VERITI OVERVIEW

Proactively monitor and remediate risk, vulnerabilities, and misconfigurations from the OS-level and up without disrupting business.

EXECUTIVE SUMMARY

Veriti equips organizations with the latest AI-driven tools for real-time risk analysis and response, while offering a clear, comprehensive view of an enterprise's security posture. This AI-powered solution is tailored for proactive security, ensuring that organizations can anticipate threats and fortify their cybersecurity infrastructure efficiently, without the need for additional resources or downtime.

ACHIEVING THE CYBER CERTAINTY YOU'VE BEEN SEEKING

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. It grants you control over your remediation strategies. Seamlessly integrate the examination, evaluation, and counteraction of threats organization-wide, guaranteeing a synchronized and strategic defense against security breaches. With Veriti, security teams are equipped to automatically correct misconfigurations and fortify security voids with a mere click. Regardless of the security domain—be it email, network, EDR, or OS-level on endpoints—Veriti provides safe remediation, shielding your enterprise from looming

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 clients' defenses for comprehensive security enrichment. Continuously

VERITI

SOLUTION BENEFITS

- Automated Security Controls Assessment
- Identify Exposures and Misconfigurations
- Eliminate False Positives
- Safe Remediation of Risk in One Click
- Zero Business Disruption
- Effective Reporting
- Increase Business Outcomes

27 REMEDIATIONS
PER SESSION ARE PERFORMED EVERY TIME USERS ACCESS THE VERITI PLATFORM

320 NON DISRUPTIVE REMEDIATIONS
HANDLED IN ONE CLICK 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.

One Click 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 address vulnerabilities before they become exploitable at the OS-Level.

Eliminate false positives: Reduce alert fatigue. Increase security effectiveness.

Validate risk posture: Identify security gaps by using AI-based querying and Cybersearch.

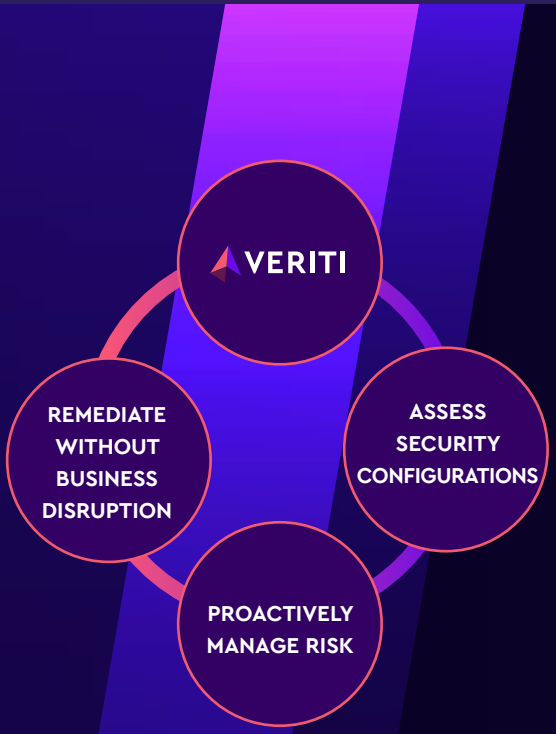
Enhance zero-day protection: Identify and stop zero-day indicators of attacks.

Vulnerability mitigation: Prioritize and remediate vulnerabilities without business impact.

Maintain cyber hygiene: Continuously monitoring the health of the security apparatus.

INTEGRATIONS

CHECK POINT · Azure Web Aplication Firewall · cynet · WIZ · orca security · netskope · Carbon Black. · tenable · paloalto NETWORKS · Azure Firewall · f5 · CORTEX · FORTINET · Microsoft Defender · Harmony Endpoint · MEDIGATE by Claroty · zscaler · RAPID7 · CISCO · SentinelOne · Microsoft Intune · nessus Professional · CLOUDFLARE · TREND MICRO · CROWDSTRIKE



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