuming to manage, they can actively increase the security risk to the business by increasing the attack surface, and any cyberattack on our company could have a major impact on business continuity and our reputation," explains Pete Shorney, global head of information security at Rentokil Initial.

The company launched an initiative to enhance its security posture and a more consistent approach to manage workplace devices. This involved replacing legacy antivirus software and centralizing device management for greater visibility of the apps staff used. To understand employee behavior, the team defined three user personas with varying awareness of security: the most cautious team members who keep security top of mind, the more relaxed persona who believes IT should protect staff from a cyberattack, and those unable to visualize what constitutes risk. The team also wanted a more proactive approach to identify and mitigate security risks, including granting conditional access to devices.

"Enabling staff to work from anywhere was a priority predating the pandemic, but we needed to urgently scale and unlock central visibility of our device estate," says Shorney. "Without a standard approach, it was much harder to see which apps people were using and impossible to identify where we were potentially vulnerable to cyberattacks."

Hybrid SOC standardizes security

To enhance its security strategy, Rentokil turned to VMware, its trusted partner of more than 13 years. Over the course of this partnership, Rentokil has leveraged VMware technology and expertise to fuel digital transformation ranging from smarter, more cost-effective storage, to establishing a company-wide network with greater bandwidth, smoother app deployment and data center management.

Collaborating with VMware Professional Services, the team designed a plan to deliver greater control, enhanced application security and a standard approach to device management outside the Rentokil network. The plan expanded and accelerated an ongoing rollout of VMware Carbon Black Cloud and VMware Workspace ONE, which VMware Professional Services delivered for 13,000 users.

"VMware Professional Services helped us configure the integration between Workspace ONE Intelligence and Carbon Black Cloud to obtain threat insights and extend threat remediation with Custom Connector and the Workspace ONE Intelligence Automation Engine," says Shorney.

> "VMware Professional Services helped us configure the integration between Workspace ONE Intelligence and VMware Carbon Black Cloud to obtain threat insights and extend threat remediation with Custom Connector and the Workspace ONE Intelligence Automation engine."
>
> Pete Shorney, Global Head of Information Security, Rentokil Initial

Rentokil purchased VMware Workspace Security Platinum, which combines the endpoint management and analytics of Workspace ONE with device protection and behavioral analytics from Carbon Black Cloud to protect users from modern cyberattacks. This also helps identify staff who need training on how actions like clicking on unverified links in emails can download malware onto their devices.

"Our users who are most likely to fall for a cyberattack don't understand what high risk behavior looks like, but VMware Carbon Black Cloud gives us such a granular level of visibility that we can actively show people where they've clicked on a suspicious link, for example," Shorney says. "It really brings cybersecurity to life when we can show people what not to do instead of just telling them."

This helps the organization strengthen security, with the VMware security model aligning to the team's requirements. VMware Carbon Black Cloud creates a standard approach to endpoint security across all user groups and devices, with all the functionality needed to support a Zero Trust framework. This allowed Rentokil to set up a hybrid security operations center (SOC) with a new team of first- and second-line responders.

The SOC monitors the device estate from a single pane of glass to actively identify and mitigate any potential threats. The level of interoperability afforded by VMware technology means the company isn't tied to any one vendor for security, which is crucial for the hybrid SOC model.

"Our hybrid security operations center works really well on VMware technology. With the help of VMware Professional Services, we've moved from being reactive to proactive, stopping attempted attacks before they get anywhere near our users and cause disruption," says Shorney.

Transitioning towards a Zero Trust environment

As Rentokil continues its optimization journey, its hybrid SOC is reducing the risks of ransomware attacks and malware, crucial for protecting business operations. "VMware Carbon Black Cloud is simply a great product. Up to 95 percent of threats have been blocked from entering our systems, and the others were identified and dealt with quickly," explains Shorney. "With central visibility of the threat landscape we can respond much faster and isolate infected or at-risk machines in minutes before the malware can do any damage."

Now, threats are caught before they can infect more devices on the network, minimizing disruption to staff and safeguarding business continuity. Whether in the office, working from home or out in the field, employees can deliver seamless services to customers securely.

The team is exploring how to enhance identity management to establish a Zero Trust environment, enabling employees to bring their own devices. This will provide users greater freedom to use the devices that best support their individual working styles.

"The VMware team has been brilliant. We have ongoing bi-weekly meetings to make sure we're realizing the full value and benefits of our VMware products," says Shorney. "We're undergoing a wider cloud transformation at Rentokil, and knowing that we can seamlessly scale up strict levels of security with VMware Carbon Black Cloud is a huge win for the team and means we can focus on high-value tasks."

> "VMware Carbon Black Cloud is simply a great product. Up to 95 percent of threats have been blocked from entering our systems, and the others were identified and dealt with quickly."
>
> Pete Shorney, Global Head of Information Security, Rentokil Initial