Focus on high impact actions with confidence.

Your challenge:

It's difficult to prioritize risk and focus resources where they matter.

The sheer number of potential threats across your infrastructure grows every week—more vulnerabilities and more workloads to protect. Many of these new threats consist of non-malware and ransomware, rendering many existing security tools and strategies ineffective.

Compounding this issue is that many of the tools in place are not designed to protect workloads. As a result, they can't address the unique characteristics of different workloads, often causing unintended collateral damage. Nor are these tools helpful in identifying which vulnerabilities represent the most danger to your business. This uncertainty leaves you guessing where you're most likely to be attacked and what the ramifications will be if you are.

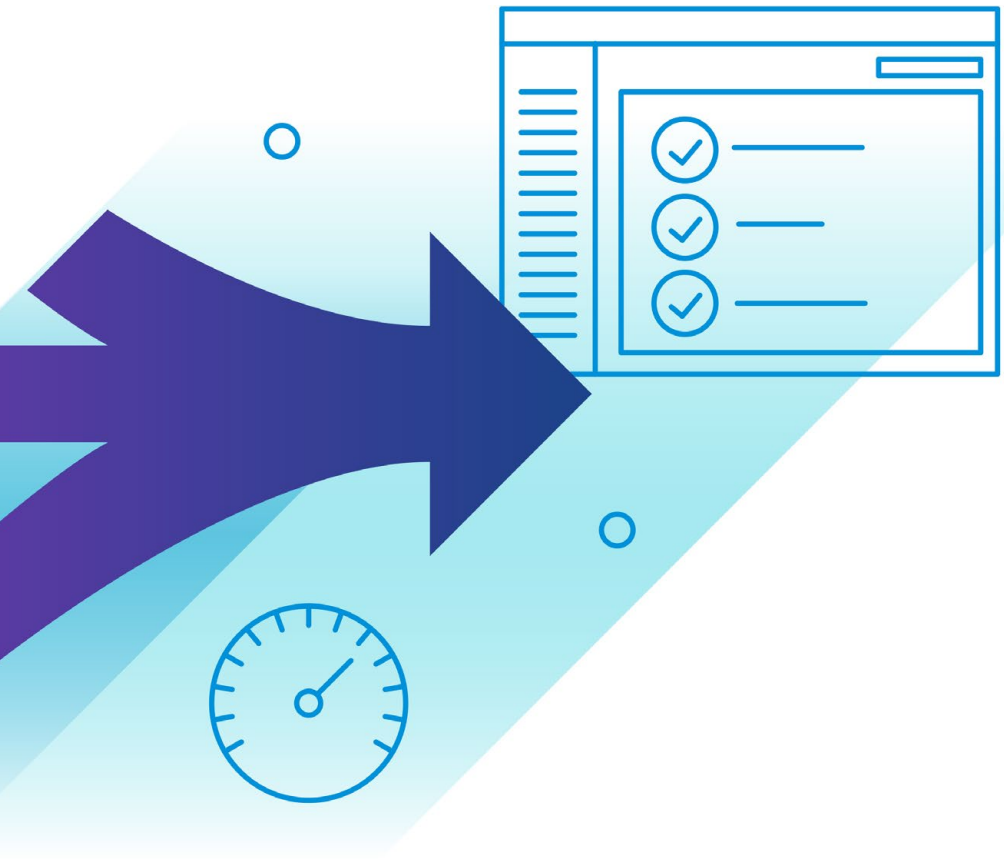
What is certain, however, is that there are numerous known vulnerabilities you just can't get to—either through lack of resources or inability to prioritize. These vulnerabilities represent an unnecessary risk for your environment—and cause incidents that could have been avoided.

On average, organizations have the ability to close about one out of every ten vulnerabilities.

Prioritization to Prediction Volume 3: Winning the Remediation Race, Cyentia Institute research study commissioned by Kenna Security

Your solution:

Focus on high impact actions with confidence.

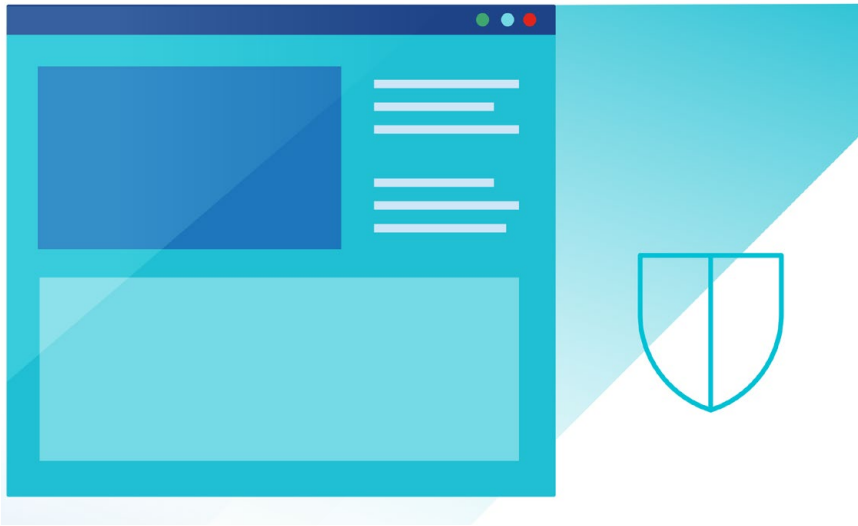


You need to spend your time and resources wisely. By working with VMware, you **will continually analyze your infrastructure and the interdependency of your workloads**. In this way you will **quickly discover when something changes** by assessing, prioritizing, and resolving any potential security impacts. You make these decisions with full awareness of how your environment operates, leveraging VMware's unparalleled knowledge of how workloads behave. And with VMware's open threat intelligence architecture, you will **expand your awareness of emerging threats** through notification of issues encountered by third parties—and then have the ability to quickly protect your workloads.
With VMware, you will have the knowledge to defend what's most important.

Here's how

Automatically prioritize vulnerabilities based on real-world risk

You need to apply your resources quickly—and where they will deliver the most value. With VMware, you can **audit and analyze the security settings and configurations of your workloads** on an ongoing basis. In addition, you can prioritize vulnerabilities based on the actual risk to the business and whether exploits currently exist. With this detailed knowledge, you will **more rapidly patch vulnerabilities and remediate misconfigurations**, closing risk windows as quickly as possible and automating remediation actions via APIs. Additionally, you can more **readily identify and address the breakdowns** in processes that create vulnerabilities in the first place, resolving them once and for all.



The VMware difference: Hardening capabilities

Ability to identify and prioritize high-risk vulnerabilities, audit, and remediate misconfigurations

Expand your understanding of what to look out for.

New threats can surface almost anywhere. With VMware you can **build upon extensive knowledge** by incorporating our threat research team's additional intelligence from third-party feeds as well as information discovered across our user base—including indicators of compromise (IOCs) and watchlists. At the same time, you can **share what you have learned with the community**. Because this intelligence can be directly ingested into the platform in a machine-readable format, you can **automatically trigger actions** based on what you've learned.

The VMware difference: Open threat intelligence architecture

Ability to integrate third-party threat intel and knowledge from the VMware community/user exchange

Understand the intricacies and dependencies within your software stack.

Workloads are not isolated entities, but part of a larger whole. With VMware, you will build a security strategy based on the most extensive knowledge pool of how workloads function in the real world. Working with our solution, you will **gain detailed knowledge** with respect to the reputation of the binaries in your software stack. You will also **know precisely which workloads are talking** with each other—as well as with external addresses—and for what purpose. What's more, you can conduct an automated inventory of your infrastructure to discover unprotected rogue workloads—then deliver this information to vSphere admins within their console so that they can **close vulnerabilities**.

The VMware difference:
Deep workload expertise
Ability to leverage workload expertise developed by running the majority of the world's workloads on the VMware platform

When you **focus on high impact actions with confidence**, you will have better hardening capabilities, a more open threat intelligence architecture, and deep workload expertise.

With VMware you'll:

Act with greater intelligence, speed, and effectiveness in closing security gaps

Thwart more attacks quickly to make a difference

Respond more surgically and better balance business resilience while mitigating risk

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