Brought to you by:

vmware®

# Securing Your Organization from Threats

for dummies®
A Wiley Brand

Deliver security as a built-in, distributed service

Implement Zero Trust with fewer tools and silos

Scale response with confidence, speed, and accuracy

Kathryn Lodato

VMware Security Special Edition

# About VMware

VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation with enterprise control. As a trusted foundation to accelerate innovation, VMware software gives businesses the flexibility and choice they need to build the future. Headquartered in Palo Alto, California, VMware is committed to building a better future through the company's 2030 Agenda.

To learn more, visit www.vmware.com/security.

# Securing Your Organization from Threats

# Securing Your Organization from Threats

VMware Special Edition

**by Kathryn Lodato**

for dummies®
A Wiley Brand

# Securing Your Organization from Threats For Dummies®, VMware Special Edition

Published by: **John Wiley & Sons, Inc.,** 111 River St., Hoboken, NJ 07030-5774, www.wiley.com



ISBN 978-1-119-87556-7 (pbk); ISBN 978-1-119-87557-4 (ebk)

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

## Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

**Project Editor:** Elizabeth Kuball
**Acquisitions Editor:** Ashley Coffey
**Editorial Manager:** Rev Mengle
**Business Development Representative:** Cynthia Tweed
**Production Editor:** Sai Karthick Kumarasamy
**Special Help:** Faithe Wempen

# Table of Contents

# Introduction

The modern enterprise faces a growing security challenge involving the need to protect apps and data as your organization concurrently innovates and delivers new applications that are built, scaled, and operated differently in the modern cloud world.

This book is your guide to help you think about cybersecurity differently. Security must be an inherent and distributed part of the modern enterprise — continuously incorporating all aspects of your technology stack to deliver more effective security through a Zero Trust strategy.

## About This Book

Don't let the compact size of this book fool you. It's loaded with information that can help you understand and capitalize on the latest technologies for securing your enterprise. In plain and simple language, I walk you through:

- The problems with today's approaches to cybersecurity
- The characteristics and advantages of security that is built in and distributed
- How this approach helps you implement Zero Trust with fewer tools and silos and scale response with confidence, speed, and accuracy
- Why this approach enables simpler, faster, and smarter security
- Four use cases that simpler, faster, and smarter security unlocks

First and foremost, this guide is a resource. It's meant to serve as an accessible resource for organizations looking to implement Zero Trust and deliver end-to-end security that is simpler, faster, and smarter. Here's a chapter-by-chapter rundown of what you can expect:

- Chapter 1 starts things off by reviewing the current state of cybersecurity. You find out about three overarching security challenges and find out how VMware approaches security.
- Chapter 2 explains how VMware's approach moves your organization beyond the limits of fragmented security that is too siloed and lacks context. This empowers a rethink of legacy security, moving your organization toward security that is simpler, faster, and smarter.
- Chapter 3 dives more deeply into VMware Security, explaining how this new approach solves today's security challenges.
- Chapter 4 gets more prescriptive, highlighting four key use cases that this security approach unlocks and calling out the technologies that enable these use cases.
- Chapter 5 examines some great reasons to partner with VMware Security.

## Foolish Assumptions

In writing this book, I've gone out on a limb and made some assumptions about you. I assume that:

- You're either an IT or security practitioner.
- You have a basic familiarity with IT security issues and products.
- You're acutely aware of the pain points in cybersecurity.
- You're not content with the status quo — you want to approach security in a new way.

## Icons Used in This Book

To make it easy to navigate to the most useful information, these icons highlight key text:

REMEMBER

Take careful note of the key takeaway points marked by the Remember icon.

TIP

The Tip icon highlights information that can save you time and effort.

WARNING

The Warning icon highlights potential pitfalls on the road ahead.

## Where to Go from Here

The book is written as a reference, so you can read it from cover to cover or jump straight to the topics you're most interested in. Whichever way you choose, you can't go wrong. Both paths lead to the same outcome — a better understanding of security in a cloud-first, cloud-native-application-first environment and the steps and technologies you need to move forward.

IN THIS CHAPTER

- Highlighting the current state of cybersecurity
- Exploring three overarching security challenges
- Introducing how VMware approaches security

# Chapter 1
# The Current State of Cybersecurity

This chapter explores the current state of cybersecurity and underscores three key reasons why you need an all-new approach to security.

## Understanding the Problems with Cybersecurity

Today's modern enterprises face a growing security challenge: protecting apps and data in a distributed world. Organizations must:

- Innovate and deliver new applications that are built, scaled, and operated differently in the modern cloud world.
- Secure a highly distributed workforce that uses a variety of devices to access apps and data without hindering productivity.

- Promote user confidence in the security of their applications and data by supporting both modern and traditional workload types running in diverse cloud environments.
- Manage the evolving networks used to connect everything.

All of this leads to exponentially more surfaces to defend.

## Speed is critical

Change is accelerating, and the speed at which your organization can deliver new applications and adapt your infrastructure is how you compete. The movement to a cloud-first or cloud-native-application-first strategy further accelerates the pace of change. It makes managing this tension between speed and security one of the greatest problems organizations face. Providing the protection your organization requires in this new scenario has become more difficult.

WARNING

## HOW EXPENSIVE IS A BREACH?

The average cost of a security breach is now a whopping $4.24 million, according to a study conducted by the Ponemon Institute. The year 2021 had the highest average cost in 17 years. All the while, attacks are becoming not only more damaging but also harder to detect. Just consider these findings from industry researchers:

- **Ransomware attacks are getting increasingly sophisticated.** Forty percent of respondents said double-extortion ransomware was the most observed new ransomware attack technique in 2020.
- **Compromised credentials caused the most breaches.** The most common initial attack vector — compromised credentials — was responsible for 20 percent of breaches at an average breach cost of USD 4.37 million.
- **The mean time to identify and contain data breaches is 287 days.**

In simple terms, the bad guys are expanding their targets, using smarter weapons, and getting better at hiding from commonly used security defenses. And this problem will only get worse. Industry observers expect security breaches and attack vectors to grow exponentially in the years to come — despite increasing investments in security solutions.

## The market is fragmented

A big part of the problem here is that the cybersecurity market is highly fragmented. This has led to a proliferation of point products focused on narrow use cases. The average enterprise deploys 45 cybersecurity-related tools, yet the growing number of tools hasn't resulted in a greater ability to detect and defend against attacks. In fact, enterprises that deploy more than 50 tools ranked themselves 8 percent lower in their ability to detect threats and 7 percent lower in their defensive capabilities compared to companies deploying fewer products.

Despite the use of dozens of security products, the cybersecurity problem is never really effectively solved. Cyber threats continue growing in sophistication, and the attacks keep coming. Data and privacy breaches keep happening, and the costs keep rising.

# Identifying the Three Big Obstacles in Cybersecurity

REMEMBER

Viewed from the highest level and in addition to the increasingly sophisticated threat landscape, organizations are facing three significant cybersecurity problems today:

- Too many surfaces to defend
- Too many silos
- Too little context

The following sections cover each of these problems in greater detail.

## Too many surfaces to defend

You have users working remotely from hundreds or thousands of different locations with workloads traversing multiple clouds — meaning the attacks you face are increasingly spread out. The legacy security model of routing firewall traffic through a single point no longer works in this distributed model. With everything dispersed and constantly changing, the deployment and management of traditional agent technology to monitor your environment is infinitely more difficult — and few organizations can keep current.

The same applies for the security controls used to protect everything. It's one thing to deploy a thousand software firewalls as your infrastructure moves out of the data center. It's quite another to manage each one on an ongoing basis.

Finally, you have to consider all the different environments you must protect — from legacy data centers to public clouds, from virtual machines to containers, and from desktop to mobile devices. The list goes on, with each requiring a different security approach. Cost and complexity continue to spiral upwards.

## Too many silos

Multiple groups in an organization focus on protecting your environment, but these different teams don't equate to additional layers of security. Instead, they create complexity and gaps that attackers can exploit. Security, IT, development, and other teams each approach protecting your environment from a different perspective. And each group uses a plethora of different point tools, generating unique — and often isolated — data in the process.

What's more, these groups are siloed from an organizational perspective. As a result, there is little commonality from a visibility and analytics perspective. Each group has its own view of the environment managing the specific vulnerabilities and threats they see. There is no shared context between the core Zero Trust control points of users, devices, workloads, and networks.

As organizations shift to the cloud and new modern application architectures emerge, getting the full picture becomes even harder because resources are more distributed and ephemeral in nature. Perhaps just as concerning is the resulting lack of coordination in terms of orchestration and automation, making it impossible to enforce your policies and act in a consistent fashion. Many organizations can't investigate issues without tremendous friction across these groups, forcing them to accept unnecessary risk.

## Too little context

Too often, you're forced to make security decisions with incomplete and inaccurate data because you require more than threat intelligence. You need deeper context about the assets you're protecting and the threats you must defend against.

Anti-malware will only get you so far. It won't help you understand what's going on when attackers deploy novel malware and

use software you trust for nefarious activities. Handling these threats requires a deeper understanding of how your systems — applications, data, network, and users — fit together. Knowing that an alert is for an IP address is different from knowing that the same IP address is for a critical database server that contains important patient records.

A chaotic stream of alerts isn't enough because you can't prioritize them to defend your most critical assets first. When you recognize something is going wrong, you need to determine the full extent of the attack and the implications of any remediation actions you plan to take. Point product security tools simply don't give you the full picture. And without the full situational intelligence, your security efforts are flying blind.

## MAKING SECURITY A TEAM SPORT

As threats and breaches grow in sophistication, it's more important than ever for security, IT, and development to adopt a unified approach to security. Despite collaboration efforts, these teams remain "frenemies." So, how do organizations make security a team sport rather than a siloed activity executed by an isolated security team?

According to "Bridging the Developer and Security Divide" (`www.vmware.com/resources/security/bridging-the-developer-and-security-divide.html`), a commissioned study conducted by Forrester Consulting on behalf of VMware, unifying security, IT, and development strategies lays a foundation for future success. Forrester surveyed 1,475 respondents and conducted five interviews with IT, security, and development managers and above (including chief information officers [CIOs] and chief information security officers [CISOs]) with responsibility for development or security strategy decision-making to explore this topic. In the study, 72.5 percent agreed that their senior leadership focuses more on strengthening the relationship between development and security than they did two years ago, but relationships are still strained. In fact, 36.5 percent of decision-makers reported that their organizations' teams are not effectively collaborating or taking strides to strengthen relationships between security and development teams. There's business justification for improving relationships — the study found that security and development teams with positive relationships can complete the software development life cycle five business days faster per app release than teams with negative relationships.

# It's Time for a New Approach

REMEMBER

So, where do we go from here? It's time to rethink security as an inherent and distributed part of the modern enterprise. It's time to envision a solution that continuously incorporates all aspects of your technology environment to deliver more effective security through a Zero Trust approach.

In 2019, NIST built out the NIST Zero Trust Framework SP 800-207 (`https://csrc.nist.gov/publications/detail/sp/800-207/final`), but it has grown in importance since March 2020 when remote work became more prevalent, causing the network perimeter to largely dissolve. Zero Trust emerged as the most effective security architecture for addressing cyber threats in this new environment.

Zero Trust, or "never trust, always verify," consists of four pillars: devices, users, workloads, and networks. You must establish trust in each pillar to make decisions to grant or deny access. By establishing trust across the four pillars, you gain visibility and gather analytics across the board. Visibility and analytics are critical parts of Zero Trust; they help to establish a deeper and broader footprint in each pillar.

Delivering security as a built-in distributed service across your control points — users, devices, workloads, and networks — helps you implement Zero Trust with fewer tools and silos. Your people are then better equipped to solve the threats of today and tomorrow — you have fewer blind spots and reduced time to detection and response because information is presented in context, combining data from all sources in an intelligent fashion. And this context is shared across teams to reduce silos. This helps you better operationalize security, making more effective use of your people and resources. With VMware Security, you can simplify complexity and better protect your organization from risk.

IN THIS CHAPTER

- Exploring how VMware approaches security
- Seeing what you can get with VMware Security
- Thinking differently about security

# Chapter 2
# Introducing VMware Security

This chapter explains how VMware Security approaches security differently. With VMware Security, you can implement Zero Trust with fewer tools and silos, better context, and security that's built in and distributed with your control points of users, devices, workloads, and networks. You achieve simpler, faster, and smarter security.

## Moving beyond Business as Usual

The built-in and distributed security approach is a fundamentally different way to secure your business. It's not a product, tool, or bundle for your organization. It's a strategy that helps you accelerate your Zero Trust journey through a connected approach — joining the critical control points of users, devices, workloads, and networks.

Using this approach, VMware Security helps you to:

- Deliver security as a built-in distributed service.
- Implement Zero Trust with fewer tools and silos.
- Scale response with confidence, speed, and accuracy.

REMEMBER

This approach isn't about ripping and replacing. It's about using what you have in new ways, so you can accelerate your Zero Trust journey and bring your teams, tools, and processes together to scale responses to threats with the right context and insights.

TIP

Watch this video and get a VMware Security overview: `https://youtu.be/SJKrKdVv4pg`.

## Identifying What You Can Get with VMware Security

REMEMBER

You can get the following security outcomes with VMware Security (see Figure 2-1):

- Simpler
- Faster
- Smarter

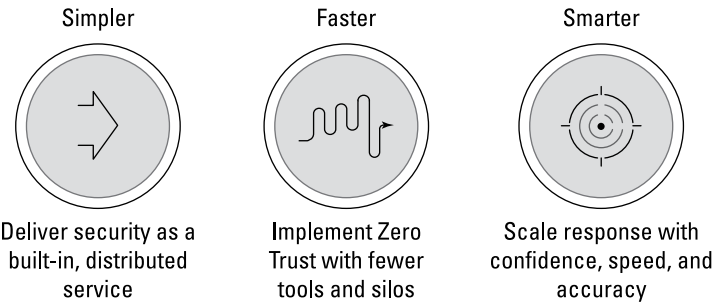


**FIGURE 2-1:** What you can get with VMware Security.

This approach solves the security challenges organizations are currently facing (see Chapter 1):

- Too many surfaces to defend
- Too many silos
- Too little context

## You get simpler security

Security is simpler when it's built-in, distributed service. This means a connected approach that joins the critical control points of users, devices, workloads, and networks. And this must extend back to your legacy environments to implement a Zero Trust strategy.

Instead of being an add-on, security must be an inherent part of these control points and distributed so you can deliver security that lives with the assets being protected — no matter what type of environment or applications you have or where your users or employees are connecting from. This approach also means no network changes, no blind spots, and no choke points. The cost and complexity of administering thousands of add-on security controls is reduced. VMware builds security into every product and platform so it's easy to "turn on."

## You get faster security

Security is faster when you use fewer tools and reduce silos by connecting the different teams so they're operationalized through a common source of truth to protect and defend your infrastructure. This results in a stronger security posture from better, faster detection and a coordinated response with your security, IT, and development teams. The silos between teams are broken down. Security becomes a team sport. The security team collaborates across the end-user services and networking teams. And with the multi-cloud and modern apps transformations, security teams can also collaborate with the cloud and infrastructure team and the DevOps team.

VMware is one of a few companies today that has a close relationship with each of these five teams. And VMware powers the key infrastructure and control points you're using. This enables VMware to not only drive more collaboration but also build simpler solutions for your most complex security challenges to protect your apps and data.

### You get smarter security

Security is smarter when you can scale your response to security events with confidence by automatically curating data from all sources, including threat intelligence and an intrinsic understanding of your applications and tech stack. Information is presented in context so your people can visualize and connect the dots on how your infrastructure fits together, the full implications of an attack, and the fastest, least disruptive way to remediate security events. With risk prioritization on vulnerabilities, you allow your most critical assets — your people — to do the most important work.

## Discovering How VMware Approaches Security Differently

REMEMBER

You need security that's built in and distributed with your control points of users, devices, workloads, and networks, to implement Zero Trust with fewer tools and silos and scale response with confidence, speed, and accuracy.

When you make this change, security becomes end to end, reducing your attack surface. Your people are better equipped to solve the threats of today and tomorrow, and you have fewer blind spots and can dramatically reduce time to detection and response and attackers' dwell time. At the same time, you can better operationalize security, making more effective use of your people and reducing unnecessary expense and effort.

With VMware Security, you reduce your attack surface to mitigate security risk, ensure compliance, and simplify security operations. You can automatically curate security data to share better context among your security, IT, and development teams. This enables you to operationalize more of your security through your IT and development teams by creating a common source of truth.

IN THIS CHAPTER

- Providing security as a built-in, distributed service
- Implementing Zero Trust with fewer tools and silos
- Scaling response to security events with confidence, speed, and accuracy

# Chapter 3
# Solving Your Security Challenges with VMware Security

This chapter dives deeper into how VMware makes security simpler, faster, and smarter to help organizations like yours.

## Simpler: Delivering Security as a Built-in, Distributed Service

REMEMBER

Your security posture needs to mirror your infrastructure. With VMware, your security controls and policy enforcement protect your distributed assets, supporting both new and legacy environments and applications. And because you can reduce the number of tools and agents you deploy while managing them in a centralized fashion, you can consistently apply your policies across multiple environments with little to no added effort. You achieve full coverage of your environment by connecting the dots while reducing complexity and blind spots.

VMware makes security simple by enabling you to:

- **Deliver security as a distributed service, built in from the start.** You must protect remote users, workloads dispersed across data centers, private and public clouds, and extensive networks — everything is spread out. With VMware, you can place your security capabilities in line with your architecture and mitigate unknown security risks by delivering distributed security that protects your assets across various environments. Although your security services will be distributed, you can control these resources and manage your policies from a single location. You gain the benefit of security living with the assets you want to protect without the cost and complexity of administering thousands of different security instances. You benefit from security that is embedded into your assets from the start and distributed across the control points of the digital enterprise. There are dramatically fewer blind spots or choke points, the cost and complexity of administering thousands of add-on security controls are reduced, and with authoritative context your security posture can be more easily distributed at scale. As a result, protecting a distributed environment is not only possible but practical.
- **Consolidate agents and tools on endpoints and deliver a frictionless experience on workloads.** Each additional security sensor requires additional effort to deploy, maintain, and manage — with agent central processing unit (CPU) overhead creating a significant processing penalty. With VMware, you can significantly reduce the number of agents and sensors you utilize, while getting security up and running faster.
    - For example, with VMware's Carbon Black Workload, you can use the workload protection capabilities already in the vSphere client to monitor your systems. With the NSX Service-defined Firewall integrated into vSphere, you gain visibility into traffic and easily create network segmentation to detect and prevent malicious traffic with a distributed intrusion detection system (IDS)/intrusion prevention system (IPS), network sandboxing, and network traffic analysis. And when workloads are deployed in the public cloud, CloudHealth Secure State can provide a comprehensive view of your environment in an agentless deployment.

- By simplifying operations, your security and IT teams will spend less money, time, and effort administering agents, devoting more attention to higher-level activities. And with less operational overhead, you get more out of your IT environment.

- **Support legacy to cloud-native apps, services, and infrastructure while moving faster.** In the rush to protect your modern applications and assets, you don't want to neglect your longstanding resources and expose them to attack. With VMware, you can protect both legacy and cloud-native apps, services, and infrastructure. Using a single-solution portfolio, you can secure traditional data centers, private cloud, and public cloud. And you can extend this security umbrella from virtual machines (VMs) to containers and code, from desktops to mobile devices. You're able to transition to next-generation systems and modern applications without increasing security complexity. You limit risk exposure in an application production environment with continuous container security hygiene delivered from automated patching and validation.

- **Easily integrate with the rest of your security tools through robust application programming interfaces (APIs) and third-party integrations.** Your staff shouldn't be burdened with coding complex custom integrations with your existing security stack. With VMware, you obtain greater value from the other solutions in your security stack. Through VMware's ecosystem of 140+ partnerships, product integrations, and open APIs, you enrich your current security and IT workflows. For instance, with VMware Carbon Black Cloud, you can integrate tools and workflows to gain holistic visibility that extends across your endpoints, networks, workloads, and containers. And you can leverage VMware's robust APIs for workflow automation.

  Additionally, you can obtain customized threat intelligence to populate workflow systems with task activity information and add customer-specific threat intelligence.

  Finally, you can detect, investigate, and remediate security and compliance risks and integrate security in the continuous integration/continuous delivery (CI/CD) pipeline via APIs. For example, with the CloudHealth Secure State Findings and Remediation API, you can build guardrails in your infrastructure provisioning pipeline. Native CloudHealth Secure State

rules or custom policies enable selective verification of configuration settings at near real-time speed during testing and staging of cloud infrastructure.

REMEMBER

With VMware, everything you can do in the user interface (UI) you can do with an API call. This enables business transformation opportunities through automation and workflow integration.

## Faster: Implementing Zero Trust with Fewer Tools and Silos

REMEMBER

Simply covering the four Zero Trust control points isn't enough — you must also connect these critical areas. This requires understanding the security situation and enforcing the appropriate policies and actions to close security gaps and reduce risk.

Not only will you realize better communication and data sharing between your security controls, but you'll also enable greater coordination between your security, IT, and development teams. With a common understanding of what they're protecting and what steps to take to provide security, your teams can act faster with greater efficiency. And with fewer security products, they'll spend less time on administration and more time focusing on initiatives that are core to your business.

With the right Zero Trust strategy in place, no vital area is left undefended.

VMware puts security into overdrive by enabling you to:

- **Reduce your reliance on point security tools.** Managing and coordinating dozens of security products can consume an inordinate amount of attention and resources. You need to reduce the number of point security products applied against the four Zero Trust pillars of users, devices, workloads, and networks, by partnering with a trusted provider such as VMware.

  You'll achieve better security outcomes, reduce security gaps, and deliver a better employee and customer experience while devoting less time to managing vendor relationships, administering contracts, and ensuring that updates

are applied in a timely fashion. This leaves you with more time and energy to direct to more strategic priorities.

- **Connect your security control points.** Your security tools work best when they work together. Because VMware supplies the infrastructure for the four critical control points within a Zero Trust framework, you can easily extract and combine the data that VMware's user, device, workload, and network solutions generate. This provides shared visibility and analytics across all four domains to establish a shared security context.

  You can use these same inherent connection capabilities for orchestration and automation purposes, enabling you to enforce your security policies uniformly across your infrastructure. With security controls that talk with each other and work as one, you establish an end-to-end security posture, enabling faster detection and a coordinated response to defend your most critical assets.

- **Foster better coordination between your security, IT, and development teams.** Security, IT, and development teams won't be inclined to work with each other if it's a burden. Working with VMware, your teams can speak a common language without changing the tools they use. For example, DevOps can automate compliance policy enforcement, minimizing risk exposure and developer toil.

  Here's what that looks like in practical terms: Instead of being buried in alerts, your teams can focus on risk-prioritized vulnerabilities and maintain auditable logs of remediations performed by their application platform. Underlying cloud infrastructure layers are secured from familiar and existing vCenter consoles. Your IT administrators can receive ongoing vulnerability information within their existing vSphere consoles, enabling them to apply patches proactively and minimizing your exposure. Your IT and development professionals are knowledgeable about security — and able to actively protect your organization — alleviating the impact of the current cybersecurity talent shortage. You operationalize your security through your IT and development teams by creating a common source of truth, dramatically increasing your capacity to protect and defend your environment.

- **Unify DevSecOps to secure your software supply chain.** Modern applications are composed of multiple containers running as microservices that can be updated and deployed independently atop Kubernetes across multiple clouds. How can you keep the container life cycle secure from code to customer?

  DevSecOps aligns development, operations, and security professionals on the goal of speeding software delivery while simultaneously enhancing an organization's security posture. You reduce vulnerabilities at every stage in the development life cycle by securing your application code and scanning your container images starting in development. You also have the automation to effectively integrate security throughout the container life cycle, along with the ability to create automated policies to enforce secure configuration of workloads and ensure compliance.

  Bottom line: You can make it easy to do the right thing, enabling you to maintain velocity and be secure by default.

## Smarter: Scaling Response with Confidence, Speed, and Accuracy

REMEMBER

Your decisions are only as good as the data upon which they're based. With VMware, you'll have more than alerts — you'll have the full authoritative context of your environment and threat intelligence that is trustworthy, actionable, and readily available.

By knowing the threats you face, where there may be gaps in your defenses, and whether these vulnerabilities are being exploited, you can quickly adjust your controls and policies to address security gaps and events faster. What's more, you can be more adept at identifying and assessing attacks when they occur, enabling you to shut them down and take the appropriate actions to repair any damage with minimal impact to your organization. Your actions are based on facts, not guesswork.

VMware raises the IQ of your security systems by enabling you to:

- **See the entire situation.** You don't protect individual endpoints, workloads, or network elements — you protect

functioning systems. VMware is present when workloads are created, meaning you generate better data on what you're protecting in terms of variety, volume, and accuracy.

For example, with VMware, container metadata includes the bill of material for the container, the results from image tests, and Common Vulnerabilities and Exposures (CVE) scan reports — providing full provenance tracking and patching tracking. With this wealth of information, you can view your infrastructure in context, pulling data together from across all your critical control points. As a result, you'll understand the true vulnerabilities your assets face, and you can prioritize your protection efforts in response.

By detecting not just bad software but also bad activities, you're in a much stronger position to root out evasive attacks. And when an attack does occur, you can see everywhere it's occurring and rewind events to determine how you got to this state. In this way, you accelerate the investigative process while minimizing the collateral impact of any remediation efforts. Your security team has the highest level of clarity regarding the events occurring within its assets and is best positioned to act based on visibility.

- **Focus on high-value activities, such as threat hunting, while automation helps you defend the business.** In a world where security talent is short, you must maximize the use of those sparse resources. With VMware, you'll receive updated defense capabilities, with no manual interaction required, enabling you to scale security. You can use VMware's unique capabilities to identify and prioritize risk, detect threats, and automate response and remediation processes. And by applying VMware's unique machine learning capabilities and orchestration, you allow your most critical assets — your people — to do the most important work.
- **Respond with confidence and ensure uptime in the face of risk.** You want to stay ahead of potential attacks. With VMware, you have access to intelligence from security experts who understand both attackers and the underlying compute fabric. With that information, you're able to better understand threats and make decisions with full awareness of how your environment operates.

Threat intelligence from the VMware TAU supports threat detection, prevention, and hunting by providing authoritative context and information about the tools, tactics, techniques, and procedures that bad actors use. VMware generates this threat intelligence using both manual analysis and automated extraction based on many forms of artificial intelligence (AI). It employs a threat research process that continuously improves customers' ability to identify known and novel threats. This means you gain an edge over your adversaries, anticipating attacks to proactively reduce your exposure, close gaps, and support decision-making.

- **Ensure seamless authentication and minimize downtime with proactive security.** Making security user-friendly is critical. With VMware, you can use comprehensive risk-based conditional access control models to authenticate users and then deploy built-in multi-factor authentication (MFA) and single sign-on (SSO) capabilities to ensure the best employee experience as they access different types of apps from a variety of devices.

  Integrating endpoint management and endpoint protection means user and device context are considered to automatically prevent, detect, and remediate threats with intelligent automation and orchestration between various IT and security tools. You provide an exceptional employee experience, no matter where employees work, without compromising security.

Chapter 4 takes a closer look at the use cases for VMware Security.

IN THIS CHAPTER

- Securing a multi-cloud environment
- Securing modern apps
- Securing the distributed workforce
- Modernizing the security operations center

# Chapter 4
# Examining Key Use Cases

The VMware Security portfolio covers all the key control points — users, devices, workloads, and networks. The complementary products in the portfolio enable your organization to leverage your infrastructure to provide adaptive protection for your apps and data no matter where they live. And you can do it all while giving your users the flexibility and freedom to work as they want.

This chapter explains how VMware Security helps modern enterprises innovate to deliver better customer and employee experiences and stay competitive in today's digital economy. With a connected approach that links the critical control points of users, devices, workloads, and networks, VMware continuously incorporates all aspects of your technology stack to accelerate your Zero Trust journey and achieve a more effective security posture.

This chapter looks at four use cases, each of which demonstrates different challenges and requires different tools and strategies. Because VMware Security consists of a suite of complementary products, you can select the best tools and protections for your unique needs.

# Securing a Multi-Cloud Environment

Accelerating digital transformation means embracing the distribution of applications and workloads across the multi-cloud. But the resulting flexibility, agility, and scale can come at a cost. A stretched perimeter and an increasingly sophisticated threat landscape increase risk and threaten to diminish these gains.

For the strongest multi-cloud security, you need to:

- Secure workloads.
- Secure workload access and communications inside every private and public cloud and across different clouds.
- Protect against cloud misconfigurations.

The following sections dig deeper into each of these requirements and show you how VMware Security solutions can help.

## Securing workloads

Securing a multi-cloud platform begins with securing the workload itself. When it comes to security, you can't secure what you can't see. Therefore, complete visibility into all workloads with detailed system context is a critical first step.

By integrating directly with vCenter, VMware Carbon Black Workload enables deeper, unparalleled visibility into your environment to reduce risk and harden workloads, while helping to streamline and operationalize security. With continuous inventory of all workloads running in a multi-cloud environment, Carbon Black Workload enables teams to close critical security gaps and ensure the integrity of hosts and applications.

IT professionals often face the challenge of having too many tools to oversee and manage, especially when it comes to security. Carbon Black Workload helps to consolidate and simplify operations by integrating directly into vSphere and VMware Cloud. This integration also enables administrators to activate multi-cloud workload protection with a single click, making installation simple and easy.

With real-time vulnerability assessment, security and infrastructure teams can better understand vulnerability context

with risk scores and links to the National Vulnerability Database, while eliminating the need for resource-heavy scans, additional administrative overhead or setup, and system downtime. vSphere administrators can easily activate workload protection as a feature right from the vSphere Client, with bulk enablement and life-cycle management for virtual machine (VM) inventory. The vSphere dashboard provides visibility into appliance health, inventory status, and installation workflow, and allows the infrastructure team to see a risk-prioritized list of operating system and application vulnerabilities found across the environment.

Security teams lack visibility and control in highly dynamic multi-cloud environments. VMware Carbon Black Workload protects workloads running in these environments by combining foundational vulnerability assessment and workload hardening with industry-leading next-generation antivirus (NGAV), workload behavioral monitoring, and detection and response capabilities for workloads. It also provides visibility into operations hygiene; indicators of compromise (IOCs); malicious tactics, techniques, and procedures (TTP); and ordinary events that occur on the system.

Security teams can analyze attacker behavior patterns over time to detect and stop never-before-seen attacks, including those manipulating known-good software. If an attacker bypasses perimeter defenses, security teams can shut down the attack before it escalates to a data breach. By embedding security into the infrastructure, security teams can easily audit the current system state to track security posture and harden workloads, while enabling easier collaboration with vSphere administrators to address known vulnerabilities.

Providing a single source of truth for IT and security teams greatly improves visibility and collaboration to help break down organizational silos. Both teams are able to see where their most critical security gaps exist, as well as the context behind the threat or vulnerability. Proper risk management also requires quick and effective action. By providing robust risk prioritization in real time, VMware enables teams to efficiently allocate the right resources to the most critical of threats by showing which vulnerabilities need attention first.

VMware takes an intrinsic approach to delivering security — building it into the infrastructure everywhere workloads are

deployed. Through this unique approach, VMware can eliminate the trade-off between security and operational simplicity by providing a single source of truth for infrastructure and security teams to accelerate response to critical vulnerabilities and attacks, while enabling collaboration and reducing friction to simplify and consolidate the IT and security stack.

## Securing workload access and communications

REMEMBER

Securing workloads is just the start. A secure multi-cloud requires securing all workload access and communications, both inside and across clouds. Securing workload access not only helps you secure your data but also ensures that you stay compliant with regulatory frameworks.

### Protection: Securing the access foundation

Securing workload communications starts with strong east–west protection of lateral communications using VMware Distributed Firewall for network segmentation and micro-segmentation, and VMware Tanzu Service Mesh for application programming interface (API) security.

### Detection: Identifying access threats

VMware Security tools detect threats on several layers, for more effective detection:

- **Layer 1: NSX Distributed Intrusion Detection System (IDS)/Intrusion Prevention System (IPS):** The first layer of threat detection uses a continually updated signature database and basic behavioral analysis to identify threats moving in in-band traffic at each individual hop. These moving threats can't be stopped by distributed firewall and service mesh protection alone. VMware NSX Distributed IDS/IPS uses its massively distributed design and knowledge of the context of relevant applications and their unpatched vulnerabilities to detect threats efficiently and without performance degradation. Most important, VMware NSX Distributed IDS/IPS can apply "virtual patches" to the hypervisor, protecting unpatched applications in real time — even in a live production environment.

- **Layer 2: Network Traffic Analysis:** The speed at which new threats are emerging means that some may not be covered by signature-based detection and basic behavioral analysis. The second layer of threat detection requires the use of signature-based multi-hop network traffic analysis and artificial intelligence (AI)–based detection of threat behavior. It must detect threats in unencrypted and encrypted traffic. VMware Network Traffic Analysis (NTA) uses a machine learning system to monitor, analyze, and protect against millions of threats every day. It leverages this threat behavior information to accurately identify known and unknown threats among all network anomalies, with the lowest false positives in the industry.
- **Layer 3: Advanced Threat Analyzer (ATA):** Many modern threats are designed to evade or hide from traditional sandboxes and enterprise IDS/IPS. The third layer of threat detection is VMware ATA, a full-system emulation sandbox that malware can't detect. As a result, it delivers visibility into every malware action, even those designed to remain hidden inside traditional sandboxes.

### Response: Bringing it together to minimize damage

Breaches can move quickly, requiring a correlated view of all detection events for an effective, timely response. VMware Network Detection and Response is an SE Labs AAA-certified advanced threat detection and response solution that correlates individual detection events from all three detection layers — IDS/IPS, NTA, and ATA — correlating them into fewer security-relevant intrusions and organizing them into a timeline for rapid threat hunting and response.

## Securing workload access across clouds

Securing workload communications and access is no longer restricted to a single data center or public cloud. These same capabilities of protection, detection, and response must work the same way across every cloud, as if they were a single environment.

Easily operationalizing security across clouds requires a scale-out architecture with software that gives underlying infrastructure — firewalls, meshes, and load balancers — the same elasticity as

modern, distributed applications. VMware's Elastic Application Security Edge (EASE) delivers this scale-out architecture, extending the protection, detection, and response capabilities of the industry's strongest secure workload access solution to the entire multi-cloud.

### Protecting against cloud misconfigurations


WARNING

Securing public clouds is a key element of securing multi-cloud environments. With public cloud misconfigurations resulting in many security breaches, organizations need a smarter approach for managing public cloud risk.

CloudHealth Secure State makes it easier for organizations to reduce misconfigurations and operationalize public cloud security. Using its intelligent cloud-native security approach, security teams can get a deeper understanding of cloud risk and collaborate with developer teams to prioritize and auto-remediate security findings.

All these capabilities combined give you the confidence that you can deploy any workload on any cloud while ensuring the strongest multi-cloud security required to keep your business moving.

## Securing Modern Apps

As business has modernized, so have applications. These changes have created new complexity when it comes to securing modern apps. A 3-tier web app is now 3,000 tiers. Each dynamic instance communicates with other dynamic instances in a complex orchestration that takes place inside and across clouds.

The key to securing modern applications — given their ephemeral and immutable nature — is understanding how these applications are built — continuous integration/continuous delivery (CI/CD) — and how they communicate — APIs. VMware Carbon Black Container is highly complementary with VMware Tanzu solutions in addressing the DevSecOps challenges of modern applications — enabling more secure applications and simplifying operations for security and DevOps teams.

REMEMBER

VMware Security follows the life cycle of the application, embedding itself into this agile process without slowing it down:

- **In the build phase,** continuous scanning saves time by revealing compliance violations and vulnerabilities in container images.
- **At deployment time,** vulnerable or noncompliant workloads are blocked from deployment.
- **At runtime,** virtual guardrails ensure that containers operate within global security policies, without perturbing the self-service, self-driven benefits of cloud-native dynamics.
- Once **in production,** VMware CloudHealth Secure State reduces configuration drift, identifies relationships and risks across Kubernetes and cloud resources, and ensures the integrity of applications throughout their life cycles.

VMware Security also protects API communications with end-to-end encryption for container communications. It sees and understands all API-level communications and detects abnormal API behaviors across the multi-cloud's distributed architecture. With VMware's API security, you can understand how the APIs are being used and make sure that they're being used properly.

With VMware, you gain visibility into and control over the security posture and compliance of containerized applications. You protect your applications from cradle to grave.

## Securing the Distributed Workforce

Remote work is no longer just an option or an initiative. Almost overnight, it has become a global imperative and essential to a business continuity plan. Organizations continue embracing the shift to support flexible workstyles. It's unlikely that businesses will ever return to a fully location-based model.

The need for solutions to secure and manage all these new edge devices has become increasingly apparent. According to the results of a study, 46 percent of global businesses have encountered at

least one cybersecurity incident and 91 percent of security professionals reported an increase in cyberattacks since shifting to a remote working model. Outdated perimeter-based security models are unable to scale with the exponential rise in threats.

Supporting today's distributed workforce needs a new approach and a rethink of how organizations enable seamless workspaces without limitation. VMware believes that the way forward is through an integrated workforce solution.

VMware Anywhere Workspace implements an integrated solution built on the pillars of industry-leading unified endpoint management, desktop and app virtualization, secure access service edge (SASE), and endpoint security technologies. It builds trust for today's distributed workforce, enabling highly engaged employees; reducing silos, disparate tools, and operational overhead; and providing for broader, more effective security that follows users, data, and apps, no matter where they are. Combining endpoint security and endpoint management with network edge security in a holistic solution means you can measure experience and risk across connected control points, and then surface for automated remediation and orchestration. No other vendor today provides a holistic approach that combines endpoint security and endpoint management with optimized network edge performance and security.

## IT'S HERE TO STAY

A distributed workforce is the new normal.

- In 2020, 71 percent of workers surveyed indicated that they were doing their job from home all or most of the time.
- More than half of employees (55 percent) would prefer to be remote at least three days a week when pandemic concerns recede.
- Thirty percent of employees say they're likely to switch jobs if returned to fully on-site work.

A critical component of the distributed workforce is the endpoint. VMware Carbon Black Endpoint offers organizations the ability to secure endpoints and move from fragmented workflows to a seamless process of identifying risk, prevention, detection, and response across the most complex of attacks. Carbon Black Endpoint can recognize the good, the bad, and the in between as it continuously collects endpoint activity because attackers intentionally try to look normal to hide their attacks. Carbon Black Endpoint consolidates multiple endpoint security capabilities using one endpoint agent and console. It minimizes downtime when responding to incidents and helps return critical central processing unit (CPU) cycles back to the business.

The distributed workforce has fundamentally changed the way networks were designed. Gone are the days of backhauling traffic to the security services, as was traditionally done. Instead, security services are bundled in SASE points of presence (PoPs) strategically located in infrastructure as a service (IaaS) and co-location data centers close to users and applications to deliver an optimal employee experience. VMware SASE:

- Secures access to on-premises and cloud-hosted apps
- Routes traffic most optimally using software-defined wide-area network (SD-WAN) gateways
- Enables you to apply security controls for all traffic that flows through

Through a cloud-native security model that encompasses user identity, device posture, and network location, VMware SASE unifies network and application security policies for branch and remote users. Securing the distributed edge means you ease your Zero Trust journey with situational intelligence and connected control points.

The VMware Workspace ONE platform enables you to better secure your employee experience across multiple devices in multiple locations. You can deliver an integrated and seamless experience, offering PC-to-Mac management in a unified manner. Workspace ONE enables this with consistent policies across the board. With VMware's solution, you can automate the workspace. From onboarding to patch management to safe configuration, you can simplify the complexity with Workspace ONE by automating

and orchestrating these processes, removing manual work, and improving experience management.


REMEMBER

VMware Anywhere Workspace builds trust to empower today's anywhere workforce — purpose-built to enable any employee to work anywhere from any device with secure and frictionless experiences. Combining endpoint security and endpoint management with network edge security in a holistic solution means you can measure experience and risk across connected control points, and then surface for automated remediation and orchestration. VMware Carbon Black Endpoint, VMware SASE, and Workspace ONE is a unique solution in the market that can help you meet your security needs and successfully embrace the future of work.

## Modernizing the Security Operations Center

Your security operations center (SOC) is responsible for responding to threats while also advising, maintaining, and overseeing your global security strategy. This requires visibility into all your control points and integration with threat intelligence to quickly respond to threats. VMware Security connects your critical control points to streamline security operations and scale your response across your modern applications, multi-cloud environment, and distributed workforce.

At the center of the extended detection and response (XDR) strategy is the VMware Carbon Black Cloud, a centralized platform that enables you to integrate multiple control points across endpoints, workloads, containers, networks, identity, and email. This solution enables you to analyze real-time telemetry from across your control points so you can modernize your security operations. You can operate at the pace of adversaries in a distributed world.

To further enhance detection and response capabilities, XDR brings together endpoint detection and response (EDR) and network detection and response (NDR), a powerful and effective combination. XDR's fundamental control points are on the endpoint and in the network — the two most challenging places in the enterprise to gain visibility.

You can easily integrate VMware solutions with other products in your environment using VMware's open API ecosystem. This means you can simplify the complexity of connecting other products in your environment with VMware's platform, delivering security that's built in and distributed with your multi-cloud environments, your distributed workforce, and modern apps, all while modernizing your SOC.

IN THIS CHAPTER

- Protecting a business's reputation and assets
- Preventing and responding faster to attacks
- Simplifying and making security a team sport

# Chapter 5
# Ten (or So) Great Reasons to Partner with VMware Security

To build a business case for delivering simpler, faster, and smarter security, your team needs to clearly articulate the benefits of this transformation. This chapter highlights compelling reasons to adopt this approach.

## Protecting Your Brand

WARNING

Security breaches that compromise sensitive corporate and customer information can be devastating to a company's reputation. They can lead to horrible headlines, lost customers, falling stock prices, and regulatory sanctions. VMware Security can help your enterprise protect your brand. We help you implement security that is embedded into your assets from the start and distributed across your control points — users, devices, workloads, and networks — to operationalize Zero Trust for a more effective security posture. With authoritative context, your security posture can be easily distributed at scale to protect the enterprise.

## Preventing and Responding Faster to Attacks

With VMware, you can be more adept at identifying and assessing attacks when they do occur. With connected control points, you establish an end-to-end security posture, enabling faster detection and a coordinated response to defend your most critical assets.

While helping your organization respond faster to attacks, VMware Security can also help stop threats from happening in the first place. With threat intelligence from security experts in the VMware Threat Analysis Unit (TAU), you can stay ahead of attackers. VMware TAU supports threat detection, threat prevention, and threat hunting by providing authoritative context and information about the tools, tactics, techniques, and procedures used by bad actors. What's even better? You can count on experts who not only understand attacker behavior, but the underlying compute fabric.

## Simplifying Security

With a simplified approach, you have fewer products, agents, and interfaces to manage, making security less complex and reducing the chances for error. With VMware, you can significantly reduce the number of agents and sensors and get security up and running faster. For example, with VMware Carbon Black Workload, you can use the workload protection capabilities integrated into vSphere and VMware Cloud to monitor your systems — all from one familiar interface.

## Enabling Collaboration

As organizations shift to the cloud and cloud-native applications, getting the full picture becomes more difficult because the dozens of point security tools do not enable a shared context between the core Zero Trust control points of workloads, networks, devices, and users.

To succeed, security must be a team sport across security, networking, cloud, infrastructure, end-user services, and DevOps teams. With VMware, you move past the limitations of fragmented security processes. Your organization can operate from a shared source of truth. Your teams, tools, and technologies can share information and implement security workflows more effectively to operationalize cybersecurity through IT and development. This helps you counteract the impact of the cybersecurity talent shortage.

## Integrating Your Existing Security Solutions

With a simpler, faster, and smarter approach, you can integrate your current security solutions while gaining the freedom of choice that comes with open application programming interfaces (APIs) and third-party integrations. This helps you drive efficiency because you can easily integrate VMware Security products with those already in your environment instead of burdening your staff with coding complex custom integrations. This also enables your teams to collaborate more effectively and increases their speed and agility when responding to new vulnerabilities.

See how real customers overcame security challenges and realized positive outcomes with VMware Security products and solutions. Learn more at `https://via.vmw.com/VMwareSecurityCustomerStories`.

# Notes

# Notes

# Notes

# Notes

vmware®

# VMware Security Blog

Address your cybersecurity challenges with the latest threat landscape insights, security best practices and updates on innovation, shared by trusted advisors, strategists and customers.

Visit the VMware Security Blog
**blogs.vmware.com/security**

## Discover how you can operationalize security for a multi-cloud world

VMware Security helps you implement Zero Trust with fewer tools and silos, better context, and security that's built in and distributed with your control points — users, devices, workloads, and network. With VMware, you get simpler, faster, and smarter security.

## Inside...

- Find out about the current state of cybersecurity
- Look at the three major challenges organizations face
- Discover the value you can get by adopting VMware's security approach
- Consider four key VMware Security use cases
- Look at the top ten reasons to partner with VMware Security

vmware®

**Kathryn Lodato** is Vice President of Security Solutions Marketing at VMware. Kathryn spent more than 20 years building integrated marketing strategies and messaging to accelerate revenue growth in high-tech and SaaS-based companies, including Intel, Zebra Technologies, Forcepoint/Websense, and Crowdstrike.



**ISBN: 978-1-119-87556-7**
**Not For Resale**


for dummies®
A Wiley Brand

# WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.