Simplify and Strengthen Your Strategy with Intrinsic Security

Using your infrastructure to secure any app, any cloud, any device

vmware®

We need better security

Our connected digital world is extremely reliant on effective cybersecurity. As more business processes become digitized, and workplaces expand on remote work and digital customer experiences, securing our apps, data, and devices is paramount.

More than ever, security and IT leaders are focused on improving their security posture. This includes minimizing risks, deploying consistent security controls, enforcing compliance, and implementing strategies, such as Zero Trust, that maximize protection. Yet achieving those goals is not easy. Most organizations are hampered by having to manage too many bolted-on security solutions with teams that are siloed and often working with limited context and information on the potential impacts of threats.

7 million
data records compromised each day[1]

56 records
compromised each second[1]

Bolted-on solutions

The average company owns upwards of 80 security products. Managing so many products is not easy, especially if each introduces a separate agent or specialized interface. Rather, it creates more complexity for you and makes security harder to manage.

Siloed teams

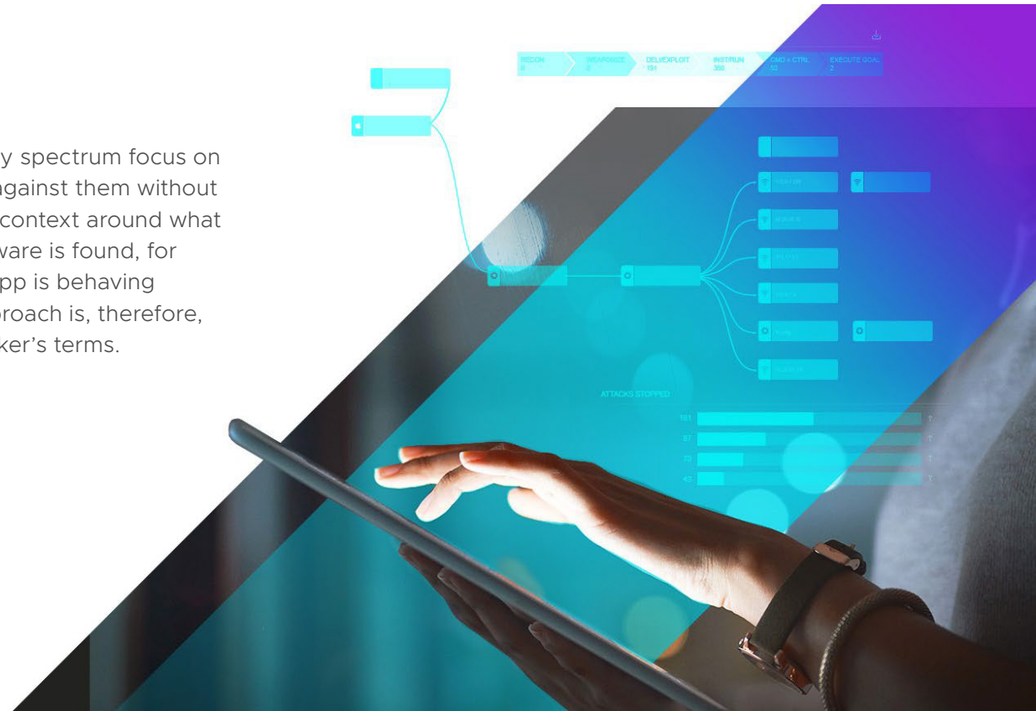
Cybersecurity is a team sport, requiring collaboration between both security and IT teams. Yet all too often, these groups are working in silos, using their own products and tools. That lack of cohesion can prevent teams from working together toward joint solutions.

Threat-centric solutions

Most solutions across the security spectrum focus on isolating threats and protecting against them without providing enough knowledge or context around what they are trying to protect. If malware is found, for example, how can you tell if an app is behaving abnormally? A threat-centric approach is, therefore, always reactive and on the attacker's terms.

More than 3,500
security vendors exist today across multiple specializations.[2]

Two thirds
of organizations do not have a unified IT and security strategy in place.[3]



[1] "The World in Data Breaches," Rob Sobers, Varonis, 2020.
[2] Cybersecurity Snapshot, Momentum Cyber, November, 2019.
[3] "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 think differently

Despite growing IT investments in security, studies show that the likelihood of getting breached is growing steadily each year.[4] It seems that the only thing rising faster than enterprise security spend is security losses. We need to start thinking differently about security.

At VMware, security has long been a top priority. We pioneer revolutionary, software-based approaches to security challenges. Given our unique expertise in infrastructure, we bring a singularly different lens to how we see and think about security. It’s time to approach security in an entirely new way—one that is intrinsic to the resources we use and rely on in our organizations.

Intrinsic security: a new approach

Intrinsic security is a fundamentally different approach to securing your business. It is not a product, or tool, or bundle for your organization. It is a strategy for leveraging your infrastructure and control points in new ways—in real time, across any app, cloud, or device—so that you can shift from a reactive security posture to a position of strength.

Intrinsic security is about using what you have in new ways, so you can help unify your security and IT teams, and empower them with deep context and insights that accelerate how they identify risk, and prevent, detect, and respond to threats.

[4] “Cost of a Data Breach Report 2019.” Ponemon Institute. July 2019. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years.

Intrinsic security is VMware's strategic approach that uses threat intelligence and your infrastructure in unique ways to protect your apps and data.

Built in

Rather than relying on standalone products, an intrinsic approach maximizes security controls built directly into the infrastructure. This is different than integrated security. It is not about taking a hardware firewall and repackaging it as a blade in a switch. It is about reimagining firewall capabilities and building those controls directly into your infrastructure.

Intrinsic security is built directly in software. By leveraging the virtual layer, you can use your existing infrastructure in new ways to protect your endpoints and workloads, networks, workspaces, and clouds, while gaining greater visibility and control over policies that protect your business.

60%
prefer built-in security controls over agent-based solutions[5]

70%
agree security controls should be built into the hypervisor[5]

[5] "To Enable Zero Trust, Rethink Your Firewall Strategy," a commissioned study conducted by Forrester Consulting on behalf of VMware.

Unified

An intrinsic security approach brings tools and teams together by enabling your security professionals to use data and events from IT and operations to more effectively control threats and policies. This unified approach leverages cloud, application, and device infrastructure to provide richer insights about applications and the infrastructure.

By bringing together the technology and insights used by your security and IT teams, your people can collaborate more and increase their agility to respond to new vulnerabilities and active threats.

Context-centric

We believe intrinsic security should provide rich context not just about threats, but about what you are protecting—your endpoints and workloads, networks, workspaces, and clouds.

Context-centric security means you know behaviors and intended actions, including data, users, access points, and configurations. It equips you with powerful intelligence that enables you to quickly understand:

- What workloads compose applications?
- How do they communicate?
- What network services do they consume?
- What users and devices are connecting to those applications?
- What is the posture of those devices?

This context-centric understanding enables you to act faster to prevent or respond to new threats.

> "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

> "A context-centric approach gives us greater insight into what's happening, so we can make the best judgments on how to further secure our environment."
>
> **Kevin Young**, Senior Systems Administrator, Ceridian

What an intrinsic security approach looks like

INTRINSIC SECURITY FOR ENDPOINTS AND WORKLOADS

INTRINSIC SECURITY FOR THE NETWORK

INTRINSIC SECURITY FOR THE WORKSPACE

INTRINSIC SECURITY FOR THE CLOUD

Our intrinsic security approach extends across key security control points with cloud-native endpoint and workload protection.

We provide an endpoint and workload protection platform that allows you to identify risk, prevent, detect, and respond to the latest and most complex attacks. Utilizing our platform modules, you can proactively hunt for abnormal activities using threat intelligence and customizable watchlists. Live response capabilities, like isolating and removing malicious files, enable your teams to respond faster when attacks have been identified.

For workloads and containers, we offer cloud workload protection that combines intelligent system hardening and behavioral prevention so you can protect critical assets against advanced attacks. As with networking, we approach workload security by embedding threat detection and response directly into the virtualization layer. This approach allows the customer to gain intrinsic understanding so they can monitor activity and server workloads.

VMware Carbon Black Cloud analyzes[6]

540TB
of endpoint data per day

1.3T
events per day

[6] VMware internal analysis, October, 2019.

What an intrinsic security approach looks like

VMware uses a software-based approach when it comes to the network. We have moved all network services to software to allow you to control traffic through segmentation, secure network access, and to inspect all traffic—including east-west—for anomalies or vulnerabilities while simplifying management.

For example, the VMware Service-defined Firewall, a distributed, scale-out internal firewall, is built right into the hypervisor. That allows us to distribute firewalling capabilities directly to the servers and workloads.

That unique placement provides a powerful advantage. It enables a more straightforward way to apply security rule sets. Traditional hardware-based firewalling requires you to run all rules against all traffic all the time. But by using our intrinsic understanding of the application and its services, we can tell the difference between the web, application, and database tiers. This approach allows us to apply only the rules that apply to the specific workload, making your approach to security granular, simpler, and more efficient.

We take the same approach with IDS/IPS, using our intrinsic understanding of the services that make up the application to match IDS/IPS signatures to the specific services. Since IDS/IPS signatures are service-specific, and we have an intrinsic understanding of your services, we can apply the right signature to the right service. You get fewer false positives and higher throughput so you can keep your traffic safe.

By implementing the VMware Service-defined Firewall with NSX, customers saw up to

60%

reduction in the number of traditional firewalls required.[7]

[7] VMware internal analysis, ROI/TCO data from DICE, February, 2020.

What an intrinsic security approach looks like

VMware gets high marks for endpoint security for the workspace.[8]

99.8%
protection rate

100%
malware protection rate

6/6
in prevention

6/6
in detection

Intrinsic security extends to the digital workspace. VMware Carbon Black Cloud combines industry-leading unified endpoint management and secure access with threat detection and response capabilities for endpoint security—while providing an exceptional user experience. Intrinsic security gives organizations the ability to turn points of vulnerability into points of control. It allows you to secure users, endpoints, and apps with better visibility to detect, identify, and prevent threats.

Our solution incorporates user, device, and application information with intelligent risk management and behavioral prevention, detection, and response. Leveraging the power of big data, you get a clear and comprehensive picture of endpoint activity using detailed telemetry data so you can investigate endpoints, follow the stages of an attack, and identify the root cause to address security gaps.

This approach enables organizations to implement Zero Trust conditional access, ensuring secure access to apps and improving device hygiene. Zero Trust also extends a least privilege model across users, apps, and endpoints to verify whether:

- Devices are trusted and compliant
- Users are authenticated
- Access is authorized

[8] AV Comparatives, Business Security Test March-April 2020 – Factsheet, 2020.

What an intrinsic security approach looks like

Your security strategy also needs to extend to your cloud infrastructure. With most organizations adopting multiple public clouds, it is imperative that you have a mechanism to detect, manage, and respond to vulnerabilities and threats in these environments.

Delivered as a service, VMware cloud security and compliance solution leverages cloud APIs, change events, threat index feeds, and best practices to help you manage risk across cloud providers.

Our intelligent solution can help you:

- Establish organization-wide best practices based on cloud security benchmarks and compliance frameworks
- Visualize security risks including resource relationships, misconfigurations, change activity, and threats
- Speed up detection and response with real-time alerts and automated remediation across cloud environments
- Drive greater alignment across security, developer, and operations teams by verifying security risks within CI/CD pipelines

VMware cloud security solutions have detected over

7M

security and compliance violations across multiple public cloud environments.[9]

[9] VMware internal telemetry and analysis, June 2020.

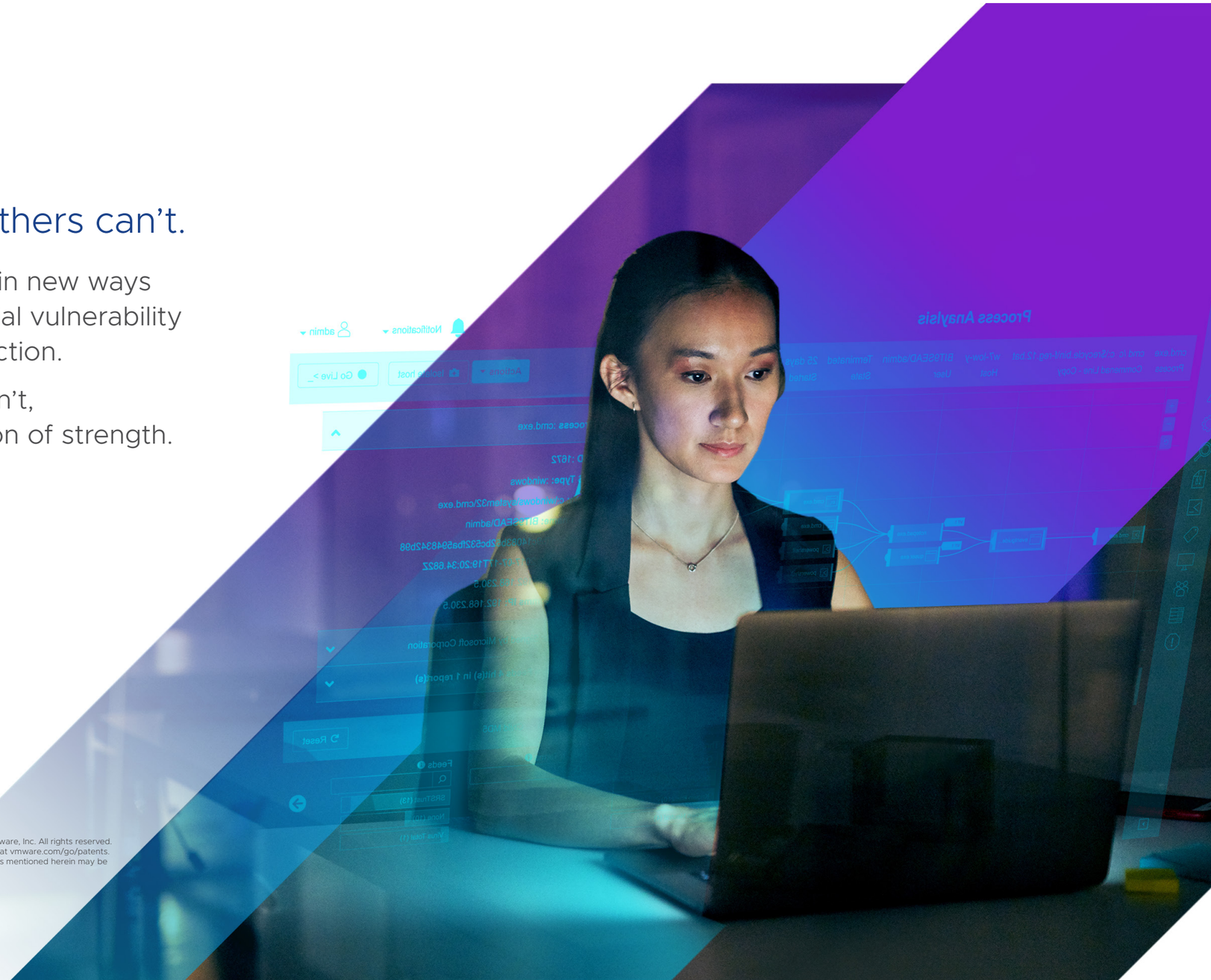
Intrinsic security

Know what others can’t. Do what others can’t.

Leverage your infrastructure and control points in new ways so you can turn every touchpoint from a potential vulnerability into an asset for gathering insights and taking action.

With intrinsic security, you know what others can’t, and do what others can’t, so you are in a position of strength.

Learn more at vmware.com/security



vmware®