zscaler™

Revolutionizing Vulnerability Management

Solution Brief

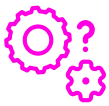
Why is Vulnerability Management Still So Hard?

Despite over two decades of industry focus on vulnerability management (VM), few companies contend they have a highly effective VM program. Gaps continue to leave companies at risk, friction persists between security and the teams responsible for remediation, and breaches leveraging known vulnerabilities are on the rise. Even the most advanced tools have significant shortcomings, including:

Limited Enrichment
CVEs continue to be the focal point, with minimal enrichment tapping threat intelligence. Broadening enrichment to include mitigating controls or other context that might better inform risk level remains beyond reach.

Opaque Risk Calculations
To the extent offerings leverage additional scoring factors, such as exploitability, in their prioritization, the overall risk calculations remain obscure.

Scalability Issues
Tools struggle to handle and process large volumes of data, leading to delays in accessing critical scan results.



Lack of Customization
Most tools support little to no ability to customize risk calculations or meet unique business requirements like workflows for remediation.

Lots of data, but very few answers

These seemingly straightforward questions are surprisingly challenging to answer using existing tools:

- How vulnerable are our most critical apps?
- Are endpoint agents installed everywhere they should be?
- How many assets do we really have?
- Which vulnerabilities my tools are reporting are duplicates?
- Do all of my assets have owners assigned?
- How has our risk posture changed since the last board meeting?

And many others...

Adding to the complexity, the notion of what defines a vulnerability has exploded as the technology stack has evolved. Vulnerabilities are no longer just CVEs — they're also misconfigurations, code flaws, and business logic gaps. But the data you need to capture this breadth of findings –– spanning vulnerability, assets, users, behavior, other business systems –– sites in dozens of separate tools, forcing teams into Excel–based correlation to try to build a complete view.

Enter Zscaler UVM: Enabling Unified Vulnerability Management

Zscaler UVM offers a fresh perspective and innovative solutions to age-old challenges. Our approach is grounded in the belief that effective risk management requires a holistic, data-centric strategy. We stand apart from traditional and second-generation VM aggregation solutions because we start with a focus on how to handle security data broadly, not just how to manage CVEs.

Our innovation lies in our Data Fabric for Security, which can use security data to address a range of challenges. Our Data Fabric for Security enables a breadth of capabilities that help companies uplevel their VM programs with far less time and effort, including:

Comprehensive Data Integration

Aggregate and correlate data from diverse sources to provide a truly unified view of an organization's security landscape.

Rich Contextual Insights

Enrich and contextualize security findings across multiple security tools and business systems, providing actionable insights into security gaps based on an organization's specific risk factors.

Dynamic Risk Assessment

Out-of-the-box multi-factor risk scores that include mitigating controls, derived from industry best practices, that allow teams to see and customize that risk calculation, so companies get a prioritized list rooted in their own environment and unique risk factors.

Automated Workflows

Automated ticket assignment and tracking, built to match an organization's structure and systems, so teams can swiftly respond to the risks that are most likely to cause harm before they can be exploited.

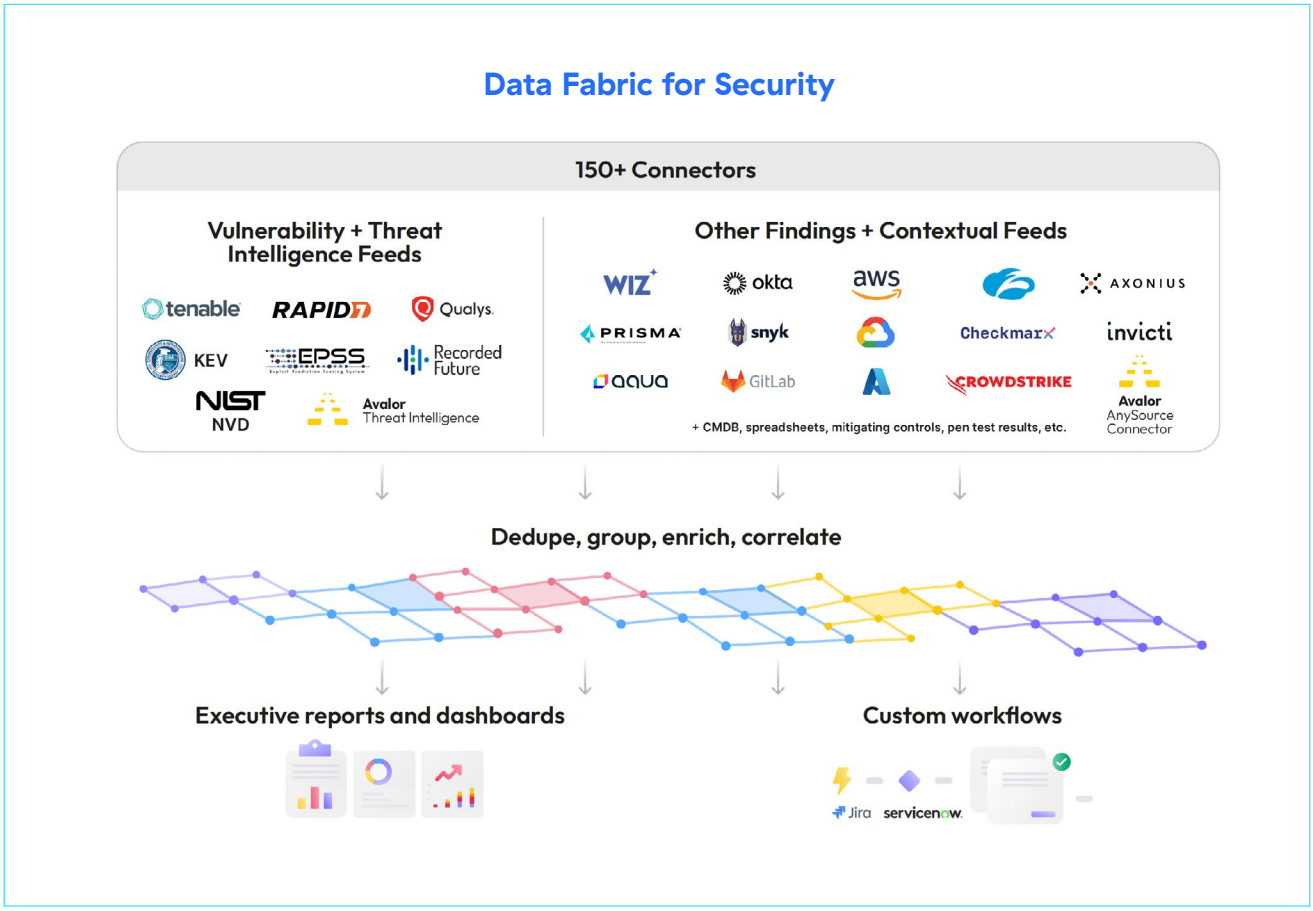
Customizable Dashboarding and Reporting

A rich dashboarding and reporting platform (pulling from a single aggregated and dynamic data set) allows organizations to create the views and reports they need, spanning their own KPIs, SLAs, and other key metrics and providing real-time insights into security posture and team performance.

The Power of the Data Fabric for Security

Vulnerability management, like a lot of security challenges, is a data problem, not a vulnerability problem or a patching problem. That's why the Zscaler team of data experts set out to build the industry's first Data Fabric for Security, with an eye toward building a range of applications on top of our data fabric to address the most challenging security problems.

The Data Fabric for Security curates and correlates data from hundreds of sources, in any format and scale, and our Unified Vulnerability Management (UVM) module uses it to aggregate risk factors, mitigating controls, and business context so organizations can understand their risk in a holistic way for the first time.



Delivering Real-World Impact

Despite its breadth of capabilities, the UVM module is easy to deploy. It takes just a few days to get up and running, and within weeks, customers begin to realize the significant benefits including:

- A Much Better "To Do" List: UVM prioritizes those risks the team should really fix first, so the company can meaningfully reduce its risk exposure.
- Streamlined Operations: Automation means no more Excel time in correlating data, assigning remediation tasks, arguing about priorities, or managing tickets.
- Accelerated Remediation: The right info goes to the right teams, based on an accurate understanding of risk in that particular organization, so the important work gets done.

As a result of these improvements and efficiencies, our customers have realized compelling operational outcomes, including:

1000:1	80%	10x	6	3
average ticket consolidation	**"critical" issues downgraded to "medium"**	**tirage capacity with context**	**moths of custom integration work avoided**	**months time to value**

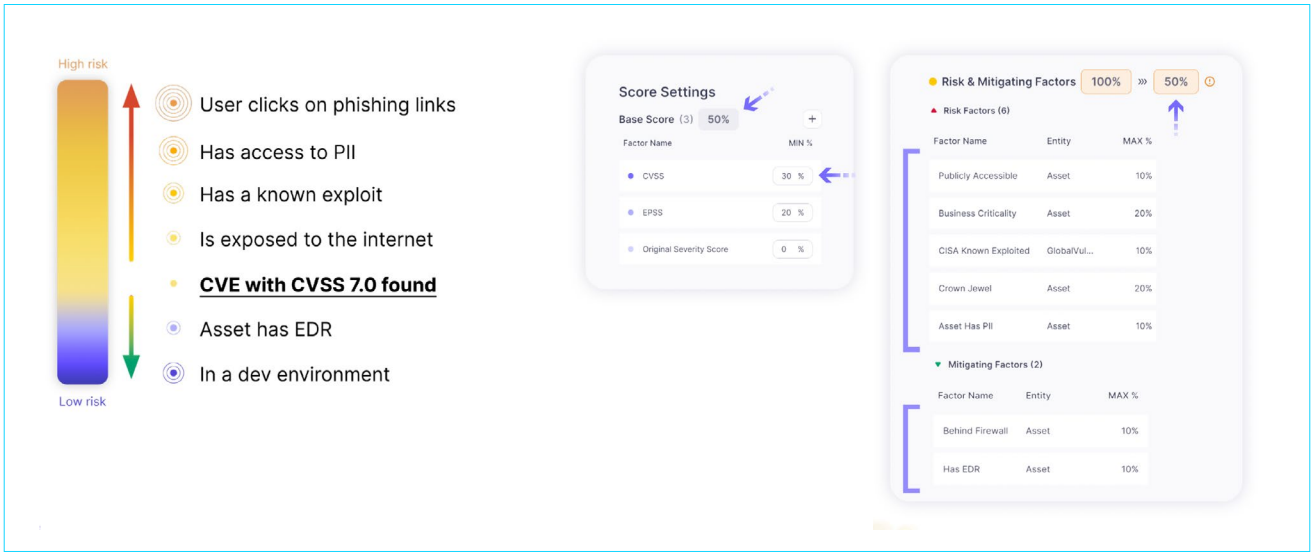
Stop Managing Risk in Spreadsheets

It's time to focus on analyzing data, not compiling it.
UVM empowers security leaders to transcend the limitations of traditional VM solutions and provide a new level of efficacy in security. UVM harnesses the power of data correlation and enrichment to provide organizations with the insights needed to improve their risk posture quickly and effectively.

UVM has also helped organizations reduce the friction between security teams and the IT or developer resources needed to remediate their findings. Having the data be more current, having the risk factors be based on a company's own priorities, and having workflows that match an organization's team structure all mean teams are finally working on the problems that really matter.

The ability of the UVM platform to take into account risk factors and mitigating controls in providing an automated adjusted risk score is one of the more tangible examples of this practicality.

The following example highlights why an IT team can more readily understand why CVE A (the example at the high end of the risk bar) must be fixed now but CVE B (the example at the low end of the risk bar) can wait. This kind of detailed rationale can also spark helpful conversations that further the understanding between groups that can sometimes be at odds.



zscaler™ | Experience your world, secured.™

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com