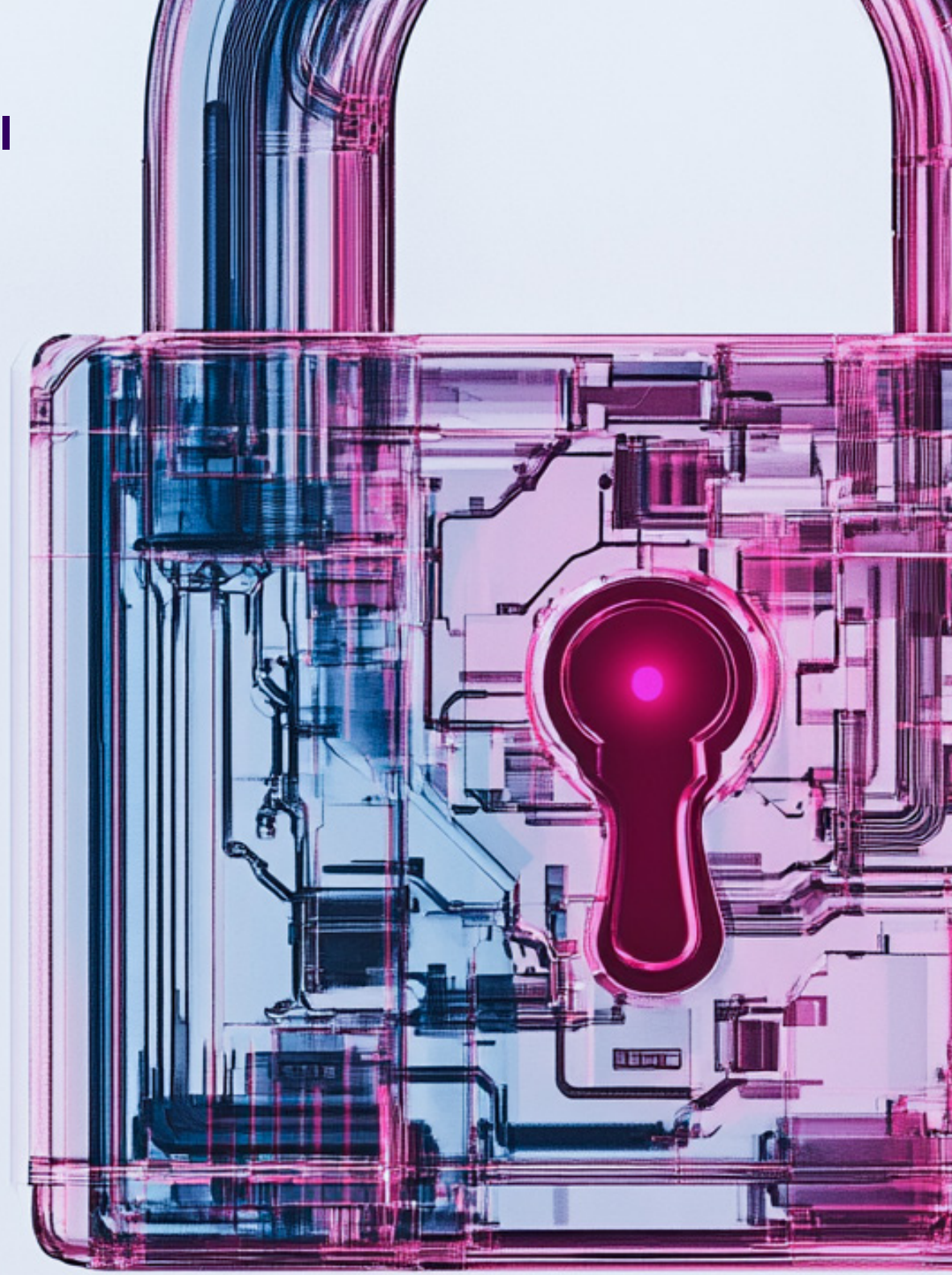
VERITI



Exposure Management Playbook

Introduction

Without an accurate understanding of vulnerabilities, misconfigurations, and exposures, the journey toward reducing risk and maintaining a resilient infrastructure cannot begin. Effective assessment means more than just running periodic scans or generating a list of vulnerabilities. It requires a comprehensive, real-time understanding of the configurations, tools, and attack surfaces that define your organization's environment.

Identifying vulnerabilities is just the first step in exposure management. The real challenge lies in determining which ones matter most and addressing them without wasting resources or disrupting operations. With cyber threats becoming more sophisticated and pervasive, the ability to prioritize exposures effectively is crucial.

Knowledge without action is a missed opportunity. Assessing vulnerabilities and prioritizing risks are crucial first steps, but true security is achieved only when exposures are effectively addressed. Mobilization, the ability to act swiftly and decisively, is the last mile of an effective exposure management program.

Part 1

Assessment

Discovering Your True Attack Surface

Modern assessment approaches leverage agentless, API-driven integrations with security tools to perform continuous scans of configurations and exposures across all critical environments. These integrations provide organizations with a consolidated view of their attack surface, delivering actionable insights into potential risks.

Your attack surface is only as visible as the security tools you are connected too.

A comprehensive assessment platform consolidates data from a variety of tools and layers, including:

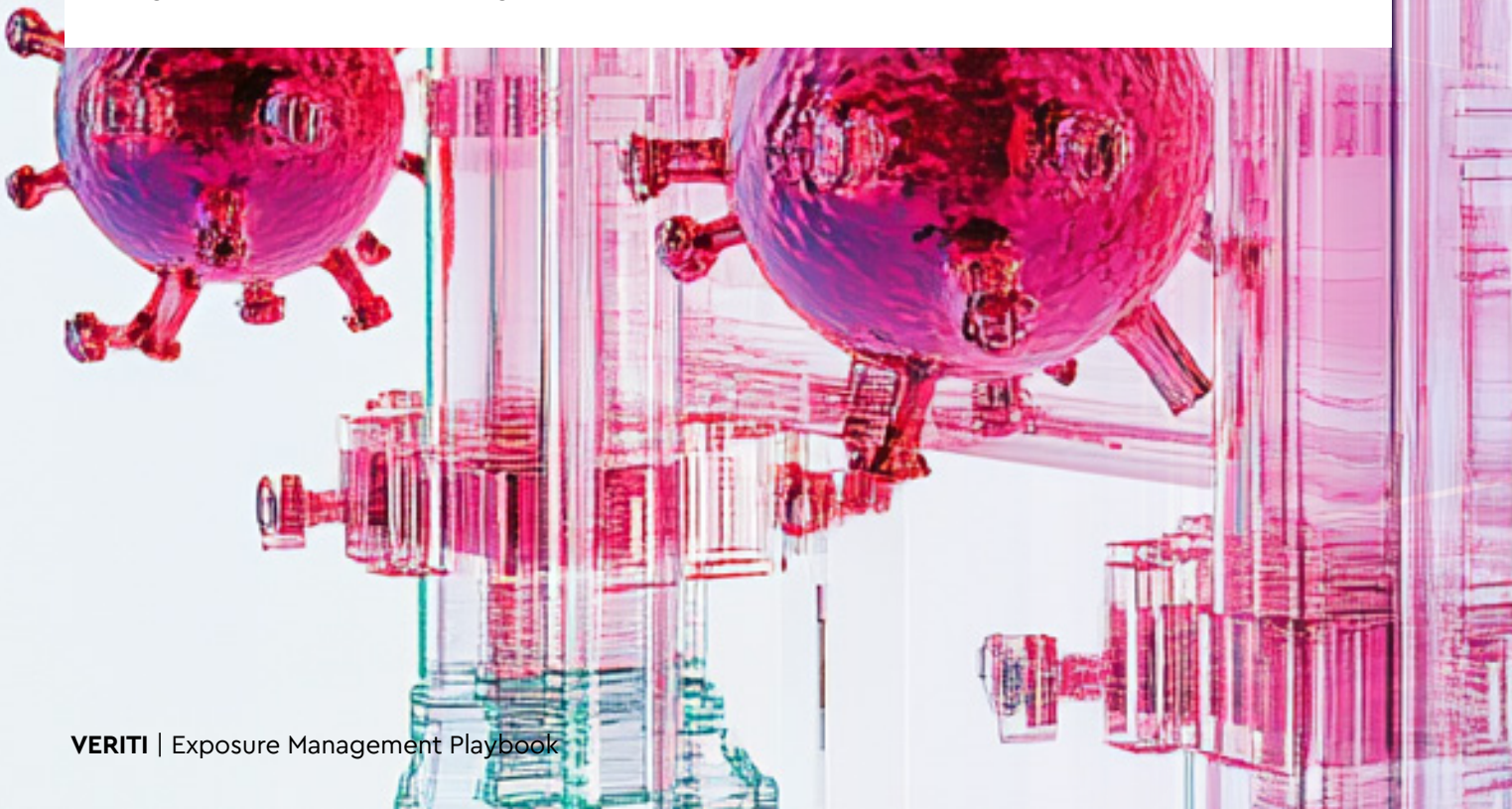
Network Security: Tools like NGFWs and intrusion prevention systems (IPS) for monitoring and securing internal and external traffic.

Endpoint Security: EDR and endpoint protection platforms (EPP) to protect user devices against malware and exploits.

Cloud Security: Solutions like Cloud-Native Application Protection Platforms (CNAPPs) and cloud security posture management (CSPM) to safeguard workloads and configurations.

Application Security: Web application firewalls (WAF) for defending against attacks at the application layer.

Threat Intelligence: Feeds and platforms that provide critical context about active threat actors and ongoing campaigns.



Part 2

Prioritization

Beyond CVSS Scores

Prioritize risk based on availability of compensating controls, business-critical assets, and real-world exploitability.

Exposure management platforms must be able to deduplicate findings across all security tools. Should be prioritized by what compensating controls are available now to reduce risk.

To make meaningful decisions, organizations need to layer in additional context, including:

Threat Intelligencey: Insights into active attack campaigns and known threat actors targeting specific vulnerabilities.

Asset Exposure Levels: Understanding which assets are vulnerable and how critical they are to operations.

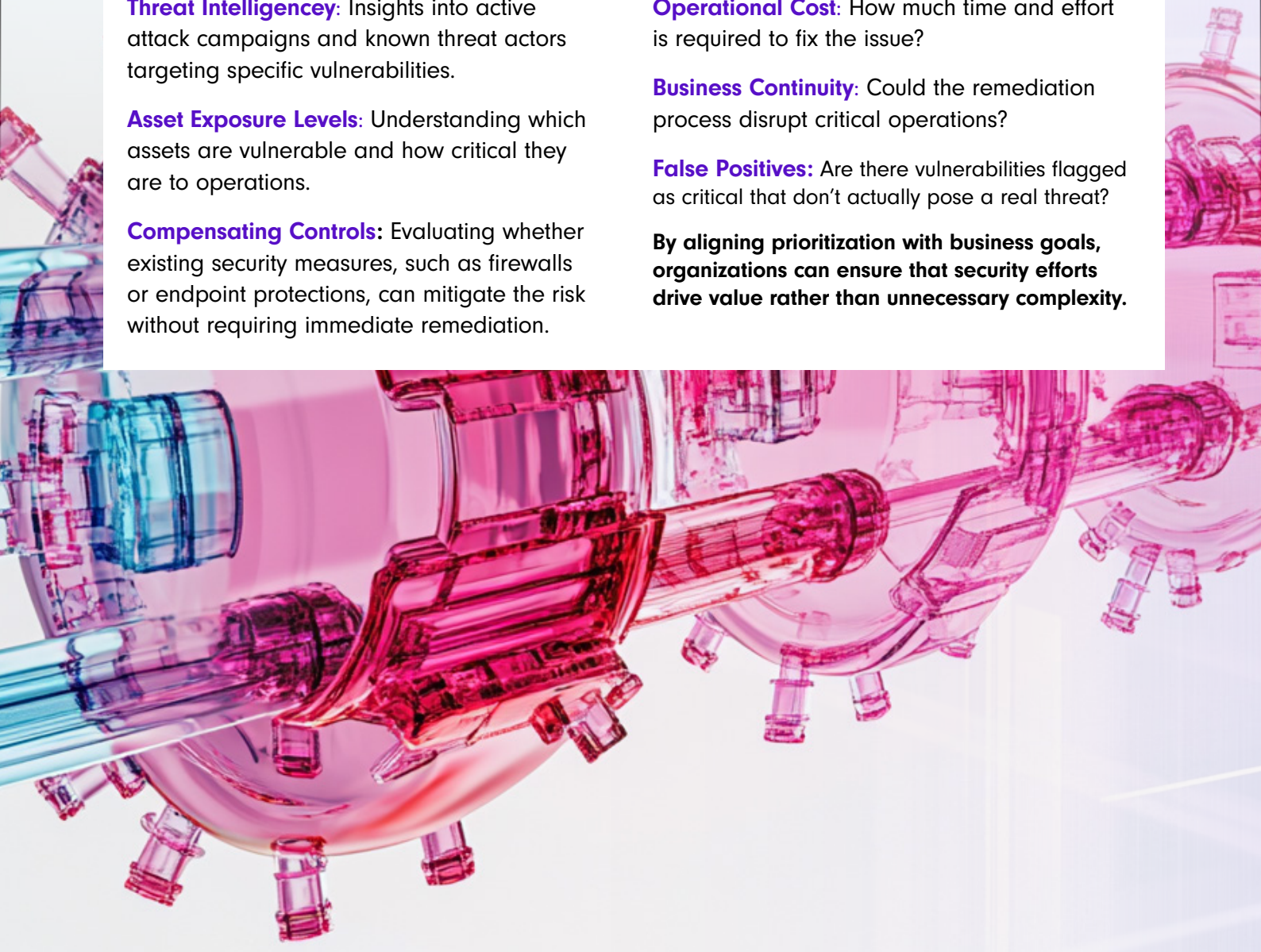
Compensating Controls: Evaluating whether existing security measures, such as firewalls or endpoint protections, can mitigate the risk without requiring immediate remediation.

Operational Cost: How much time and effort is required to fix the issue?

Business Continuity: Could the remediation process disrupt critical operations?

False Positives: Are there vulnerabilities flagged as critical that don't actually pose a real threat?

By aligning prioritization with business goals, organizations can ensure that security efforts drive value rather than unnecessary complexity.



Part 3

Remediation

Fixing Issues Without Disruptions

Mobilize remediation efforts and accelerate approval cycles by integrating automated workflows and existing controls, enabling rapid response to exposures.

Remediate via direct API changes, automated workflows, or ITSM tools for efficient risk reduction. Addresses every facet of your exposures and adjust for the ripple effects of remediation actions to ensure business continuity.

Effective mobilization begins with seamless integration across the tools and platforms organizations already rely on. This includes IT Service Management (ITSM) systems, collaboration platforms, and Security Orchestration, Automation, and Response (SOAR) tools.

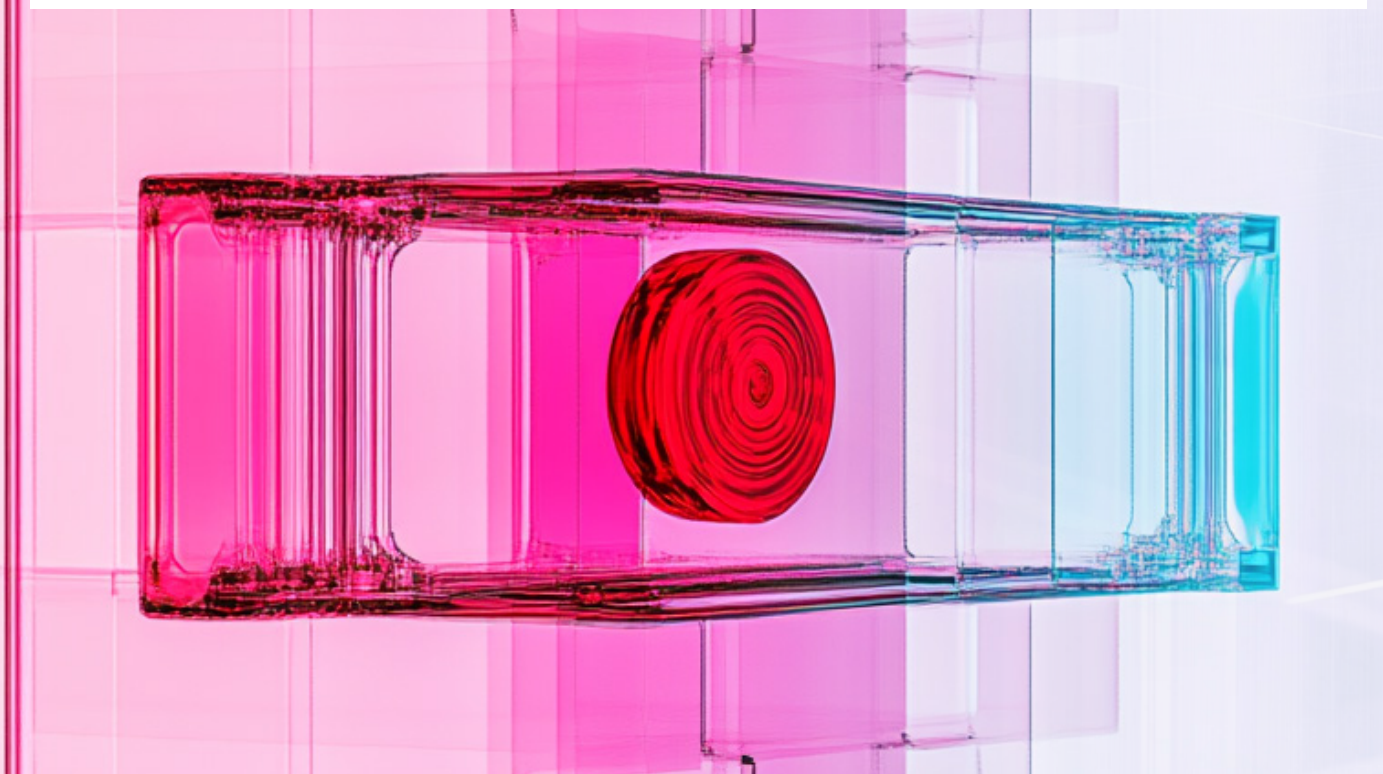
By integrating remediation workflows directly into these systems, organizations can ensure that security and operational teams are aligned. Key benefits include:

Automated Ticketing: Automatically generating tickets with detailed remediation instructions.

Real-Time Collaboration: Using tools like Slack or Microsoft Teams to keep stakeholders informed and engaged.

SOAR-Driven Playbooks: Triggering predefined playbooks to automate routine remediation tasks.

These integrations ensure that mobilization efforts are both efficient and scalable, even in complex environments.



Part 4

Validation

Ensuring Effectiveness

Manual processes can slow down remediation efforts, especially when dealing with large volumes of vulnerabilities. Automation addresses this challenge by streamlining workflows and reducing human error.

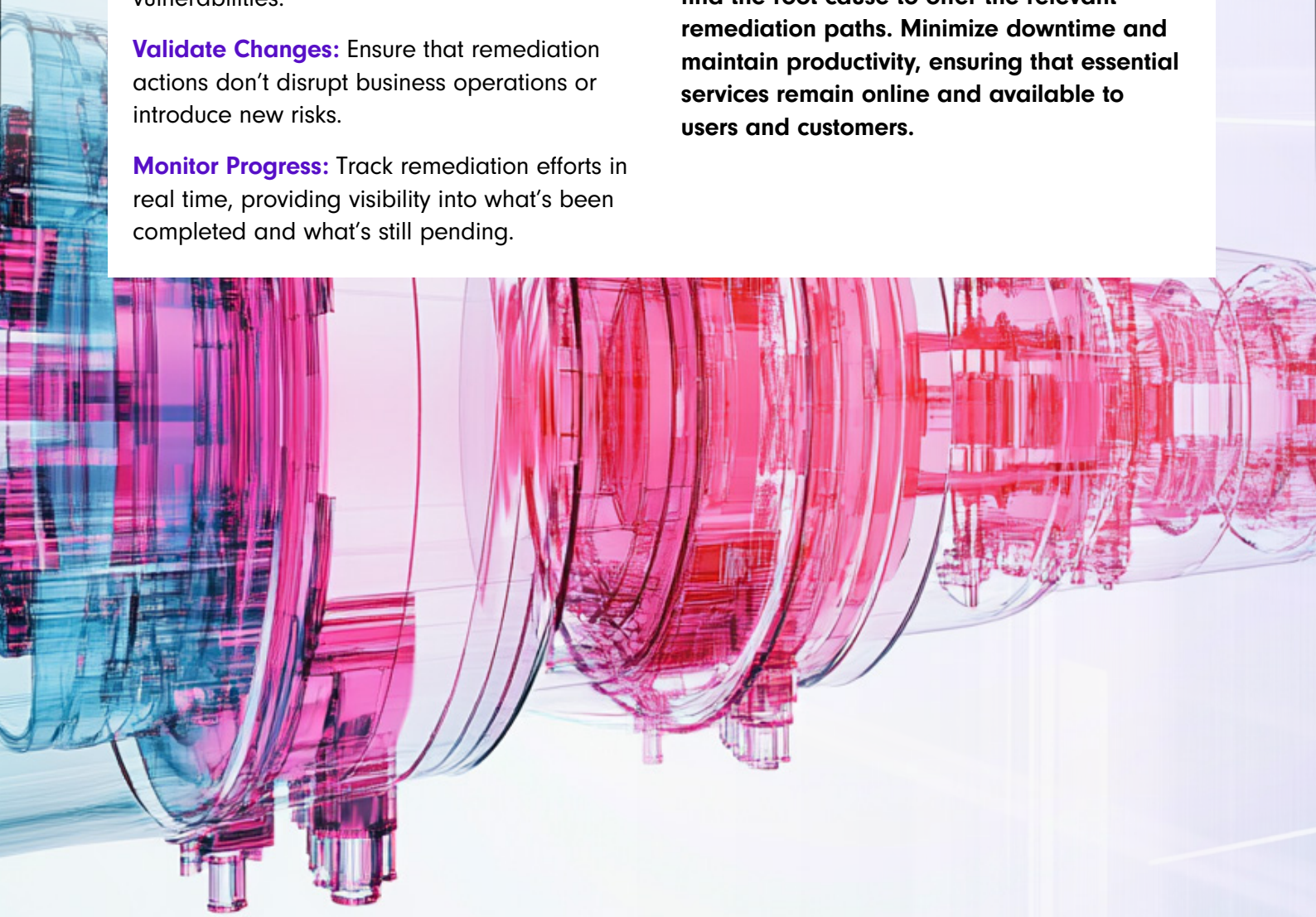
Modern mobilization approaches leverage automation to:

Initiate Remediation Actions: Automatically configure security controls to address vulnerabilities.

Validate Changes: Ensure that remediation actions don't disrupt business operations or introduce new risks.

Monitor Progress: Track remediation efforts in real time, providing visibility into what's been completed and what's still pending.

Exposure management platforms must identify false positives and automatically find the root cause to offer the relevant remediation paths. Minimize downtime and maintain productivity, ensuring that essential services remain online and available to users and customers.



Part 5

Continuous Monitoring

Making Exposure Management Sustainable

Proactively monitor for security gaps and misconfigurations both on-prem and in the cloud that can jeopardize your security posture and disrupt critical business operations.

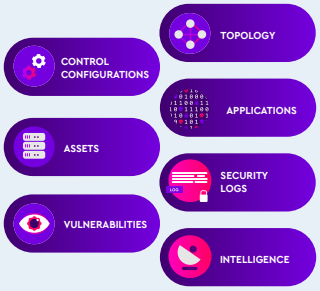
Continuous monitoring incorporates a real time intelligence layer that consolidates all security tools access logs and reported threats into a unified, high fidelity threat landscape.

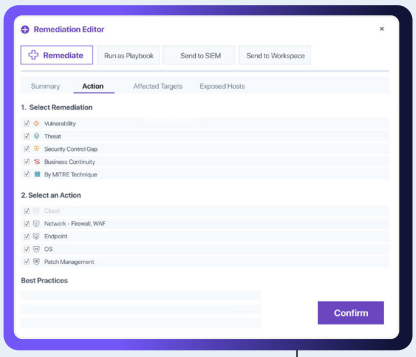
Multivendor Coverage Across All Security Logs - Aggregates and normalizes access logs and threat data from all deployed security tools, giving organizations a complete, unified exposure map view.

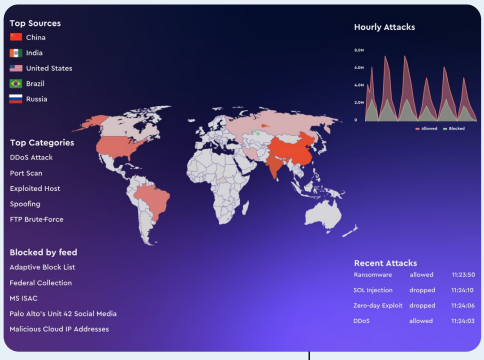
Real Time Reputation Scoring for Actionable Intelligence - Aggregates multiple reputation services to differentiate benign from malicious IPs, assigning a real time risk score that evolves dynamically based on live traffic.

Every Threat Is Malicious, But Was It Blocked? - Validates every threat shown is confirmed malicious, with a clear differentiation between attacks that were blocked versus those that got through.

Exposure Assessment Platform







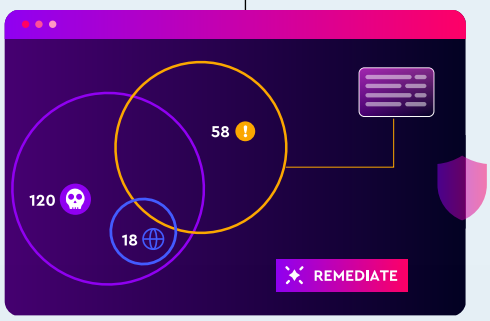
Assessment

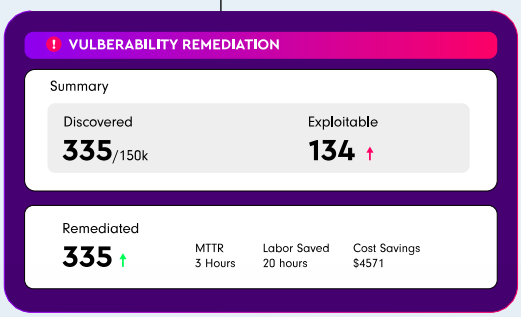
Prioritization

Remediation

Validation

Continuous Monitoring





VERITI

Veriti is an AI-driven exposure assessment and remediation platform that continuously identifies vulnerabilities, misconfigurations, and exploitability across the entire security stack on-prem and in the cloud. By leveraging compensating controls and layered defense strategies, Veriti ensures potential and active threats are proactively managed and remediated - all without disrupting business continuity.

veriti.ai