VERITI

TECHNICAL SOLUTION BRIEF

UNIFIED SECURITY POSTURE MANAGEMENT

Proactively identify and remediate security gaps and misconfigurations throughout your security stack, without sacrificing business uptime.

The growing number and diversity of security solutions deployed in every organization adds unprecedented levels of complexity to managing the security of your entire organization. Combined with operational overhead, murky security infrastructure visibility, growing employee turnover, the severe skills shortage, and insufficient process automation, optimizing your organizational security posture is more difficult than ever before.

Veriti is a consolidated security platform that maximizes the value of your existing security stack without impacting business operations. It unifies all threat prevention configurations into a single, comprehensive language, providing complete visibility into your risk posture, current security gaps, and available countermeasures. Using machine learning, Veriti automatically analyzes all configurations and correlates them with sensor telemetries, security logs, and threat intelligence feeds to generate contextual, actionable insights for the relevant security teams.

Veriti's mission is to eliminate unnecessary complexity and operational friction and reduce the time spent in manual oversight and managing multiple cybersecurity solutions. The solution platform enables security teams to proactively improve security posture and focus on tasks that require discretion while automating repetitive, tedious tasks.

THE VALUE PROPOSITION

COMPREHENSIVE VISIBILITY

into all vulnerabilities and misconfigurations within the security infrastructure.

REDUCE RISK EXPOSURE WITHOUT SACRIFICING BUSINESS UPTIME

using machine learning and business-impact prediction models

MAXIMIZE RETURN ON INVESTMENT

by continuously analyzing and optimizing existing security controls

SHORTEN REVIEWS AND INVESTIGATION TIMES

by proactively monitoring, prioritization, and remediating postural gaps

OPTIMIZE RESOURCES

A cross-team collaboration platform that facilitates the federation of information and accountability to effectively mitigate cybersecurity threats.

SECURITY ORGANIZATIONS REQUIRE CONSOLIDATION AND AUTOMATION

Security teams spend an exorbitant amount of time on tedious tasks as there are just too many security operations and procedures to follow, dashboards to manage, alerts to handle, and new features and functions to learn. These time-consuming and repetitive actions are typically performed manually and require more time, training, and insight than available to keep up with tuning and optimization the overall security posture. In addition the overhead of managing the growing number of disparate solutions and the resources requires to maximize every solution's functionality, create a potentially inadequate security posture with security gaps. This brings up a question of cost effectiveness for every security product the organization would like to procure to strengthen its cyber-resiliency.

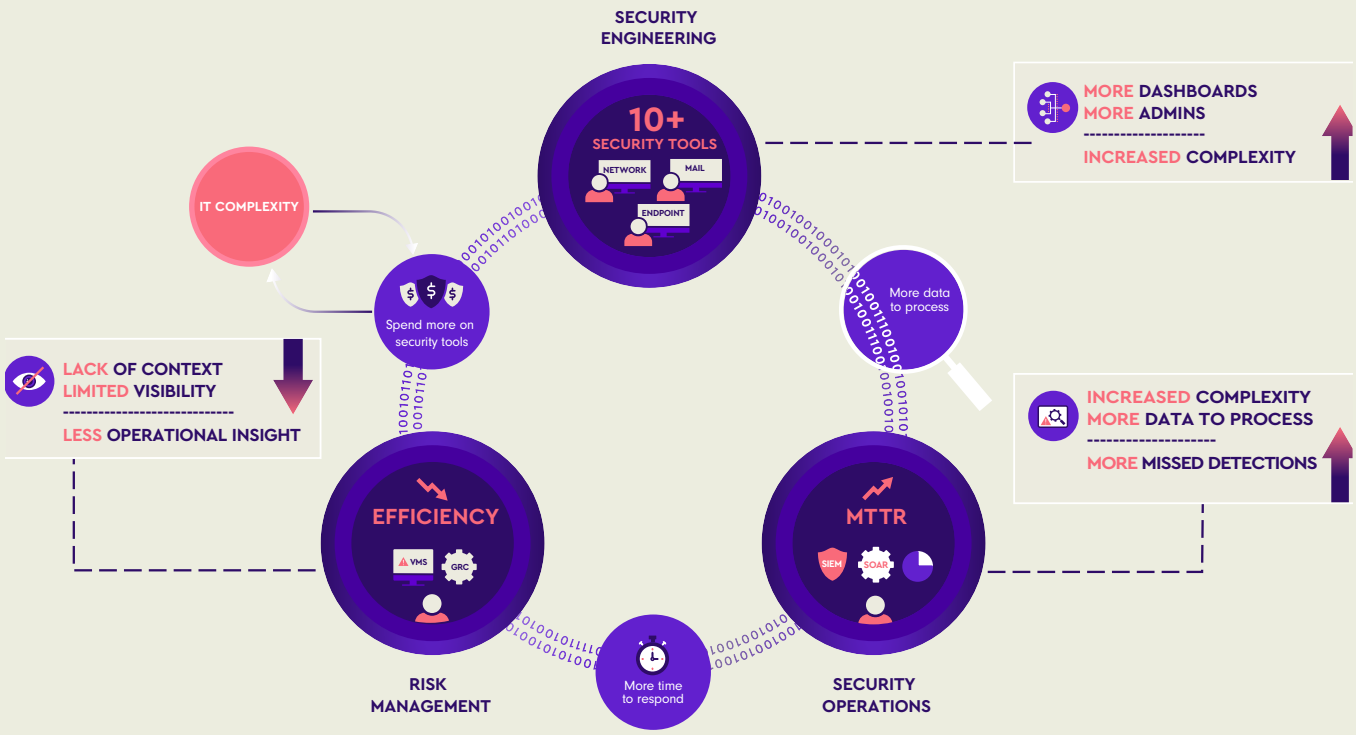
57% ARE IMPACTED BY CYBERSECURITY SKILLS GAP

62% INCREASE IN WORKLOAD DUE TO SKILLS GAP

38% INCREASE IN EMPLOYEE BURNOUT

THE CYBERSECURITY INEFFICIENCY CHALLENGE

Proving the ROI of your security products is achieved not only by the number of data breaches that have been thwarted, but also by the operational overhead each product requires. If the result is overburdened, security teams that fail to handle misconfigurations, security gaps, alerts, and complex investigations, organizations should consider a better way to optimize the potential of their security infrastructure and operations.

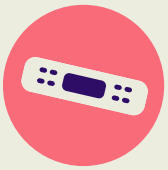


REDUCE ENGINEERING TIME; AUGMENT ENGINEERING EFFORT

EFFECTIVE VULNERABILITY MITIGATION

Vulnerability assessment tools scan network infrastructures and establish a baseline of weaknesses and vulnerability conditions for hosts, applications and databases per compliance and security frameworks. The continuous assessment of the enterprise requires IT operations group to implement remediation processes in order to keep pace with the changing IT infrastructures and growing numbers of high-risk vulnerabilities spotted in the wild.

Veriti replaces the tedious task of continuously remediating and patching all vulnerabilities with a effective mitigation and a unique virtual patching mechanism. By continaully correlating assessments reports and BAS reports with all existing security configurations, Veriti prioritizes all vulnerabilities based on threat data and business impact and pinpoints the responsible misconfiguration. It then closes the loop with full remediation by applying security updates and configuration changes at the network segment level (rather than waiting endlessly to patch the unpatchable). This method effectively reduces the time and effort needed to patch individual devices, and helps minimize business disruptions.



60%

OF BREACHES

occur because a patch was available for a known vulnerability but not applied

PROACTIVE BUSINESS-LEAD DEFENSE

With Veriti, organizations can easily take remediation actions without fearing they will disrupt business operations. Using machine learning and advanced analytics, Veriti finds the root cause behind potential and actual business disruption e.g. false positive events and closes the loop with one-click remediation actions.
Veriti prioritizes risk based on business impact prediction models, asset criticality, and available security controls. By focusing on high-risk threats and potential vulnerabilities, it helps organizations maintain the equilibrium between hardening security controls and business considerations, reducing the impact of security events on business operations.

A False positive event is defined by NIST as "an instance in which a security tool incorrectly classifies benign content as malicious" (NIST SP 800-83 Rev. 1).

46%

OF ALL APPLICATION DOWNTIME

are caused by false positives

FINDING THE SMOKING GUN

Fail-open mechanism has a fair objective, which is keeping the business operations running at all costs. But this is a two-way street that can lead to opening up your environment willingly (yet unknowingly) to threats.

Veriti's unique integration with security vendors, leverages APIs and rich telemetry to drive effective investigation with improved contextual insights regarding security incidents and cyber attacks. To avoid cases of fail-open, triggered by high CPU utilization spikes, Veriti fetches all CPU and memory feeds from every security product including connection tables and high-load applications sessions, and continuously looking for irregularities.

For every potential or actual high-CPU incident, Veriti generates an insight that provides the exact root cause, whether a triggered protection or a certain rogue connection, and the recommended remediation steps. To ensure that the business applications are prioritized without sacrificing security posture, recommended action could be dropping the connections or creating an exception for the signature that will free up the relevant resources.

For every potential or actual high-CPU incident, Veriti generates an insight that provides the exact root cause, whether a triggered protection or a certain rogue connection, and the recommended remediation steps.

SECURITY POSTURE VIGILANCE AND CYBER HYGIENE

As the cyber plot thickens, organizations find it hard to implement cyber hygiene practices due to the endless attempt to keep pace with the dynamic nature of cyber threats. What would normally require a large team of Subject Matter Experts (in-house or through a MSSP) and time, Veriti provides at a fraction of the cost, helping IT, Risk, and/or Security teams to better manage, analyze and optimize the security posture of the organization automatically.

When a new security practice is enforced (e.g. enablement of security products or update of prevention engines), the risk score of the relevant security asset and the overall security posture is changed in real-time.

What would normally require a large team of Subject Matter Experts and time, Veriti provides at a fraction of the cost, helping IT, Risk, and/or Security teams to better manage, analyze and optimize the security posture

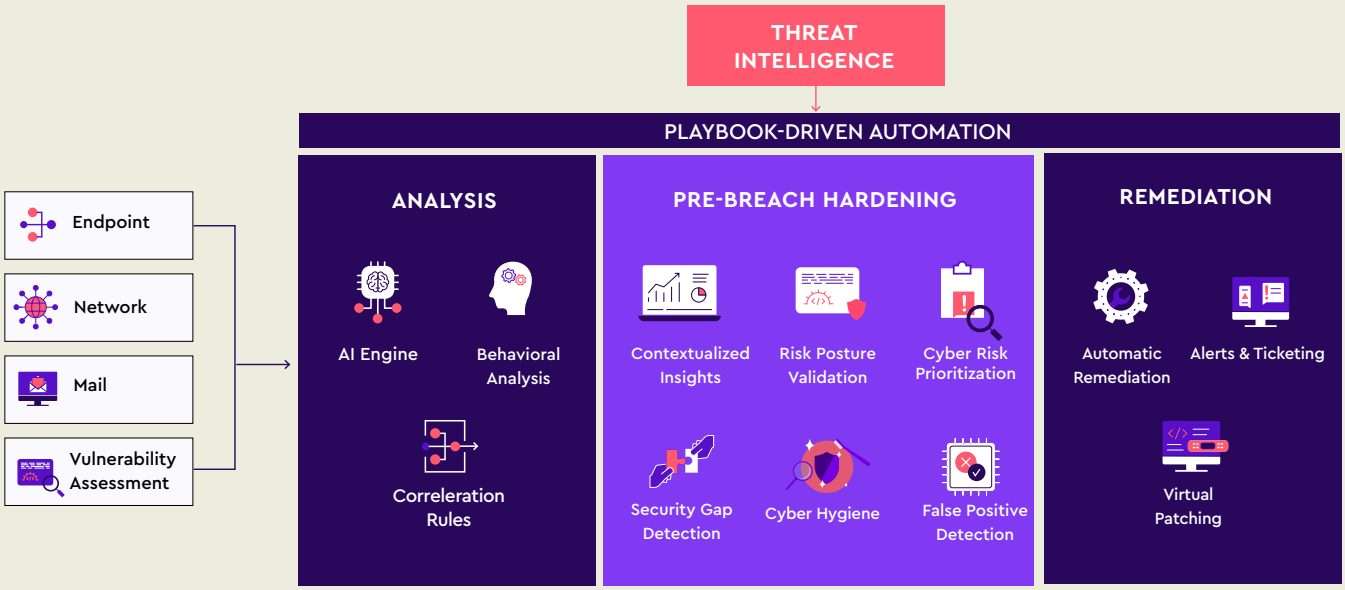
EXAMPLE

Veriti is mapping CVE signatures that are inactive on all firewall segments, signatures that are currently in allow mode can be safely converted to 'block' without impacting business operations or firewall performance.

MAXIMIZE YOUR CYBERSECURITY INVESTMENT

For every security solution, there is a significant operational friction and knowledge requirement to maximize functionality without disrupting business operations and access. This might lead to subpar security posture and potential underutilization of the tool's capabilities. Veriti consolidates different security solutions into a single, unified platform. So instead of juggling multiple security solutions with various dashboards, it brings everything together into one cohesive platform, eliminating the complexity of managing the organization's security posture from multiple dashboards.

Using advanced machine learning, it analyzes and correlates security data, including configurations, telemetries, logs, and threat intelligence, to identify potential risks or security gaps throughout the entire security stack. Consolidating security solutions into a configuration-aware security platform can help organizations maximize the value of their security investment, reduce investigation times, and improve the MTTR when responding to threats.



VERITI

Veriti's consolidated security platform helps organizations maximize the value of their existing security investment proactively without sacrificing business operations. It amplifies the efficiency of security teams by providing a single platform to automatically analyze, detect, triage, and remediate postural gaps.