cymulate

Cymulate Exposure Management Platform

Product Whitepaper

A technical overview of how the Cymulate Exposure Management Platform automates validation and drives an integrated process to improve threat resilience by mitigating threat exposure.

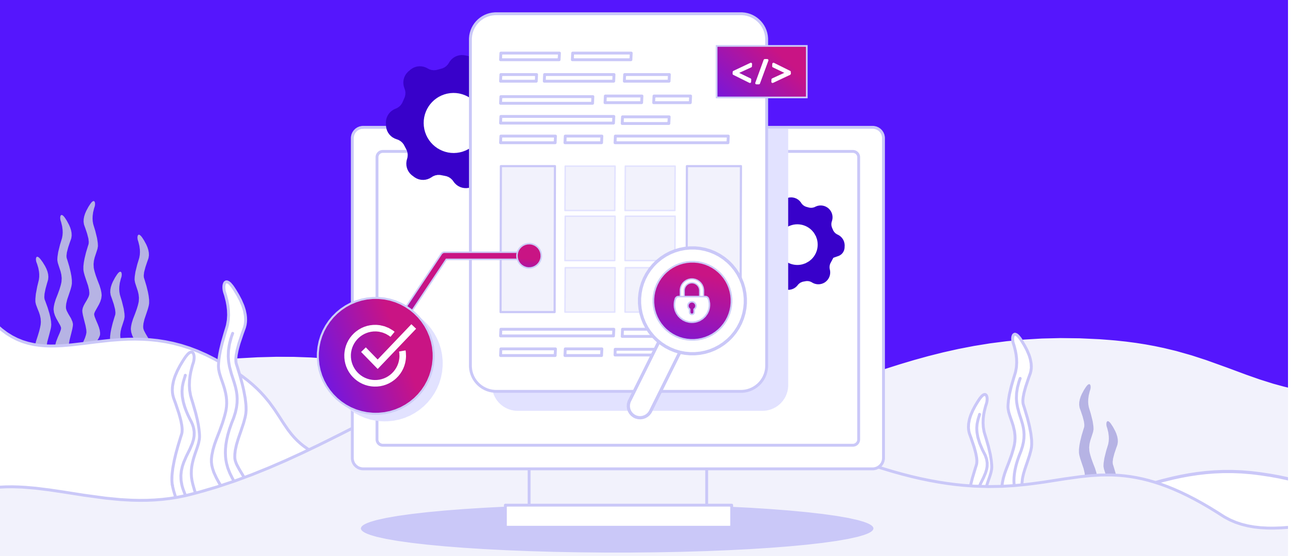


TABLE OF CONTENTS

Introduction

Security teams recognize the need to go beyond detection and response to proactive threat resilience.

Facing a daily backlog of alerts and new vulnerabilities, security teams struggle to understand the urgency of what demands immediate attention and how they can quickly optimize their defenses to mitigate attacks against known vulnerabilities, weaknesses and other sources of exposure.

Continuous threat exposure management (CTEM) closes this gap by giving security operations insight into current exposures and includes validation to test how security defenses perform against real-world threats. With a new understanding of validated threat exposure, security teams can then build threat resilience by escalating urgent remediation and optimizing defenses to provide prevention and detection for the known exposures.

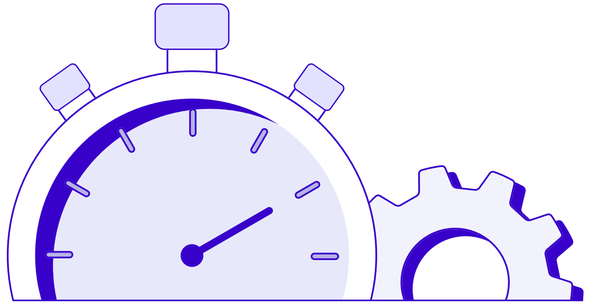
Organizations using Cymulate have demonstrated:

52% **reduction** in critical exposures

30% **increase** in threat prevention

60% **increase** in team efficiency

These results are achieved by unifying exposure discovery, validation and contextual risk analysis in a single platform. By correlating vulnerabilities with validated prevention and detection, Cymulate provides essential validation for every CTEM program. Cymulate includes threat intelligence and business context of affected assets to stack rank exposures based on a comprehensive analysis of risk.



To deliver these results, organizations require an exposure management solution that continuously validates threats within their environment while analyzing exposures in the context of their business. The Cymulate Platform provides this through a cloud-native architecture, lightweight test point and automated data collection via connectors and control integrations.

In this whitepaper, you'll discover how Cymulate is deployed and how each component, from the test point to integrations and exposure analysis, works together to deliver continuous, validated visibility into organizational resilience.

Deployment and Architecture

The Cymulate Platform is cloud-native and delivered as a software-as-a-service (SaaS) platform. This architecture eliminates the need for any on-premises management servers or complex configurations, enabling rapid deployment and low operational overhead.

At the core of the Cymulate deployment is a single, lightweight test point that serves as the bridge between your environment and the Cymulate Cloud. The test point provides the infrastructure needed to both simulate attacks and integrate with security controls, vulnerability scanners and other elements of the infrastructure, such as Active Directory.

Only one test point is required per environment, deployed on a representative system, whether hosted on-premises, in the cloud or across a hybrid infrastructure. Cymulate supports installation on Windows, Linux and macOS, as well as in-cloud environments such as AWS, Azure, Google Cloud and Kubernetes (deployed in either cloud or on-prem environments).

The Cymulate test point is deployed in production environments on a system that mirrors the configuration or “gold image” for that environment. For example, a Linux-based data center requires one Linux test point, while a mixed environment of Windows and Mac user workstations would require one test point per OS type. For testing web applications, no test point is required.

Attack simulations encompass both inbound attacks from the Cymulate Cloud and the test point, as well as outbound simulations from the test point to the Cymulate Cloud. No control integrations are needed for Cymulate to validate threat prevention. However, out-of-the-box integrations allow for validation of threat detection and deeper analysis of threat prevention events, such as logging, policy violations, alerts and more.

Control Integrations

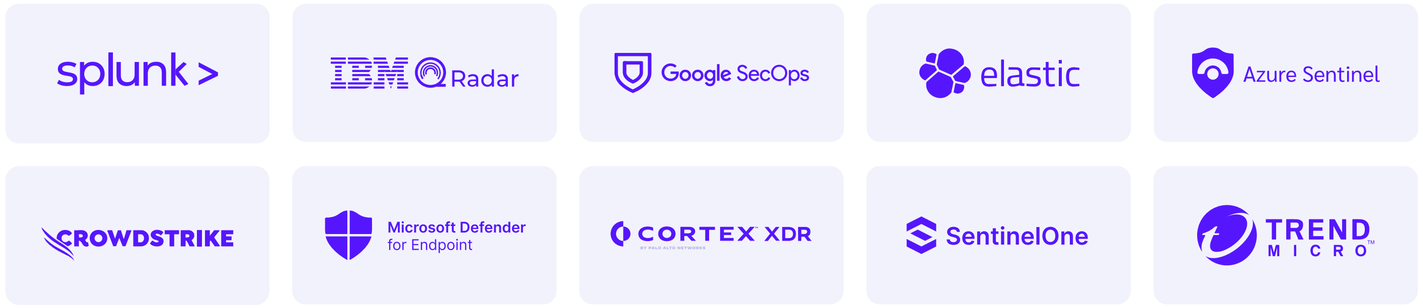
Cymulate integrates with more than 50 security controls to validate detection and analyze how defenses respond to simulated attacks. Through secure, read-only API connections, the test point queries integrated systems to collect data such as:

- Prevention measures taken
- Detection alerts, severity and classification
- Response time
- Policies triggered
- Logs and events

For many controls, Cymulate offers API-based integrations to automatically update security controls to block threats that evaded prevention during simulations.

Here's a complete list of Cymulate-supported control integrations.

Sample of more than 50 integrations, with new integrations added regularly:



> *"The team integrated Cymulate quickly and easily with our other technologies."*
>
> — **Security Assurance Manager and Regional CISO**
> IT Services & Consulting Organization

Connectors, Asset Criticality and Business Context

Cymulate Connectors collect and correlate comprehensive data on an organization's assets and exposures, forming the foundation for accurate risk assessment and business-aligned prioritization. The Cymulate test point securely interfaces with key infrastructure and security tools, including vulnerability scanners, cloud environments, EDR and identity management systems like Active Directory.

The connectors automatically collect and normalize data, including:

- Vulnerability scan results
- Asset inventories and configurations
- User and group permissions
- Exposure details across endpoints and cloud services

The test point securely transmits the collected data to the Cymulate Platform, where it's parsed, correlated and visualized to provide a unified view of the organization's attack surface and security posture.

Once assets and exposures are collected, users can define asset criticality, reflecting each asset's importance to operations and security. Assets are categorized into tiers based on business impact:

- **Crown Jewel (Tier 0)** – The most critical assets, such as domain controllers or administrative accounts, which are essential to maintaining operational integrity.
- **Tier 1–3** – Assets of high, medium and low importance, respectively, ranked by their potential impact on business continuity.

Assets are then grouped into business contexts, which are logical clusters, such as business units, applications, subsidiaries or regions. These clusters represent how different parts of the organization contribute to overall operations and risk.

Each business context is assigned a risk score, calculated as the average of the asset risk scores within that group. This enables clear comparison across business areas, ensuring that the most critical contexts, especially those containing Crown Jewel assets, receive priority in remediation and control enhancement.

Here's a complete list of Cymulate-supported Connectors.

> *"I showed our board of directors the comprehensive visibility that Cymulate provides, and they told me that we needed it before I even had the budget to purchase it."*
>
> **— Liad Pichon**
> Director of Cybersecurity, BlueSnap

Encryption and Safety

All data exchanged between the test point and the Cymulate Cloud is encrypted and adheres to industry-standard security protocols. This ensures that sensitive telemetry and test data remain confidential and protected throughout the assessment lifecycle.

All requests and responses used during the simulation are managed within the platform's secure testing infrastructure. No persistent or sensitive data is stored beyond assessment results and all communications are encrypted in accordance with industry-standard security practices.

Additionally, custom cleanup commands ensure that once an assessment is complete, the testing environment is restored to its prior state, including deleting files, resetting configurations or cleaning injected processes.

Inbound Attack Assessments

For Cymulate inbound threats, the Cymulate Cloud launches an attack simulation targeting the designated test points. Real-world threats, such as phishing emails, web exploits and malware injections that target the organization's environment. These attacks originate outside your network, just like a real attacker would, and attempt to infiltrate through the same channels adversaries commonly exploit.

The Cymulate attack simulations test and validate threat prevention and detection for controls such as endpoint security, email gateway, web gateway, network firewall, network intrusion prevention, web application firewalls, SIEM and more. In coordination with Cymulate Cloud, the test point continuously monitors whether the inbound threat reaches it and how security controls respond to the threat.

> *"When I ran the Cymulate assessment against my newly configured security control, I discovered that it wasn't monitoring or mitigating threats the way I expected it to. I realized then that I needed a solution like Cymulate to independently validate Hertz's security."*
>
> **— Ariel Kashir**
> CISO, Hertz Israel

Outbound Attack Assessments

For outbound threats, the test point initiates the attack simulation in coordination with the Cymulate Cloud. These attack simulations test many of the same controls as the inbound attacks and include data loss prevention. Outbound attack assessments test for threats such as:

- Ransomware and outbound traffic from malware simulations
- Command and control, beaconing and botnet activities
- Data exfiltration through FTP, DNS tunneling and other covert channels
- Endpoint initiated behaviors

During execution, the test point creates network traffic patterns that resemble real attack communications, including malware callbacks, lateral movement and data exfiltration attempts. This phase evaluates how security controls, such as firewalls, proxies, DLP solutions and EDR systems respond to suspicious outbound activity and whether they can effectively detect, block or report these simulated events. The test point monitors how each layer of defense reacts to the outbound simulations.

> *"Cymulate is helping us validate our security controls comprehensively and realistically from both internal and external threats."*
>
> — **IT Security and Risk Management**
> Telecom Company

Web Application Assessments

Cymulate includes web application attack simulations that align with OWASP and common application exploits. Because the assessment focuses solely on web-facing components, no internal test point is required. The user provides Cymulate with the URLs or endpoints of the web applications to be tested. These targets are typically publicly accessible over HTTP or HTTPS and represent the organization's external-facing web assets.

The web application firewall (WAF) assessment launches simulated exploit payloads directly against the provided endpoints, replicating common web attack techniques, including SQL injection (SQLi), cross-site scripting (XSS), remote file inclusion (RFI), command injection and others.

In addition to testing WAF resilience, Cymulate supports configuring and validating web applications that use OAuth 2.0 authentication, enabling assessment of sites protected by modern single sign-on (SSO) methods from identity providers such as Okta, Azure AD, Ping Identity, Google Workspace and Auth0. This allows realistic validation of WAF protections within authenticated areas of enterprise web applications.

Cymulate evaluates how the application, WAF and authentication layers respond to each simulated exploit. Results identify:

- Exploit attempts prevented or not prevented
- Response to harmful requests
- Effective threat mitigation

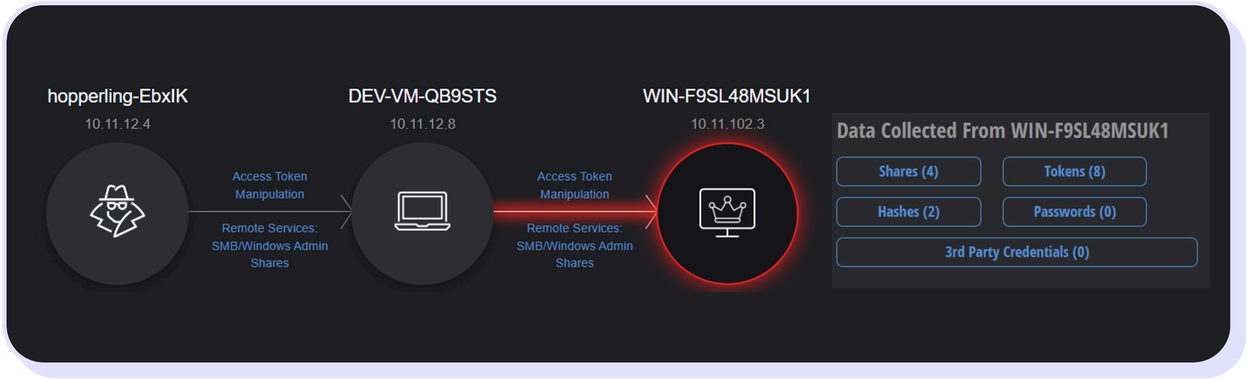
> *"When our executives wanted to rush a compromised server back online, the Cymulate WAF assessment showed that 96% of web-based attacks were still getting through. That validation proved how critical it was to strengthen and continuously test our WAF before pushing anything into production."*
>
> — **SecOps Team Lead**
> Retail Organization

Attack Path Discovery Assessment

Cymulate Attack Path Discovery assessments map potential lateral movement from a compromised host to critical assets, enabling organizations to identify and mitigate risks. The assessment begins with privilege escalation attempts on the compromised host using standard techniques such as token manipulation, service modification and process injection. Once elevated, it collects credentials (e.g., tokens, hashes, Kerberos tickets and cleartext passwords) to expand potential access.

The test point then performs host and network discovery to identify endpoints, accounts, shares and other accessible assets. Using gathered data and credentials, it simulates lateral movement through methods such as Pass-the-Hash, Pass-the-Ticket, Kerberoasting and password spraying. If Crown Jewels are defined, attack paths are mapped toward those critical assets.

Throughout execution, the test point monitors defensive responses to validate whether controls detect, alert or block key attack phases. Upon completion, results are transmitted to the platform, which aggregates findings and provides visibility into successful and blocked techniques, discovered attack paths and prioritized remediation recommendations.



Visualization showing how an agent moved laterally to a workstation and server and the data collected.

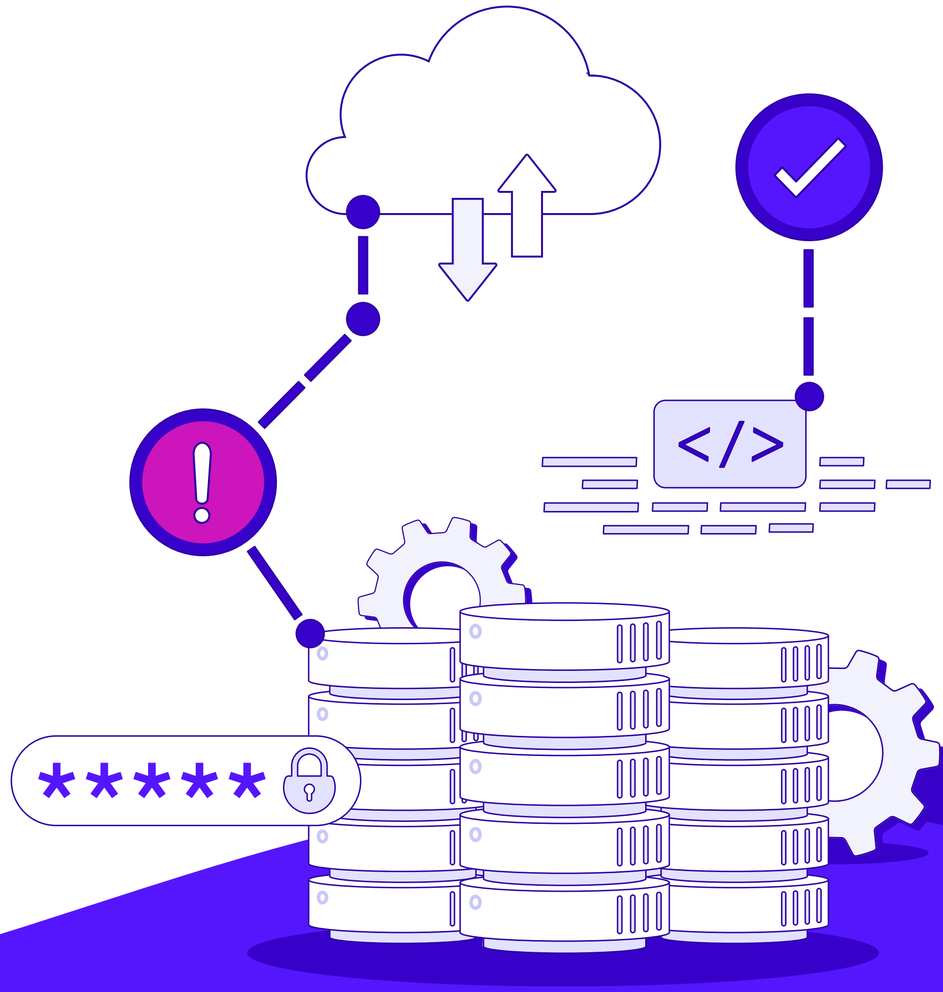
> *"We were unaware that there were open ports in our network, which would have been the easiest way for an attacker to breach our systems. Cymulate alerted us to these gaps and provided remediation guidance, so that we could improve our network segmentation and reduce risk by 98%."*
>
> — **Senior Security Manager**
> Bank

API-Based Assessment Control

Cymulate includes an API that allows users to automate and integrate assessments into their workflows. Through the API, users can:

- Start and schedule assessments for environments and web applications
- Monitor progress and retrieve live assessment data, including payload outcomes and blocked/unblocked exploit attempts
- Fetch detailed findings and reports, listing tested exploits, their success or failure and recommended mitigations

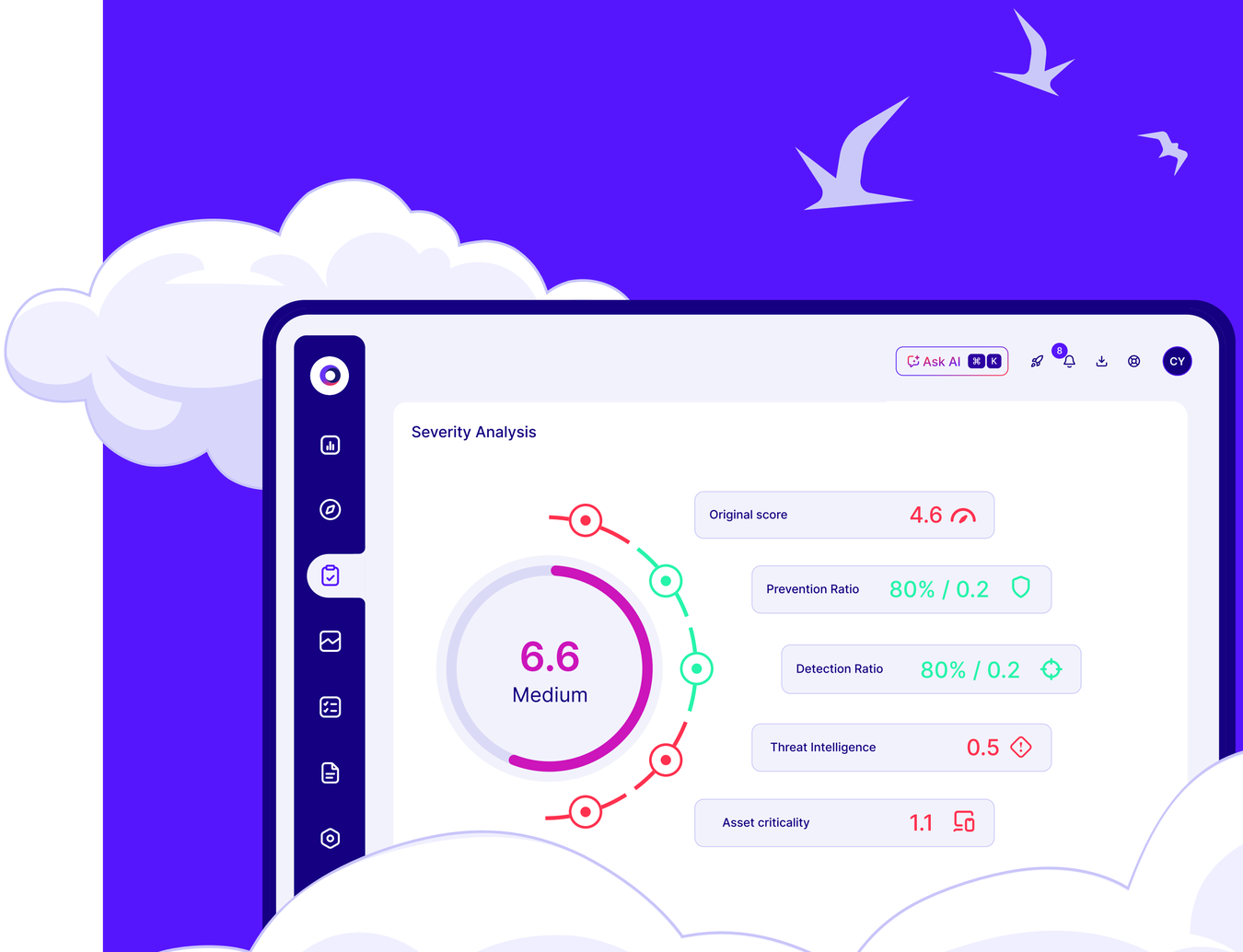
The API also enables integration with external systems, such as SIEMs, SOARs and vulnerability management tools for automated correlation and remediation.



Exposure Analysis

By correlating insights from both exposure data and defense performance, Cymulate enables security teams to identify and escalate the most critical risks. The platform provides actionable guidance to proactively strengthen security controls and policies, ensuring exposures are mitigated through effective prevention and detection.

The Cymulate Platform quantifies and prioritizes vulnerabilities, misconfigurations and other weaknesses by combining vulnerability data, business context, threat intelligence and validated control performance into a unified and validated risk score. This delivers a clear, contextual understanding of exposure impact and remediation priority.



Cymulate calculates a validated exposure score for each exposure using a weighted model that reflects both technical severity and business context. By default, the weighting is distributed as follows:

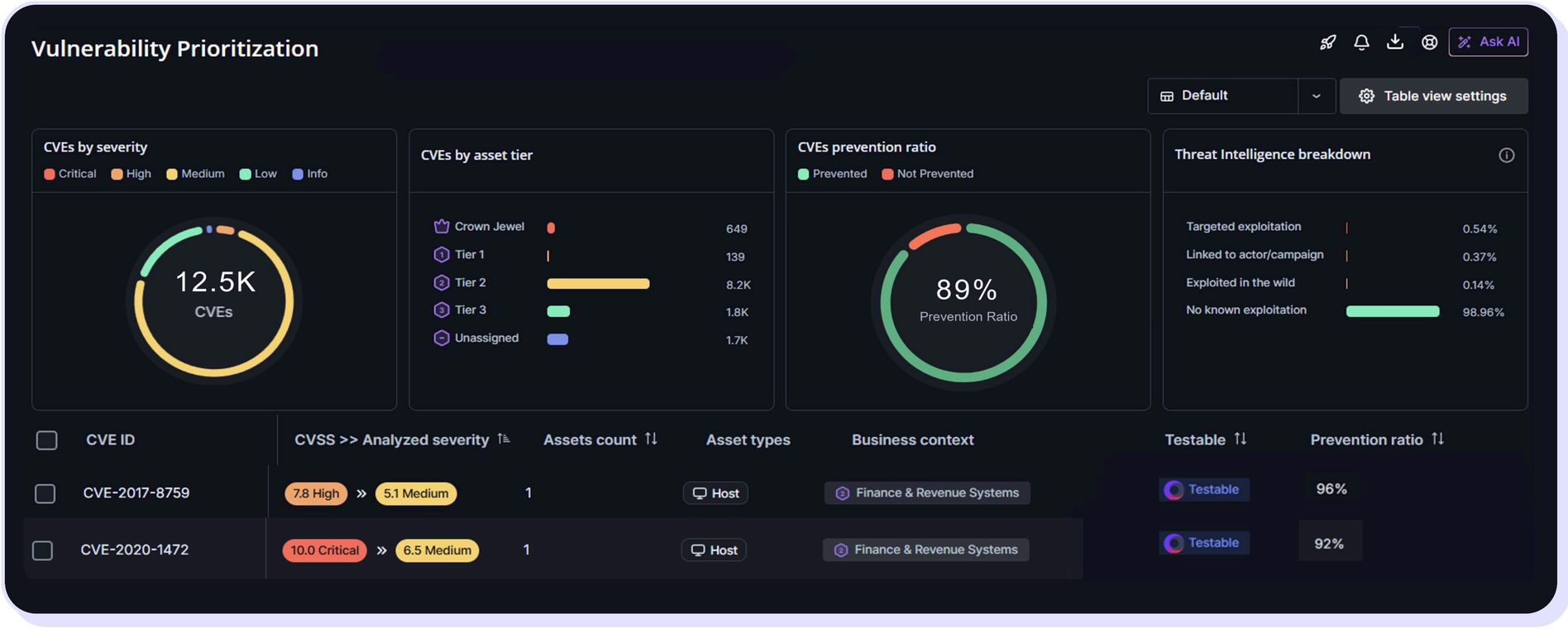
Metric	Weight	What it measures
Original Score	**40%**	The normalized base score, taken from CVSS for vulnerabilities or from the Connector for other exposure types.
Prevention Ratio	**30%**	Results from attack scenarios that test how well your security controls successfully prevented exploitation attempts of the exposure.
Detection Ratio	**10%**	Results from attack scenarios that test how well your security controls successfully detected exploitation attempts of the exposure.
Threat Intelligence	**10%**	Classifies CVEs into four threat intelligence levels, providing deeper context on exploitation activity and relevance: • **Targeted exploitation** – CVEs actively exploited by threat actors or campaigns targeting your industry or region. • **Linked to actor/campaign** – CVEs exploited by known threat actors or campaigns, though not directly targeting you. • **Exploited in the wild** – CVEs observed in real-world exploitation without known attribution. • **No known exploitation** – CVEs with no evidence of exploitation.
Asset Criticality	**10%**	Business impact weighting based on business contexts and the tier of the affected asset.

If no validation history (prevention or detection ratio) exists for a given exposure, *Cymulate automatically correlates and lists all associated attack scenarios. Once these attack scenarios are executed, the existing prevention and detection findings are factored into the severity risk score calculation, which reflects the organization's actual risk, not theoretical risk.*

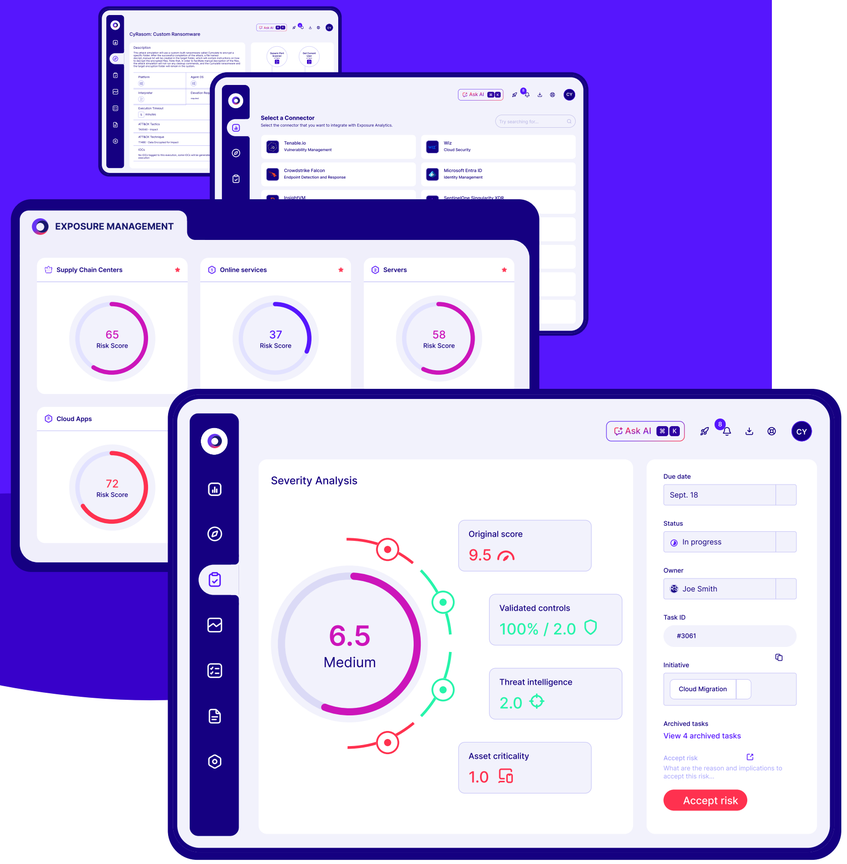
This default weighting provides balanced prioritization across technical, operational and contextual factors. However, organizations can customize these weights to align with their specific risk tolerance, security policies and business priorities, allowing the scoring model to reflect each organization's unique operational context.

In this example, the CVE was originally rated Critical with a CVSS score of 9.3. After applying the Cymulate contextual severity analysis, which incorporates real-world detection and prevention coverage, threat intelligence insights and asset criticality, the rating decreased to Medium with a score of 6.6. This new score reflects its true operational risk.

Findings are consolidated in Cymulate dashboards and reports, providing visibility into exposure severity, asset risk and prioritized remediation steps. Follow-up validations confirm that mitigation actions are effective and that the organization's overall security posture continues to improve.



Organizations receive automated and actionable dashboards to view metrics and filter their most critical vulnerabilities, prioritizing them effectively.



See Cymulate in Action

Validation transforms exposure management from a theoretical exercise into measurable risk reduction. Cymulate enables security teams to continuously test, validate and improve their defenses against real-world threats, providing quantifiable results in prevention, detection and prioritization.

Schedule a Cymulate Demo

Experience how continuous exposure validation and exposure management can strengthen your defenses, streamline your workflows and deliver measurable resilience gains.

Start Your Live Demo

cymulate

About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. Cymulate integrates with assessment tools and continuously tests defenses against the full kill chain of attack techniques providing cybersecurity teams with the automation and insights to prove and optimize threat resilience; accelerate detection engineering; drive continuous threat exposure management; and measure and baseline security posture. Prove the threat. Improve resilience. For more information, visit www.cymulate.com.