Sharing the Workload of Workload Security

How to operationalize and simplify for security teams and IT admins

vmware®

Table of contents

Introduction 3
Security teams need the help of IT operations to secure workloads 3
The challenge 4
Workloads have become a finger-pointing vulnerability 4
Four steps to operationalize and simplify workload security 5
Step 1: Minimize agent overhead 5
Step 2: Share visibility into vulnerabilities 5
Step 3: Automate risk prioritization 6
Step 4: Streamline workload processes 6
What's next? 7
Aligning IT on workload security reduces attacks 7
Learn more 7

Introduction

Security teams need the help of IT operations to secure workloads

IT admins and security teams both play their parts to keep systems secure, but in relative isolation of each other. However, the transition to cloud environments for applications and workloads is forcing a change in how these roles are executed.

Security teams within an organization tend to be composed of policy and audit groups as well as threat hunting and incident response teams. The day-to-day burden of security and compliance falls on the IT operations staff and resources that aren't necessarily security oriented. In fact, according to a Forrester Consulting Spotlight report, only 33 percent of organizations have IT and security as one unified team today, but 47 percent believe unification will be the norm in three to five years.[1] There is no better time for a new approach that facilitates cohesion between these teams.

This white paper covers the key constructs to enable both security and IT teams to proactively reduce the attack surface and harden assets. Adopting these constructs will bridge the gap between these teams, simplify operations, and share the workload of workload security.

KEY CONSTRUCT	DESCRIPTION
Minimize agent overhead	Eliminating the need to install agents onto workloads reduces security agent sprawl, minimizes installation and reboots, and reduces operational overhead. This simplifies the delivery of security as a service for IT.
Share visibility into vulnerabilities	A unified view of security data ensures clear communication and understanding as to the vulnerabilities detected.
Automate risk prioritization	To minimize alert fatigue and overworked resources, both teams need to know what to focus on to make the biggest impact on defenses. Having a context-centric system that can automatically prioritize vulnerabilities without bias is critical.
Streamline workload processes	With shared visibility and risk prioritization, security and IT teams enjoy a frictionless experience through automation and operationalizing consistent security as part of IT hygiene.

TABLE 1: Four key constructs to reduce the attack surface and harden assets.

1. Forrester Consulting, commissioned by VMware. "Security As A Team Sport: A Spotlight On The Growing Role Of IT In Security Tasks." May 2020.

The challenge

Workloads have become a finger-pointing vulnerability

Workloads are increasingly becoming distributed as our environments continue to get broader and more complex. Many cloud-based applications are business critical but vulnerable to compromise if any part of the workload (app, data or OS) malfunctions. Of course, the solution isn't to shut down a corporate server when an incident occurs. Security and IT operations are secondary to business productivity. This means that securing and monitoring each part of the workload is now an additional—and critical—part of securing your business.

Who is responsible for securing workloads?

When workloads lived in static rack servers in on-premises data centers, it was easy to assign responsibility for keeping them secure. Today, workloads can exist on physical servers, virtual servers, in the public cloud, or even serverless. And workloads can move across all these environments, which makes them difficult to track and manage. Security, IT admins, cloud admins, VMware vCenter® admins, site reliability engineers (SREs), DevOps, and developers all can play a part in the workload lifecycle. Sometimes, they can impact workloads in ways that achieve common goals, but their goals can counteract at other times.

IT admins can efficiently secure workloads. However, they are blind to most workload vulnerabilities and certainly don't have the context to prioritize impact. And because IT admins often don't have control over the cloud environment, the roles and responsibilities become clear as mud. Security teams may have some of the information needed to identify vulnerabilities but may not have clear risk prioritization or context to manage remediation effectively.

In other words, workload security is likely not being sufficiently managed by anyone.

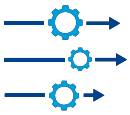
Can responsibility be shared?

The bottom line is that both security teams and IT admins need to play a role in workload security. But to avoid finger-pointing, these teams need to be unified with the processes, information and tools specific to workloads.

With a shared understanding and methodology to automate discovery and prioritization of vulnerability fixes, it becomes much easier for IT admins to share the responsibility of hardening and reducing attack surfaces. In fact, workload security can be operationalized to eliminate the tension and finger-pointing between these two critical teams. All it takes are four key steps to make this a reality.

KEY DATA TO SHARE BETWEEN SECURITY TEAMS AND IT ADMINS

- Indicators of compromise (IOCs)
- Tactics, techniques and procedures (TTPs)
- Visibility into blocked and detected attacks
- Ordinary events that occur on the system
- Evaluation of more than 2,000 workload configuration states
- Inventory of workloads and their state of protection
- Scanless vulnerability context with risk scores and links to the National Vulnerability Database
- Tracking and trends of IT hygiene over time



Four steps to operationalize and simplify workload security

Step 1: Minimize agent overhead

Bolted-on security agent sprawl causes many problems for both IT admins and security teams. The most common challenges are:

- Disparate sources of security information leading to poor communication
- Increased maintenance burden and higher chance of errors
- Added storage costs for data collected

To eliminate these issues, consolidate the IT and security stacks by replacing multiple point solutions with a holistic security approach—one that can collect data across on-premises and cloud environments.

Choose a single built-in agent

The optimal solution is to utilize a single agent in the virtualization layer that is built into your existing infrastructure. This will enable registration of the events needed for full visibility across environments. Having a single agent brings security monitoring as close to a zero footprint as possible.

Big benefits from one agent

Consolidating security solutions down to one agent—a single, comprehensive data source—has big benefits for improving workload security:

- Makes operationalizing agent management easy for IT
- Allows for workflow integration and data sharing across teams
- Provides context-centric information, making outputs more actionable
- Removes point-in-time vulnerability scans, which improves performance and accelerates response time to attacks
- Reduces storage costs and maintenance efforts

Step 2: Share visibility into vulnerabilities

The group responsible for patching is rarely the same group looking at the security impact of vulnerabilities. Classic scanner data rapidly gets out of sync, and ticketing systems are slow, which results in various interpretations of the fixes needed.

IT admins consume data sources that are separate from what the security team consumes but are expected to contribute to larger security processes. This leads to mismatched expectations and poor hygiene outcomes.

A unified view of security data ensures clear communication and understanding of the vulnerabilities detected and their associated risk level.

A unified view reduces risks effectively

Consolidation to a single agent in Step 1 produces security data that can be easily shared between IT admins and security teams. Ideally, this information should be presented within the tools that those teams use daily, such as virtualization tools (for example, VMware vSphere® and vCenter).

Having the same data and evaluation outputs across teams improves communication and collaboration. The most important key is having current vulnerability data always on hand rather than a point-in-time scan. This will ensure the teams are always on the same page. A shared inventory of workload vulnerabilities prioritized by risk will ensure resources are being directed to resolve the most critical issues.

Step 3: Automate risk prioritization

Utilizing a single agent and having shared visibility into security data are great steps toward managing workload security. However, access to known vulnerabilities alone doesn't mean there is a shared understanding of where to focus resources.

A logical next step is to have a standardized way to assess risk. Consider a security solution that automatically handles risk assessment and prioritization.

Risk-prioritized data within current tools for actionable outcomes

A risk assessment solely based on the Common Vulnerability Scoring System is not enough. Contextual data curated from customized threat data sets—including exploit and threat intelligence feeds and more than 7 billion managed vulnerabilities—will give organizations the ability to apply predictive modeling to forecast new vulnerabilities and prioritize remediation activities based on the level of criticality.

Ideally, IT admins should have a view of the most common exploits and high-risk vulnerabilities within their vCenter console. This will easily incorporate workload hardening into daily hygiene activities.

Additionally, IT admins need audit information of the current system state so they can collaborate with security teams to remediate threats. Having a shared view of this information will naturally enable these teams to work together to apply patches by priority or take alternative measures, such as powering down vulnerable systems.

A shared view of current threats and vulnerabilities with associated risks allows for clear prioritization and focus of effort, which leads to faster resolution of existing threats and better protection from future attacks.

Step 4: Streamline workload processes

Vulnerability scans have historically been a monthly or quarterly activity. But these point-in-time exercises are not enough. With the continuous expansion of workloads across multi-cloud environments, these scans aren't providing information that is as broad or as timely as it needs to be to mitigate critical security risks.

With shared visibility and risk prioritization, the next step for both security and IT teams is to make workload security a regular part of IT hygiene.

Operationalizing workload security

Operationalizing workload security requires IT admins to continuously reduce attack surfaces as part of standard IT hygiene practices. IT admins need to access evaluations of thousands of configuration states on their workloads as well as the information and direction to remediate discovered vulnerabilities.

IT management should have access to a shared view of IT hygiene trends over time. This will encourage team discussions around the management of vulnerabilities and measure performance. IT managers should use this information to ensure priorities are being followed and resources are allocated appropriately to continually harden workloads.

What's next?

Aligning IT on workload security reduces attacks

Security teams and IT admins can work together to improve workload security. And with the right security capabilities, this collaboration can be pain free and easily operationalized into daily practice. To capitalize on this opportunity, ensure these teams:

- Are using a built-in solution with a single agent
- Have a unified view of security data embedded in their current work tools
- Have the necessary context and continuous monitoring for vulnerabilities with automated risk prioritization
- Have leadership support to ensure operationalization of workload hardening

Three keys to improve workload security

1. Bring IT admin and security leads together to discuss the opportunity to work together to reduce attacks.
2. Identify current gaps in data collection and visibility to be able to better prioritize vulnerabilities and harden workloads.
3. Explore solutions that will get IT admins and security teams the shared visibility and context needed to be successful.

Addressing workload security yields major dividends

- Coverage and visibility across all workloads
- Simplification of the IT security stack
- The ability to respond more quickly to issues with early detection
- Better hardened assets
- Better prevention of malware and non-desired software and processes
- Complete elimination of non-malware
- Activation of security for the future—modern environments and workloads

Learn more

Read this datasheet to find out how VMware Carbon Black Cloud™ empowers IT and security to improve workload security together.

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