Avalor

Unified Vulnerability Management

Security – tons of data, very few answers

Companies today have dozens of security tools, but security leaders still struggle to answer basic questions like “How many assets do we have?” or “How vulnerable are our most critical applications?”

Despite having so many tools, CISOs and security teams still face two main challenges:

- The data stays in silos – vulnerability, asset, cloud, user behavior, and other data sit in separate tools
- “Intelligence” is vendor-defined – risk calculations, metrics, workflows, and other insights are hard coded

Avalor – a data-first approach for VM that actually works

Avalor knows data – how to ingest, enrich, and correlate inputs from hundreds of sources. Avalor built a Data Fabric for Security™ that enables companies to aggregate and correlate findings across dozens of security and business context tools to better understand and manage risk.

Our Unified Vulnerability Management module taps into that data fabric to ingest any risk factor or mitigating control, provide contextual risk scores, and support detailed workflows and dynamic reporting and dashboards.

Breadth of inputs

- Traditional vulnerability and threat intel feeds
- Asset details
- AppSec findings and misconfigurations
- Identity and user behavior
- Mitigating controls
- Pen test results
- Flexibility to ingest any desired data source

Contextual prioritization

- Aggregation, de-duplication, grouping, and correlation across 100s of inputs
- Out-of-the-box scoring for immediate utility
- Optional customization of the factors and weighting that constitute your risk score
- Any data source can contribute to the risk score

Automated reporting and workflows

- Reports and dashboards dynamically updated
- Custom workflows matching org structure and processes
- Split/clustered ticketing + auto open/close tickets
- Any data source supported in reporting and dashboards

Delivering results for our customers

Our customers have achieved compelling efficiencies in a short amount of time.

1000:1
average ticket consolidation

80%
“critical” issues downgraded to “medium”

10X
triage capacity with context

6
months of custom integration work avoided

3
months time to value

Avalor

Next-Gen Unified Vulnerability Management

150+ Connectors

Vulnerability + Threat Intelligence Feeds

tenable · RAPID7 · Qualys. · KEV · EPSS · Recorded Future · NIST NVD · Avalor Threat Intelligence

Findings + Contextual Feeds

WIZ · okta · aws · AXONIUS · PRISMA · snyk · Checkmarx · invicti · aqua · GitLab · CROWDSTRIKE · Avalor AnySource Connector

+ CMDB, spreadsheets, mitigating controls, pen test results, etc.

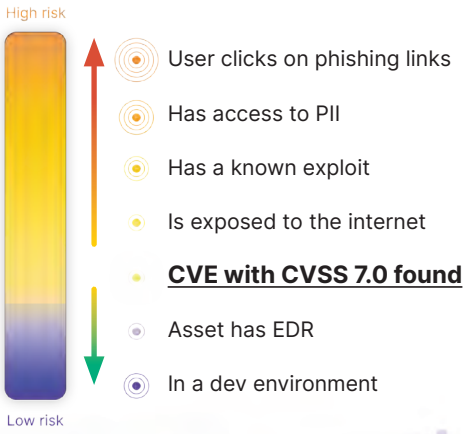
Dedupe, group, enrich, correlate

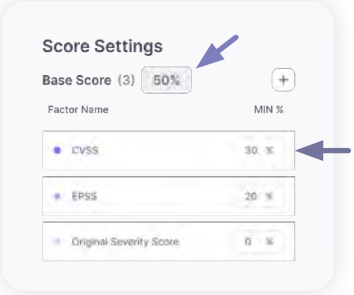
Executive reports and dashboards

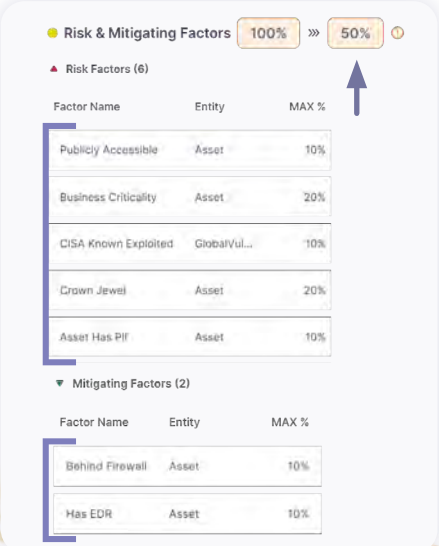
Custom workflows

Focus on analyzing data, not compiling it

Avalor automatically enriches and contextualizes security findings, rationalizing factors that increase and decrease risk to give you an accurate assessment. We provide an opinionated rating, and you can adjust factors and weighting to match your business definition of risk.







Avalor, **a Zscaler company**, 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 Avalor 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. Avalor enables full transparency into and customization of risk calculations and remediation ticket handling. Dynamic reports and dashboards help security teams understand and communicate threat exposure, security posture, and other key risk metrics, all without spreadsheets or BI tools.

SB-UVMOverview-03282024