Leverage your infrastructure as your security control.

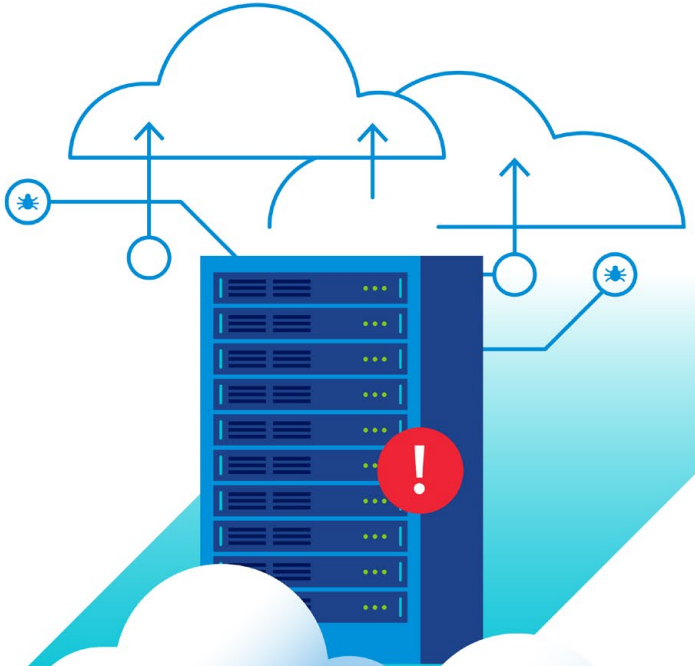
Your challenge:

Complexity can kill efforts to protect workloads

The rapidly expanding attack surface presents vulnerabilities if left undetected. With dozens and even hundreds of security tools in use by most organizations and the number of threats expanding daily, there are plenty of gaps to exploit.

According to the 2019 Forbes Cybersecurity Trailblazers Report, 77% of security practitioners indicated that they have too many point products to track and manage.

Complexity leads to overspending, and for IT, it's also a huge administrative burden to ensure every workload has the proper security agents installed—and all are up to date. Security experts become reluctant systems integrators, constantly writing scripts to stitch all the different security products together. Meanwhile, everyone is frustrated by the difficulty in communicating between teams.



Security system complexity is the most expensive of 25 cost factors, increasing the average cost of a breach by $292,000 for an adjusted average total cost of $4.15m.

IBM Cost of a Data Breach Report 2020

Your solution:

Remove operational impediments

Without coordination between security and infrastructure—and active participation by both teams—your efforts are hamstrung. By partnering with VMware, you will **streamline the process of gathering security data**. You can **extend advanced security functionality** into the vSphere Client Console. And, you will be able to **align your policies across multiple use cases**.

Here's how

Enable security with a single click

The constant demand to monitor and process security data takes your people away from other initiatives—while the performance overhead on the systems limits the speed of operations. With VMware, you **eliminate the need to install multiple dedicated security agents for your vSphere workloads**. Instead of responding to requests, you can proactively monitor for anomalies and remediate vulnerabilities, delivering actionable data as a consumable service to provide greater security coverage. And because there is no additional overhead caused by agents consuming memory or CPU cycles, you're able to devote more of your infrastructure to running the business.

The VMware difference:
Automated risk & response analysis
Ability to assess, prioritize, prevent, and detect risks of workload-specific vulnerabilities and behaviors, and to enable automated responses

Automate your threat and risk analysis

Manual efforts limit speed and perspective. With VMware, you can automate workload analysis to evaluate vulnerabilities and investigate incidents. You can more quickly identify the riskiest behaviors across your environments and apply policies in a consistent, impartial fashion. You can prioritize threats for targeted system hardening while preventing noncompliant actions. Within the VMware ecosystem, you can easily build automation using consistent APIs and integrations.

The VMware difference:
Automated risk & response analysis

Ability to assess, prioritize, prevent, and detect risks of workload-specific vulnerabilities and behaviors, and to enable automated responses

Reduce the number of point security tools

It's tough to align all your security policies when you're constantly flipping between different consoles. With VMware's consolidated toolset, you can easily define, align, and monitor your security application controls across the workload lifecycle. You will eliminate script writing to link your stack together along with multiple agents and training. By giving your security and infrastructure teams access to the same information with the right context, you can drive consistent security across your environments.

The VMware difference: Consolidated security in a single platform

Ability to align multiple security use cases—including response, detection, prevention, and audit—combined with vSphere operational management

When you **remove operational impediments**, you'll save time and resources to focus on high-impact actions that reduce the most risk, automate IT hygiene and compliance reporting, and consolidate multiple security tools into a single platform.

With VMware you'll:

Spend less effort deploying and managing security solutions, and getting more out of your IT environment

Achieve higher fidelity alerts, leading to more targeted, confident, and faster actions

More easily and effectively adjust your hardening to counter future threats

To learn more, please visit **vmware.com**