VERITI OVERVIEW

Proactively monitor and safely remediate exposures across the entire security stack, from the OS-Level and up.

EXECUTIVE SUMMARY

Veriti equips organizations with the latest AI-driven tools for real-time exposure assessment and remediation while offering a clear, comprehensive view of an enterprise's security posture. Veriti eliminates silos, and enhances the security team's ability to prioritize and proactively respond to exposures that can jeopardize your security posture without disrupting critical business operations.

ACHIEVING CYBER CERTAINTY

Enterprises today are overwhelmed by cybersecurity threats, with an unrelenting wave of security alerts that often prove to be false alarms. This constant barrage strains resources and obscures the detection of genuine threats. Compounding this challenge is the rapid evolution of cyber threats, which outstrip traditional security responses, leaving businesses exposed and reactive in their security strategies.

Adding complexity, enterprises juggle a multitude of security tools, creating a patchwork of solutions that can be challenging to manage and integrate. This disparate security environment is often compounded by a shortage of skilled cybersecurity professionals, creating gaps in expertise and leaving organizations at risk. Moreover, limited visibility into overall security posture conceals exposures and misconfigurations, while budget constraints limit the ability to implement comprehensive solutions.

Veriti emerges as the answer to these challenges by integrating disparate configurations to establish a unified security baseline. It synthesizes data from CAASM, BAS, vulnerability management tools, security logs, and intelligence feeds to identify and prioritize critical misconfigurations and gaps that are leading to exposures. This prioritization is based on factors like exploitability, severity, exposure level, and the availability of compensating controls, streamlining effective risk management and remediation strategies.

Leveraging proprietary machine learning, Veriti empowers security teams to safely remediate exposures by predicting the ripple effects of any remediation action and adjusting accordingly to ensure uninterrupted business operations.

SEAMLESS AND AGENTLESS ASSESSMENT

Effortlessly optimize your security controls with Veriti's seamless and agentless assessment. Our non-intrusive assessment process empowers you to easily identify exposures, understand their root cause, and fortify your defenses for comprehensive security enrichment. Continuously.

VERITI

SOLUTION BENEFITS

- Automated Security Controls Assessment
- Identify Exposures and Misconfigurations
- Eliminate False Positives
- Intelligent Prioritization
- Safe Remediation of Risk
- Zero Business Disruption
- Effective Reporting

27 REMEDIATIONS
per session are performed every time users access the Veriti platform

320 NON DISRUPTIVE REMEDIATIONS
handled on avg. per month

<25 SECONDS
to complete a safe remediation on average

KEY FEATURES

Comprehensive Visibility into all security gaps and exposures across the security infrastructure.

Actionable Insights within Minutes by continuously analyzing your security controls, Veriti provides data-driven insights that simplify investigations and reduces MTTR dramatically.

Eliminate False Positives Focus on actual cyber events, rather than wasting resources on false alarms.

Safe Remediation without Business Disruption Identify the root cause and automatically mitigate risk with confidence as every change is verified to not cause business disruption.

Increase Business Outcomes Maximize security efficiency with automated assessment and AI-powered security control optimization capabilities.

USE CASES

Agentless OS-level Remediation: proactively safeguard your systems directly at the os-level on the endpoint.

Vulnerability Remediation: streamline exposure management through intelligent prioritization and safe remediation of vulnerabilities.

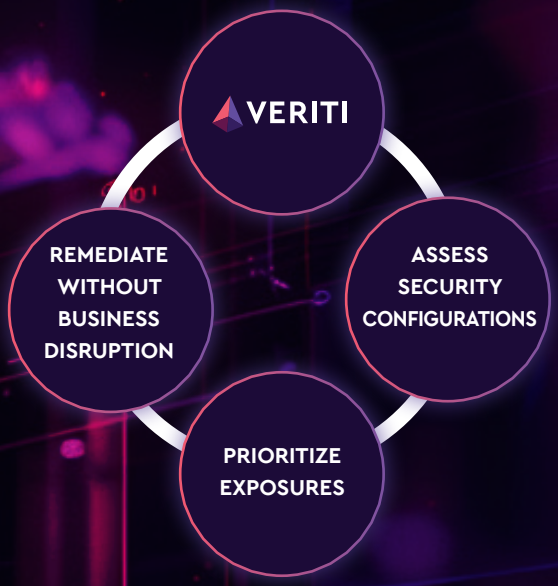
Business Continuity: proactively monitor and eliminate false positives using machine learning to achieve optimal security posture while verifying for business continuity.

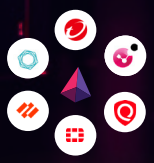
Misconfiguration Management: proactively neutralize misconfigurations to minimize exposure risks.

Mobilizing Threat Remediation: identify zero-day indicators of attack from any one vector, and then mobilize threat remediation to the rest of the security stack automatically.

INTEGRATIONS

CHECK POINT, Azure Web Aplication Firewall, cynet, paloalto NETWORKS, netskope, Carbon Black., tenable, FORTINET, Azure Firewall, Harmony Endpoint, CORTEX, zscaler, Microsoft Defender, CISCO, MEDIGATE by Claroty, Microsoft Intune, RAPID7, SentinelOne, Akamai, nessus Professional, CLOUDFLARE, TREND MICRO, CROWDSTRIKE, Azure, Microsoft Intune, Jira, servicenow, radware, Qualys., Trellix, Microsoft Sentinel, CISCO SECURE





INTEGRATE

Security controls, vulnerability assessment and BAS tools

ANALYZE & CORRELATE

Security Configurations, logs, sensor telemetries, and intelligence feeds

IDENTIFY & REMEDIATE

Threat exposure for vulnerabilities, security gaps and misconfigurations

VERITI