DATA SHEET

Cymulate Exposure Analytics

CISOs and their teams are being challenged to report on cybersecurity risk and resiliency in ways that are consumable by both technical and business leadership. This requires a new approach to create both a consistent view of security posture and an actionable improvement plan.

Today, cyber programs require separate tools to find vulnerabilities, assess attack surface exposures, gather threat intelligence, and test security controls. Pulling this data together is often manual and too focused on technical or operational metrics without reference to business impact. Automating this aggregation and applying business contextual analysis is an essential step in moving from one-off threat mitigation projects to a repeated program that Gartner calls continuous threat exposure management (CTEM).

CTEM creates a common language for managing risk and resilience. By aligning with this program, organizations gain a framework to scope, discover, prioritize, validate, and mobilize their cybersecurity initiatives. However, without the means to aggregate and correlate data from multiple sources and align the data with business context, CTEM programs lack the means to fully scope their initiatives, effectively prioritize based on business risk, and mobilize teams to action.

Correlate and Analyze Third-Party Data for Risk-based View of Security Posture

Cymulate Exposure Analytics is a data aggregation and exposure intelligence solution that collects data from across enterprise IT, clouds, and the security stack to support exposure management programs to measure and baseline cyber resilience, focus on the biggest risks, and accelerate mitigations. Cymulate Exposure Analytics pulls data from vulnerability management platforms, asset inventories, clouds, security controls, and the IT infrastructure. Data are aggregated to contextualize the information with business relevance, prioritize remediation, and measure and optimize cyber resilience.

Deployed on its own, Cymulate Exposure Analytics creates centralized intelligence and visibility to security posture with business context essential to an exposure management program. When deployed as part of the Cymulate Exposure Management and Security Validation Platform, the total solution enables and optimizes CTEM programs by merging the traditional vulnerability-based view of risk with the “attacker’s view” of the attack surface.

Benefits

- Focus on the greatest risks with business context, attack surface assessment, and security validation
- Accelerate mitigation by mobilizing teams to action with a full view of the business impact
- Baseline cyber resilience by measuring the risk posture of business systems and security tools
- Deliver cybersecurity performance metrics for leadership, audit committee, and board reporting

Cymulate Exposure Analytics visualizes data by business contexts (business unit, programs, sensitivity to downtime, or other factors) and assigns assets to one or more contexts. By correlating exposure potential with business information, Cymulate Exposure Analytics quantifies risk and resilience so security teams can make informed data-based decisions and provide better insights to strategic leadership and company boards.

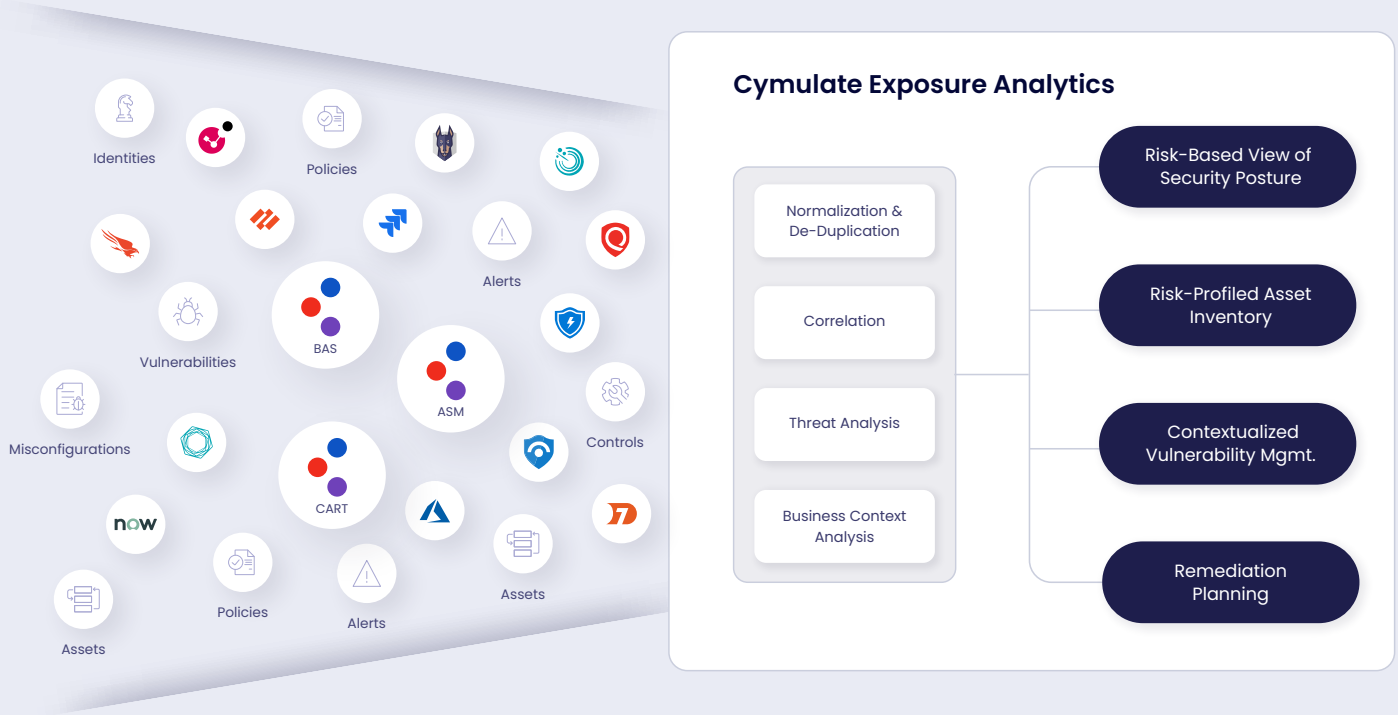
Cymulate Exposure Analytics:

- Correlates exposure potential with business context
- Reports on issues to be addressed, in context, by risk and area of responsibility
- Creates remediation plans to reduce exposure and close gaps
- Baselines risk and security posture with continuous assessment and improvement tracking
- Builds risk metrics and performance tracking for CTEM program scoping and mobilization

Security Data Fabric Fuses Technical Data with Business Context

With its integrations and visibility to the IT infrastructure and security stack, Cymulate Exposure Analytics creates a security data fabric that combines cybersecurity vulnerability data and control validation with business context. Through integrations with existing systems or user-driven tagging, organizations enrich the technical data of vulnerabilities and control effectiveness by assigning assets to one or more pre-defined "business contexts" (business unit, sensitivity to downtime, etc.). This security data fabric provides the ability for Cymulate Exposure Analytics to translate traditional vulnerability management data into an exposure management program with:

- Diagnostic analytics on the current state of threat exposure relevant to the organization
- Predictive analytics on the probability of a threat event and its risk to the organization
- Prescriptive analytics for recommended actions considering multiple options for remediation/mitigation options



Cymulate Exposure Analytics is available in two options.

Cymulate Exposure Analytics - CVM

Provides a full-featured option with the contextualized vulnerability management (CVM) capability, including integrations to vulnerability management solutions and other Cymulate products.

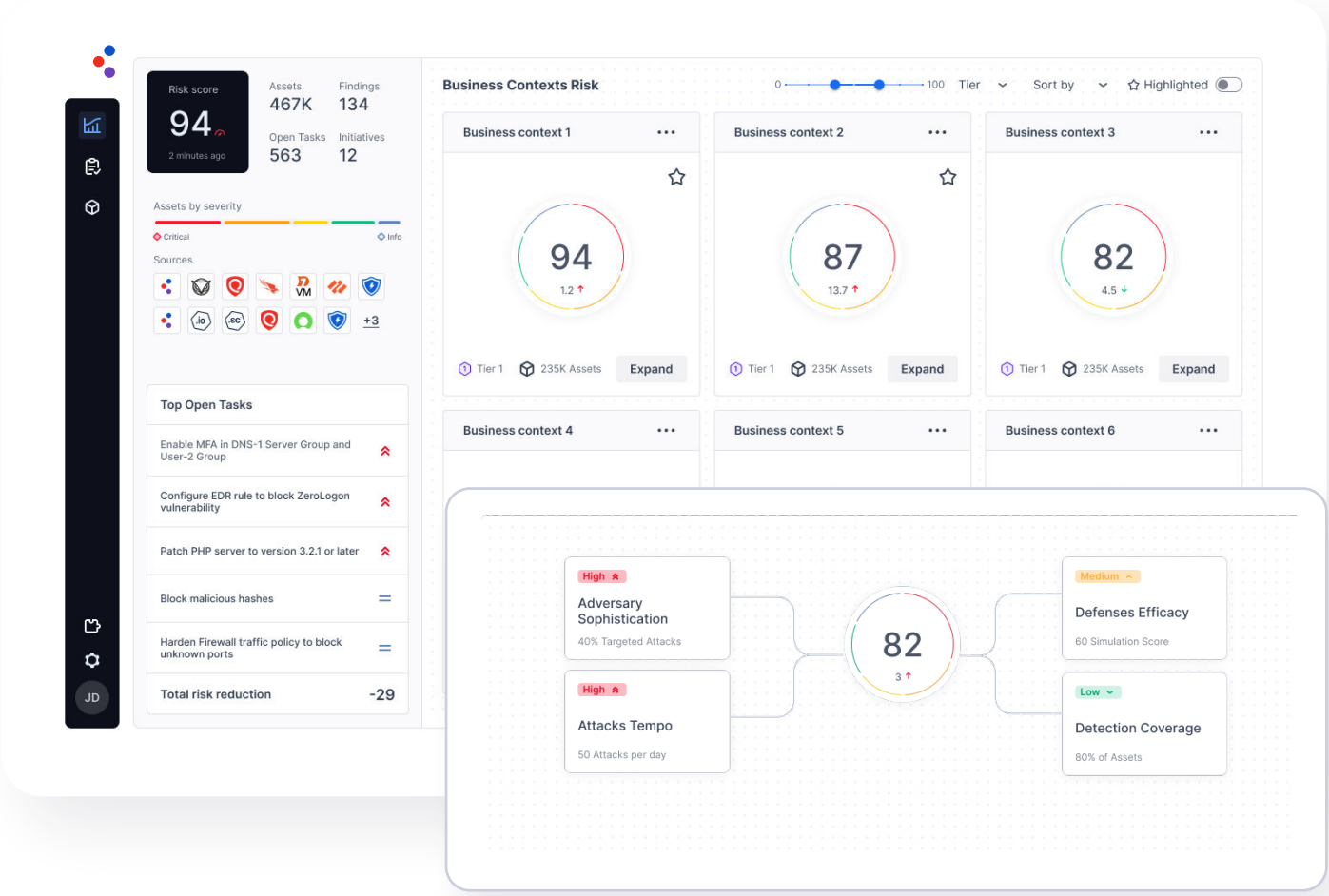
Cymulate Exposure Analytics - Enterprise

Provides a full-featured option with correlated analysis of any third-party data (including vulnerability management solutions) and other Cymulate products.

Risk-Based View of Security Posture

Cymulate Exposure Analytics quantifies risk as a key metric of cyber resilience to understand security resilience and business risk. Risk scoring considers the attack surface, business context, control efficacy, breach feasibility, and external data such as CVSS scores and threat intel.

With dynamic reporting and dashboards for baselines and visualizations, Cymulate Exposure Analytics empowers security leaders to measure and communicate cyber resilience and risk to executives, boards, and their peers. Cymulate Exposure Analytics presents a risk posture view for the organization with an option for a hierarchy of business units, mission-critical systems, and business operations.



Organizational risk and resilience are quantified, baselined, and broken down into different business contexts. This is visualized alongside security initiatives with the highest risk reduction impact.

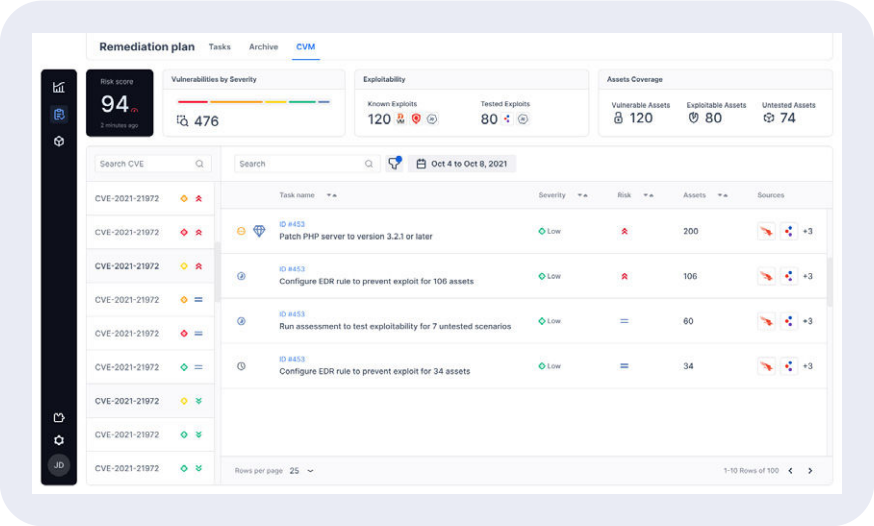
Risk-Profiled Asset Inventory

Cymulate Exposure Analytics creates a consolidated view of assets with context to their risk. The product aggregates data from vulnerability management, attack surface management, configuration databases, Active Directory, cloud security posture management, and other systems. Then it applies its risk quantification to score each asset. This risk-profiled asset inventory contains a quantified risk score for every endpoint, system, cloud container, virtual machine, application, email address, web domain, IoT/OT device, and more. This data can also be aggregated by business or operational context. The inventory includes details for each asset, including:

- Existing security controls
- Current enforced policies
- Known vulnerabilities
- Un-patchable vulnerabilities or security gaps
- Mitigation status
- Device type

Contextualized Vulnerability Management

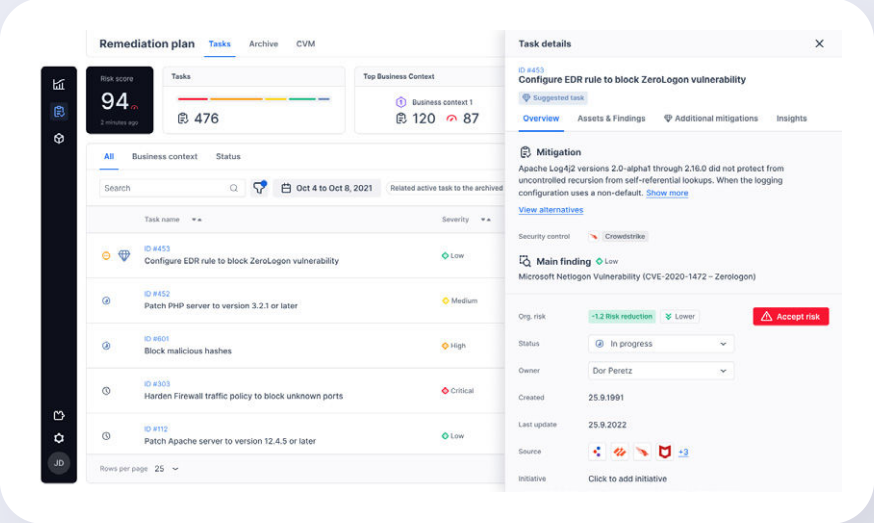
Cymulate Exposure Analytics integrates with common vulnerability scanners and cybersecurity validation solutions to continuously provide organizations visibility, context, and risk for each vulnerability. Rather than simply prioritizing based on CVSS scores, Cymulate Exposure Analytics provides contextualized vulnerability prioritization that correlates vulnerability findings with business context and security control effectiveness. By integrating with tools for breach and attack simulation and continuous automated red teaming, Cymulate Exposure Analytics creates a risk score that considers the exploitability and effectiveness of compensating security controls.



Contextualized vulnerability management aggregates data from multiple vulnerability management tools and correlates it with attack simulation results to prioritize the most exploitable vulnerabilities.

Remediation Planning

Cymulate Exposure Analytics applies its risk quantification and aggregated asset inventory to create a prioritized list of mitigations that deliver the most significant risk reduction and improve cyber resilience. When available, the remediation plan presents remediation options that consider urgency, severity, and compensating controls – as well as the forecasted outcomes by modeling the risk impact of the mitigation.



Remediation plans provide mitigation guidance and prioritization based on the severity of threats and on the overall impact on critical assets and business context.

Easy Deployment for Comprehensive View of Security Posture

Cymulate Exposure Analytics delivers a complete view of security posture via a cloud-based software-as-a-service (SaaS) application. Cymulate Exposure Analytics can ingest and process any data from any source in any format through API integrations or manual uploads.

To support the data collection and integration with the IT infrastructure, clouds, and security controls, Cymulate Exposure Analytics include a service-based agent installed at the customer premise within a customer environment – typically one per agent. The agent includes API connectors that integrate with third-party data sources. With its API connectors, the agent pulls JSON files from the integrated data sources and then transmits data to the Cymulate Cloud, where the data is normalized, de-duped, and mapped into a taxonomy. Alternatively, users can upload CSV or XML files to the Cymulate Cloud.

Map Cyber Security Posture to Control Frameworks & Compliance

When analyzing data for cyber resilience, business contexts can expand to include security control frameworks and regulatory compliance requirements. Cymulate Exposure Analytics then scores and baselines the security posture against those frameworks and compliance so that security leaders can visualize the current state and track changes over time.

Sample Mappings

- ISO 27001
- CIS Critical Security Controls
- NIST 800-53
- PCI
- HIPAA
- GDPR
- FISMA

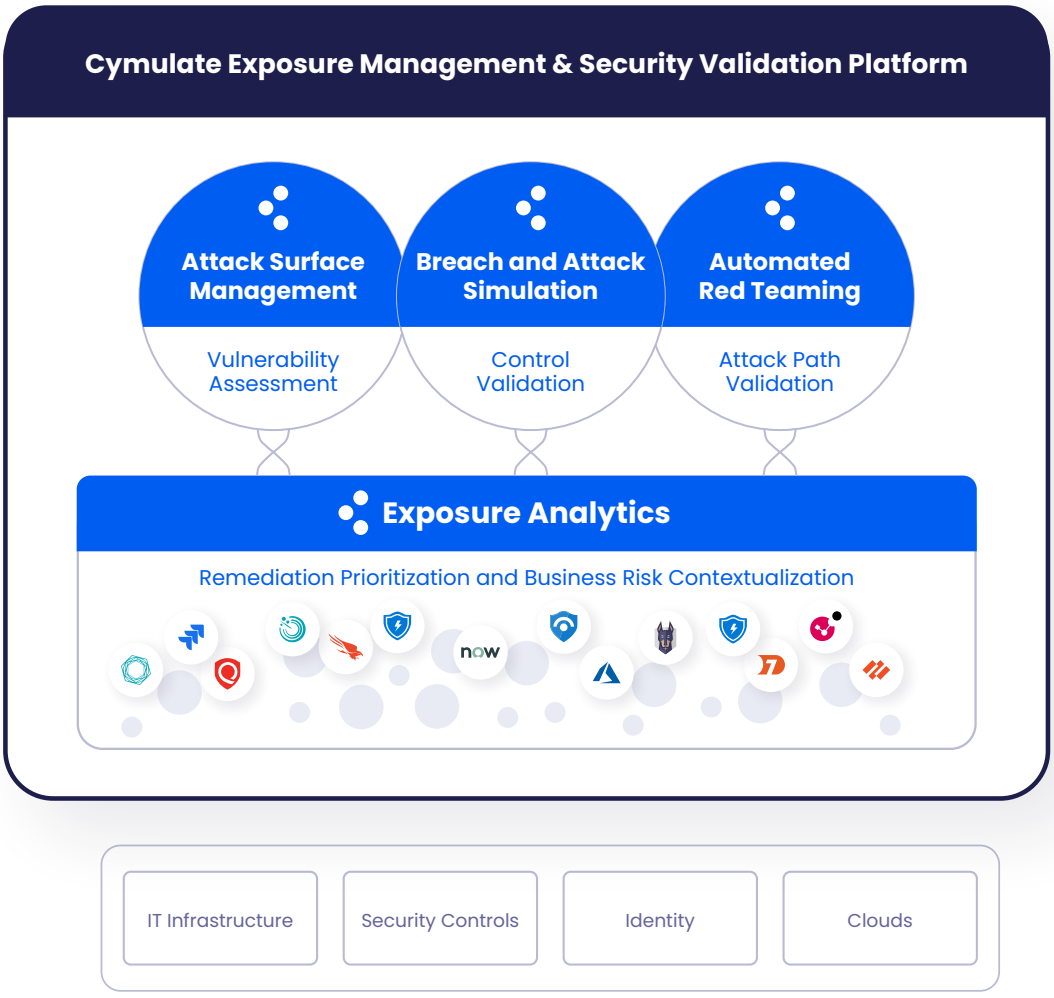
Integrations

Cymulate Exposure Analytics aggregates information from across the IT and security stack to create a security data fabric that combines internal control views with an external attacker view of viable targets.

Sample Integrations	Vulnerability Management	Endpoint Protection & EDR	Cybersecurity Validation	Attack Surface Management
	○ Tenable ○ Qualys ○ InsightsVM by Rapid7 ○ Nessus	○ CrowdStrike ○ Microsoft Defender for Endpoint	○ Cymulate Breach and Attack Simulation ○ Cymulate Automated Continuous Red Teaming	○ Cymulate Attack Surface Management
Application Security	**Cloud Security Posture Management**	**Configuration Database**	**Active Directory**	**IT Service Management**
○ Snyk ○ Tenable ○ Qualys ○ Rapid7	○ Microsoft Defender for Cloud ○ Dome9 by Checkpoint ○ Prisma by Palo-Alto Network	○ Microsoft	○ Microsoft Azure Active Directory	○ ServiceNow ○ JIRA

The Cymulate Platform

Cymulate Exposure Analytics is available both as a standalone SaaS offering and as an integrated offering within the Cymulate Exposure Management and Security Validation Platform. The Cymulate platform provides a comprehensive and scalable solution for security leaders, regardless of their security posture maturity, to drive their continuous threat exposure management program and support both the technical and business requirements of scoping, discovery, prioritization, validation, and mobilization.



About Cymulate

Cymulate, the leader in exposure management and security validation, provides a modular platform for continuously assessing, testing, and improving cybersecurity resilience against emergent threats, evolving environments, and digital transformations. The solution has a quantifiable impact across all five continuous threat exposure management (CTEM) program pillars and on a business's ability to reduce risk by understanding, tracking, and improving its security posture. Customers can choose from its Attack Surface Management (ASM) product for risk-based asset profiling and attack path validation, Breach and Attack Simulation (BAS) for simulated threat testing and security control validation, Continuous Automate Red Teaming (CART) for vulnerability assessment, scenario-based and custom testing, and Exposure Analytics for ingesting Cymulate and 3rd-party data to understand and prioritize exposures in the context of business initiatives and cyber resilience communications to executives, boards, and stakeholders. For more information, visit www.cymulate.com.

Contact us for a live demo

Start Your Live Demo

info@cymulate.com | www.cymulate.com