FEATURE OVERVIEW

Risk-Prioritized Vulnerability Assessment

Before and After — For vSphere Administrators

INTRINSIC SECURITY VISION

Intrinsic security is all about bringing the right data at the right time to the right user, all in a consistent and actionable fashion. VMware Carbon Black Cloud Workload is a testament to our Intrinsic Security vision.

We are delivering capabilities that give the vSphere Admin faster and easier access to the data necessary to identify risk, harden systems, and reduce the attack surface.

Vulnerability management is a foundational element to harden and protect an organization’s workloads and infrastructure. But it’s not about finding the most vulnerabilities — it’s about finding the right ones, at the right time, and in front of the right people — so we can best operationalize the patching process, collaborate with security teams and address the risks that threaten our infrastructure. But existing solutions do little to address these fundamentals.

Before: The Challenge of Vulnerability Scanning

Today, security teams periodically scan their environment for vulnerabilities. Infrastructure teams are handed a long list of vulnerabilities to patch. This, often quarterly process, frustrates infrastructure and security teams alike. It is both operationally inefficient and ineffective, leading organizations to harbor massive unnecessary risk and operational burden.

Organizations simply aren't getting the right data, with the right context, fast enough, to the teams that run the infrastructure. As a result;

1. **There's not enough context** to effectively prioritize this work, so time is wasted on smaller risk items while vulnerabilities with active exploits are left open.
2. **Vulnerabilities are left unpatched** for long periods of time, leaving the organization unnecessarily exposed to ransomware and other forms attacks.
3. **We saddle the infrastructure team with technical debt** they must work through each quarter - when they are already overtaxed with ever-expanding responsibilities.
4. **The information comes far too late** to identify vulnerabilities that are caused by inappropriate changes to the workloads.
5. **The entire process is taxing on the infrastructure itself**. More agents. More network scans. More consoles and security products to manage.

It is a huge missed opportunity. Fixing this problem could have the most significant impact on reducing an organization’s workload risk. It reduces operational burden, and it could dramatically improve the collaboration between IT and InfoSec teams.

After: Implementing the Vulnerability Assessment

VMware Carbon Black Cloud Workload makes it easy for Infrastructure teams to keep their environment patched and hardened with far greater efficiency, effectiveness and focus on the biggest risks. With the new Vulnerability Assessment functionality now available directly in the vSphere Client, you can see and instantly prioritize vulnerabilities, allowing you to effectively reduce risk, speed up workflows, and cut down the cost of administration.

The new Vulnerability Assessment capability inside vCenter changes everything:

1. **Get a prioritized view of vulnerabilities** – not just on CVE scores, but whether there are real-world exploits. An organization might find thousands of vulnerabilities with a CVE score of 5. The Vulnerability Assessment capabilities inside the vSphere Client offer a more focused, prioritized list of vulnerabilities combined with the right source data to understand what to fix, how to fix it, and why. Proven data science techniques apply machine learning and natural language processing to uniquely curated and customized threat datasets. As a result, you can focus on the items that represent the greatest risk.

2. **Greatly speed up patching** because you don't wait weeks or months for a scan — you see vulnerabilities as they occur. We understand vSphere Administrators need to keep the infrastructure up-and-running, and are mandated to patch many vulnerabilities quickly. This capability allows you to maximize uptime while securing your infrastructure effectively.

3. **Greatly reduce technical debt** — and focus on a few critical vulnerabilities per day, not a thousand at the end of the quarter. Save time and money as you become more efficient by only focusing on the vulnerabilities that matter, as prioritized by VMware Carbon Black's integration with Kenna Security. In a TechValidate survey[1], fifty-five percent (55%) of organizations using Kenna Security's Risk Scoring cut their time spent investigating vulnerabilities by more than half.

4. **Get to the root cause** of operational issues causing risk. Because you see vulnerabilities as they occur, you can see when workloads are being changed inappropriately by someone into a vulnerable state. And because both the InfoSec team and the Infrastructure team see these vulnerabilities in their respective console, the teams stay in sync and have common "ground truth". This enables far greater collaboration between teams. A shared view of the data leads to faster resolution!

5. **Seamlessly incorporate vulnerability and lifecycle management into your daily operations**, with no scanning required and no agents to manage — so it's far less taxing on the infrastructure. Our native vSphere integration provides a single page of glass with the vulnerability data you need right at your fingertips, and easier management to reduce the burden on the Infrastructure team. You get exactly the same data as the security team, and can either work to apply patches by priority, or take alternate measures such as powering down non-critical but vulnerable systems.

Just the Beginning

The VMware Carbon Black team is committed to leading the Cloud Workload Protection space and delivering new security capabilities to protect any workload; whether physical, virtual, cloud, or container. We are focused on delivering the Intrinsic Security vision through low impact, built-in security solutions that support the full lifecycle of modern workloads, and unifying Security and IT teams to accelerate the process of identifying risk, prevention, detection, and response to threats with the right context and insights.

[1] *Source: TechValidate survey of 135 customers of Kenna Security - Published: Nov. 1, 2019 TVID: E0D-8B7-70D*

VULNERABILITY ASSESSMENT KEY VALUES

- **Prioritized:** Focus on critical vulnerabilities that pose a real risk to maximize uptime.
- **Scanless:** Leverage the data we collect in the cloud to gain immediate visibility.
- **Built-in:** Native vSphere integration provides a single pane of glass.

LEARN MORE

Workload Essentials Free Trial
carbonblack.com/workload-free-trial

VMware Carbon Black Cloud Workload
carbonblack.com/products/vmware-carbon-black-cloud-workload

Vulnerability Risk Scoring
carbonblack.com/resources/understanding-the-kenna-security-vulnerability-risk-score