

Revamping VM to Meaningfully Reduce Risk

Company Overview

In mid-2023, a global consumer goods enterprise decided to take a deep look at its vulnerability management (VM) program and analyze the potential impact of its gaps. This US-based company offers an extensive range of health, beauty, and home care products. Operating in more than 100 countries with 10,000+ employees, it drives over \$7 billion in annual sales.

The company's senior information security specialist, with the company more than 15 years, was tasked with streamlining the company's vulnerability management (VM) program. "In theory, we've always had four pillars to our VM program: scan, report, remediate, and verify," he explains. "In reality, though, we've really only ever been able to do the first two."

Challenges

Unfortunately, incorporating those findings into a more comprehensive approach to VM had complicated an already limited program. "Everything we were doing was manual. We'd run the scans, but using Kenna to do prioritization was totally useless. We didn't have any kind of mature process for remediation, and we weren't even trying to do validation."

The company had been extremely frustrated at the high cost — in both time and money — of trying to implement ServiceNow VR. "It takes many months and many 100s of 1000s of dollars to build any kind of customization into that platform."



PROFILE

Location

Midwestern U.S.

Industry

Consumer Goods

Customer Size

10000+ employees

BACKGROUND

Zscaler Unified Vulnerability Management (UVM), provides continuous risk management, giving large enterprises contextual insights into their top security issues and automated workflows to reduce cyber risk. Built on the patented Data Fabric for Security, the platform curates and correlates data from 100s of sources, in any format and scale, to aggregate risk factors, mitigating controls, and business context.

Solutions

The company tested the Zscaler Unified Vulnerability Management (UVM) with just a few data integrations — vulnerability scanning, endpoint tooling, and web scanning. Right away, the security specialist could see the difference. As the company has evolved its deployment, the teams have realized several additional benefits.

“The UVM platform gives us a much more accurate priority list, combining the vulnerability information with details about our environment to adjust our risk score. Where we have a protected endpoint or an asset behind a firewall, the UVM automatically lowers the risk score for us, and we have all the control over how the platform calculates our risk.”

The other major win for this company is how UVM has automated workflows for remediation.

“The platform automatically creates tickets for the fixes we need, and we’ve been able to create workflows that match how our teams are set up without paying ServiceNow.”

This security specialist and his team consider UVM a key partner in shifting the company’s approach to security. They have gained a more structured perspective, allowing for efficient prioritization of vulnerabilities based on real-world exploitability and the company’s other risk factors and mitigating controls.

The team is also using UVM for the last pillar of its VM program — verification. “With Zscaler UVM, we have an always up-to-date view into ticket status. If a vulnerability has been addressed, and the IT side forgot to close the ticket, UVM does it for them. And similarly, if a vulnerability pops up and someone had closed the ticket, UVM will reopen it. This automation saves us hours and hours each week that we used to spend just synching on status between teams.”

The adjusted prioritization means the right items get worked on, and the automation and efficiency mean the company is succeeding in improving its security posture.

“For the first time, we really have the VM program we’ve always wanted but didn’t think was possible. It’s changed our whole game.”

—Senior Information Security Specialist



Holistic Data Integration

The Zscaler Data Fabric eliminates data silos, enriches contextual information, and enables the company to query and analyze data from various perspectives, enhancing the ability to manage risk effectively.



Effective Prioritization

UVM aggregates and correlates data from the company's vulnerability scanning, endpoint security, and cloud scanning systems now, and the company intends to add findings from its application development testing tools as well. UVM adjusts risk scores to account for risks and mitigating controls.



Enhanced Remediation

By leveraging the UVM capabilities for remediation, the company has implemented efficient and effective measures to remediate top vulnerabilities promptly, facilitating a more streamlined approach to resolving security gaps in its infrastructure.



Streamlined Verification

UVM automates the verification stage of vulnerability management. The company can now automatically close and open tickets as needed to reflect the status of the vulnerability findings, eliminating the back-and-forth needed to validate ticket status.

“We'd been swimming in vulnerabilities, with our different tools finding the same issue over and over. Zscaler UVM immediately deduplicated those findings down to 1 for every 1000 original tickets. That saved us countless hours of manual work.”

—Senior Information Security Specialist



Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/ trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.