VMware Workspace Security

USE CASES

UTILIZE A ZERO TRUST APPROACH TO SECURITY

Deliver an always verify, never trust approach to security through combined device management and trust, intelligence-based conditional access, and threat detection and response.

SECURELY SUPPORT WORK-FROM-HOME INITIATIVES

Enable secure access from corporate or employee-owned devices to software-as-a-service (SaaS), mobile, web and virtualized apps and desktops supported by next-generation antivirus (NGAV) and threat response and remediation.

CONSOLIDATE ENDPOINT AGENTS AND SECURITY VENDORS

Reduce the number of point product agents and vendors across device lifecycle management, mobile device management and endpoint security.

Security has never been easy. In today's dynamic environment of users, applications, endpoints and networks, security solutions have become more complex and siloed. And while investments in security increase, vulnerabilities and breaches continue to grow exponentially. Annually, these security incidents cost each organization an average of $2.79 million.[1] Studies show that most enterprises see more than 10,000 alerts per day, while 27 percent of IT professionals report receiving more than 1 million cyberattacks.[2]

Security and IT organizations must fundamentally change the way they approach security

Meanwhile, the security landscape is constantly evolving. The rate of change in the way people work, driven by the need to work remotely, has exacerbated IT and security concerns. New work expectations have redefined priorities for the technology teams that support them. These redefined concerns include:

- Remote, flexible workstyles
- Heterogeneous environments across corporate and employee-owned devices
- Proliferation of cloud technology providing ubiquitous and diverse business apps

Security doesn't need another point product, it needs a new approach. Most of the focus over the past decade has been on the threats—identifying and responding to different types of attacks, and then adding additional products or agents to address those threat vectors.

VMware believes that the way forward lies in combining endpoint management with intelligence and endpoint security. Hardening the infrastructure enables us to leverage unique control points, and gain better visibility to detect, identify and prevent threats. VMware calls this intrinsic security because it's focused on leveraging existing infrastructure across any app, any cloud and any device to provide unique capabilities to secure your business.

VMware Workspace Security™ combines the endpoint management and analytics of Workspace ONE® with the endpoint protection and behavioral analysis provided by VMware Carbon Black Cloud™ to deliver on the intrinsic security vision.

Leveraging the power of big data, VMware Workspace Security provides comprehensive endpoint visibility and actionable insights in conjunction with data-driven prevention technology through a single dashboard. VMware Workspace Security provides both compliance and threat analytics to drive actions through its automation engine or through real-time query tools to remediate threats.

1. IBM Security and Ponemon Institute. "Cost of Insider Threats: Global Report." 2020.
2. Cybint. "15 Alarming Cyber Security Facts and Stats." Devon Milkovich. June 20, 2020.

KEY CAPABILITIES

CONTEXT AND COMPLIANCE

Provides a complete and contextual view into configurations and events taking place across the entire digital workspace

THREAT DETECTION AND PREVENTION

Detects modern malware and behavioral threats using continuous and adaptive monitoring, plus automated remediation for rapid mitigation response

CONSOLIDATION

Provides a single, cloud-based solution for Sec Ops and IT Ops, helping reduce complexity and improve overall performance

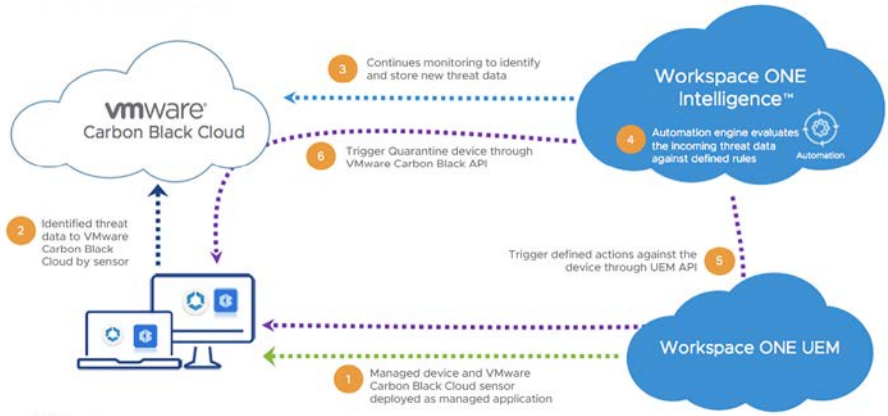

FIGURE 1: Workspace ONE Intelligence and VMware Carbon Black Cloud integration.

Built on a unified cloud platform, organizations can quickly reap benefits, such as:

- Fully investigate and contain attacks on any networks
- Expand protection globally without new architectural design requirements
- Improve attacker analytics with each new customer as more data is analyzed
- Get deeper insights into device compliance and security threats to drive a unified response by combining the management and security of endpoints
- Reduce costs and IT burden to manage multiple solutions by eliminating multiple security point products
- Enable coordinated response to security events across IT and infosec teams to reduce team silos
- Reduce alert fatigue generated by multiple, overlapping security vendors/tools that lack integration

How it works

Workspace ONE integrates access control, application management and multi-platform endpoint management into a single platform to streamline IT processes while providing an excellent user experience.

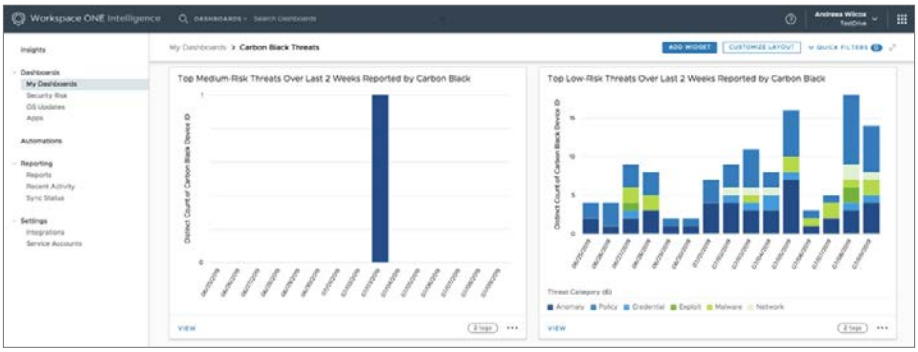

FIGURE 2: Workspace ONE and Carbon Black Cloud Integration.

To learn more, visit *vmware.com/security/workspace-security*.

CONTACT US

For more information or to purchase VMware Carbon Black products, please call 855-525-2489 in the U.S. or +44-118-908-2374 in EMEA.

The VMware Carbon Black Cloud NGAV sensor can be automatically and silently installed when an endpoint is enrolled in Workspace ONE Intelligence. Once the sensor is installed, the process of collecting and sending comprehensive endpoint telemetry data to VMware Carbon Black Cloud begins. Through advanced behavioral analytics, the VMware Carbon Black Cloud NGAV detects suspicious or malicious behavior and generates alerts.

Workspace ONE Intelligence polls the VMware Carbon Black Cloud via API for new alerts and notifications. It then ingests that data into Workspace ONE Intelligence for correlation with data from Workspace ONE or Workspace ONE Trust Network partners to generate data and valuable insights or automated actions. Customers can also choose to deploy audit capabilities that provide real-time query capabilities for further investigation and remediation of security threats.

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