vmware®

GET STARTED

Simplify Your Zero Trust Journey

For full feature access to this ebook, please view in *Adobe Acrobat*.

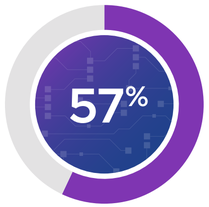
Why change: Complexity kills security

Today's modern enterprise faces a growing security challenge with protecting apps and data. Your organization is innovating and delivering new applications that are built, scaled and operated differently in the modern cloud world. You must now secure a highly distributed workforce that uses a variety of devices to access your apps and data, without hindering productivity.

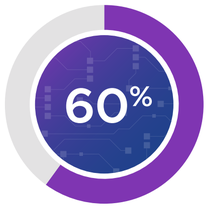
You must also secure your applications and data by supporting both modern and traditional workload types running in diverse cloud environments. Finally, there are the ever-evolving networks used to connect everything. All of this leads to exponentially more surfaces to defend.

Using bolted-on point products focused on narrow use cases, security is viewed as a checkbox activity made worse by siloed teams. Understanding your true vulnerabilities can be close to impossible. Alerts lack context and remediation is slow, providing attackers greater dwell time. And security consumes too much time, money, and effort.

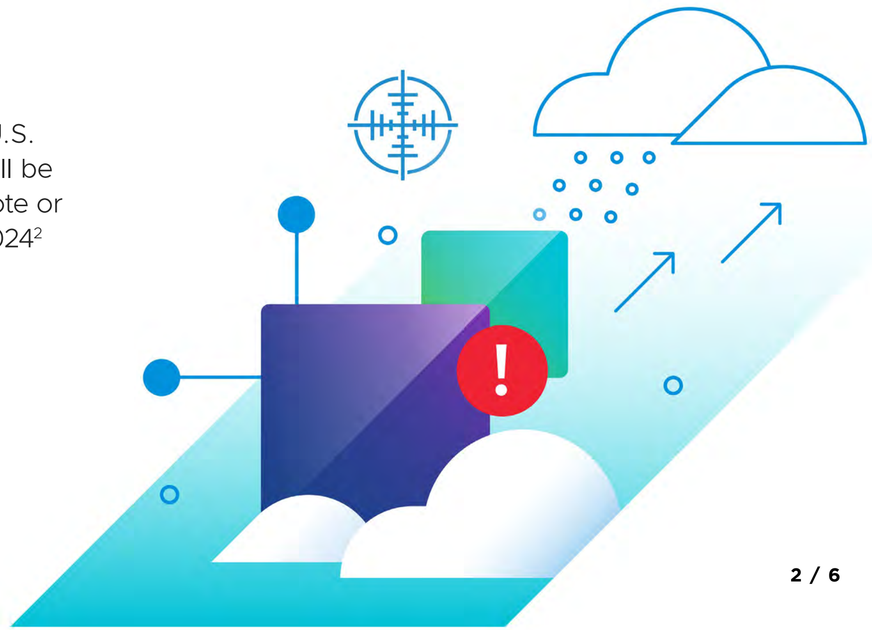
breaches on average per year per organization[1]



of organizations agree there is too much complexity in the security solution industry[1]



of the total U.S. workforce will be entirely remote or mobile by 2024[2]



1. Global Security Insights Report 2021, VMware Carbon Black, June 2021
2. U.S. Mobile Worker Population Forecast, 2020-2024, IDC, August 2020

Today's security challenges

Too many silos

Security, IT, and operations teams each use a plethora of different point tools, generating unique—and often isolated—data in the process. These groups are often siloed from an organizational perspective, with each one having its own approach to managing the specific vulnerabilities and threats. There is no shared context between the core Zero Trust control points of workloads, networks, devices, and users.

3,500+ security vendors exist today across multiple specializations[3]

Too many surfaces to defend

Employees are working remotely from thousands of various locations with workloads traversing multiple clouds. Managing and deploying traditional agent technology to monitor and secure your disparate and evolving environment becomes incredibly difficult. At the same time, you must now consider taking a different security approach to protect all the other environments—legacy data centers to public clouds, VM to containers, desktop to mobile devices.

2/3 of organizations do not have a unified IT and security strategy in place[4]

Too little context

Too often, you are forced to make security decisions with incomplete and inaccurate data. You need deeper context about the assets you are protecting and how your systems fit together to defend against growing threats. A chaotic stream of alerts is insufficient—you're unable to prioritize them to defend your most critical assets first. Point security tools simply don't capture this information. And without the full situational intelligence, your security efforts are flying blind.

- Users +
- Devices +
- Workloads +
- Networks +
- Infrastructure +

3. Cybersecurity Snapshot, Momentum Cyber, November, 2019
4. "Tension Between IT and Security Professionals Reinforcing Silos and Security Strain," a commissioned study conducted by Forrester Consulting on behalf of VMware.

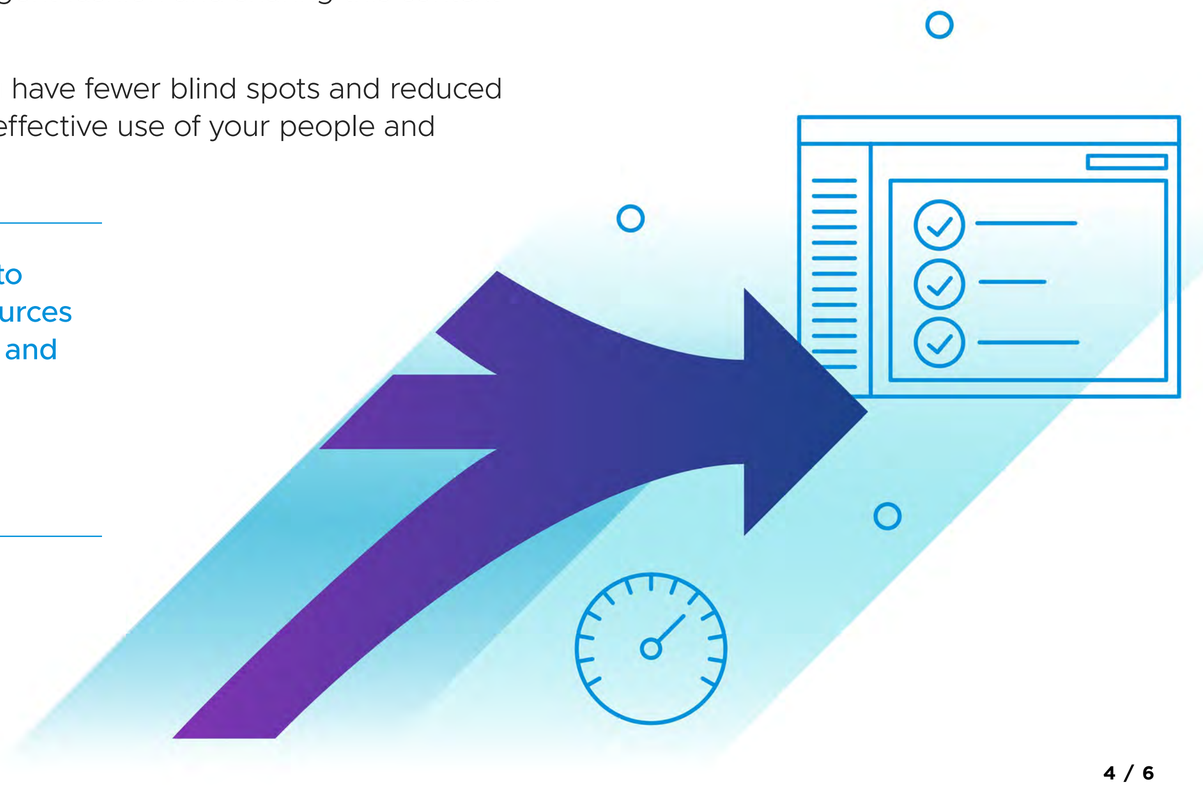
It's time to rethink security

You need to rethink security as 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.

This means a connected approach—joining the critical control points of users, devices, workloads, and networks. Security must be an inherent part of your control points and distributed to where they are across your infrastructure. Finally, information must be presented in context, combining data from all sources in an intelligent fashion and sharing this context across teams to reduce silos.

Your teams are then better equipped to solve the threats of today and tomorrow—you have fewer blind spots and reduced time to detection and response. You can better operationalize security, making more effective use of your people and resources. You can deliver the speed and security required of the modern enterprise.

> "When security and operations work together, it really empowers the security team to move things quickly, and it also gives me the opportunity to take super-scarce resources from the security side and build more security acumen within my network, hosting, and infrastructure teams so that I get really smart technologists that also get security."
>
> SUZANNE HALL
> GLOBAL CISO & VP OF TECHNOLOGY INFRASTRUCTURE
> CIRCLE K



Simplify your Zero Trust journey with VMware

With VMware, security becomes intrinsic to your infrastructure. You reduce your attack surface to mitigate security risk, ensure compliance and simplify security operations and architecture.

Implement Zero Trust with fewer tools and silos

Simply covering the Zero Trust control points of users, devices, workloads, and networks is not enough—you must also connect these critical areas. With VMware, you can accurately understand the security situation and enforce the appropriate policies and actions to close security gaps and reduce risk. This not only enables easier sharing of data between security controls, but also enhances coordination between Security, IT, operations, and development teams to act faster and with greater efficiency. And with fewer security products, you spend less time on administration.

Deliver security as a built-in, distributed service

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 are able to 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.

Scale response with confidence, speed, and accuracy

Your decisions are only as good as the data upon which they are based. With VMware, you will have the full authoritative context of your environment and threat intelligence that is trustworthy, actionable, and readily available. By knowing the threats and seeing whether vulnerabilities in your defenses are being exploited, you can quickly adjust your controls and policies to address security gaps and events faster. You be more adept at identifying and assessing attacks when they occur, enabling you to take the appropriate actions to repair any damage with minimal impact to your organization.

Users +

Devices +

Workloads +

Networks +

Infrastructure +

Get started today

Operationalize **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 network. When security becomes intrinsic to your infrastructure, you reduce your attack surface to mitigate security risk, ensure compliance and simplify security operations and architecture.

Learn More

Join us online:

vmware®

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