

# VERITI TECHNICAL BRIEF



Proactively monitors and safely remediates risk in one-click, without disrupting the business from the OS-Level and up.

## EXECUTIVE SUMMARY

Veriti consolidates and normalizes all threat configurations to a single, unified language to proactively monitor and remediate exposures. Organizations can effectively combat security configuration drift, reduce the occurrence of false positives, and maintain consistent configurations. Rather than merely confirming the existence of security controls, you can ensure these controls are correctly and consistently configured, without disrupting the business.

## REMEDIATE RISK SAFELY ACROSS THE ENTERPRISE

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 addresses the pressing need for a system that not only consolidates alerts but intelligently distinguishes between benign and serious threats, allowing for focused and effective decisions. 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.

## TYPICAL ENTERPRISE SECURITY STACK AND COMMON EXPOSURES



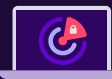
### MAIL SECURITY

- Sandbox (email) - Detection only
- CDR - turned off on XLS files (understandable why)
- Antivirus - no knowledge on the hash




### FIREWALL

- IPS - no SSL inspection (signature is turned on)
- Antivirus - no knowledge on the hash
- Sandbox (no SSL inspection)




### EDR

- Behavioral - license is not valid
- Signature based - no knowledge on the hash
- HIPS - no signature for the specific vulnerability used in the attack



### OS

- Allows CVE-2017-11882 (default) - no Detection and Prevention + no management for the OS-Level
- Allows authentication using WinRM (default) - no Detection and Prevention + no management for the OS-Level



### LATERAL

- Hosts allows SMBv1 inside the LAN & between micro-segmentation that was conducted on the network - no policy enforcement in the OS level for not allowing SMBv1

## INDUSTRY CHALLENGES

**16-46+**

avg. number of security tools in a given company - difficult to harden security defenses

**15**

Every organization faces an average of 15 high-risk vulnerabilities caused by misconfigurations

**\$4.45M**

avg. cost of data breach in 2023 \*IBM Data Breach Report

## TECHNOLOGY INTEGRATIONS

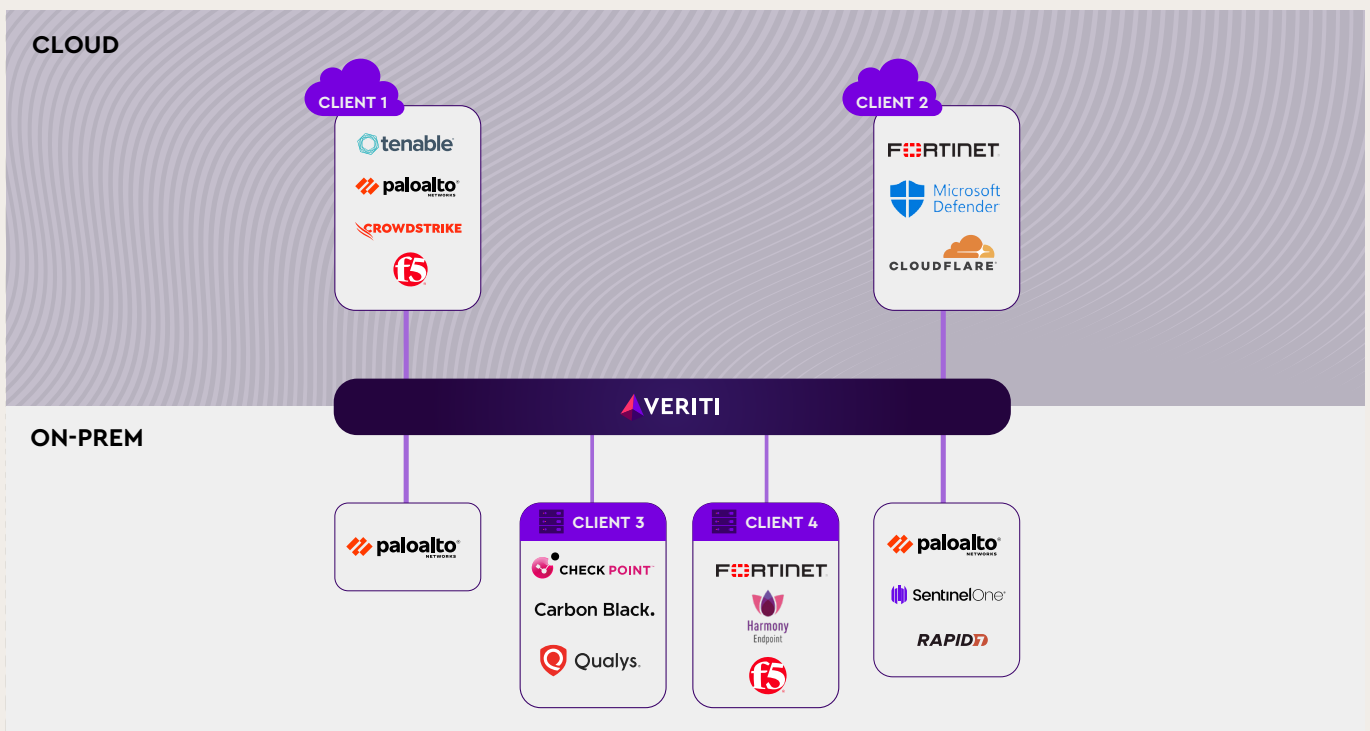


## VIRTUAL MACHINE HARDWARE SPECIFICATIONS

	CPU	Memory	Disk*
Minimum	8 Cores	16 GB	250 GB Thick-Provisioning Eager Zeroed
Recommended	16 Cores	32 GB	500 GB Thick-Provisioning Eager Zeroed

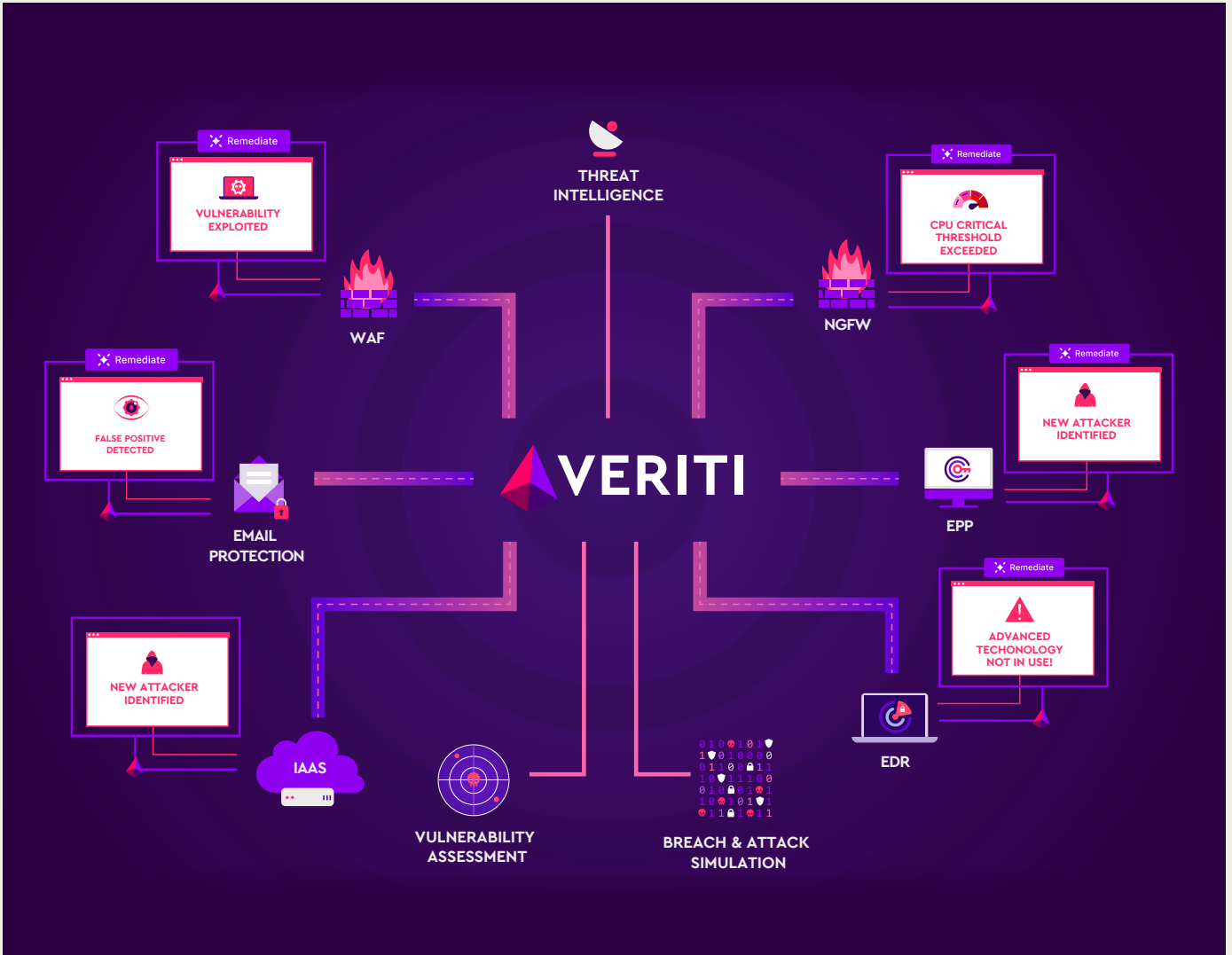
### Supported Virtual Machine Platforms

VMware ESXI - Version 6.7+  
 HyperV - Version 8.1+  
 Nuantanix AOS - Vrsion 5.18+  
 AWS EC2  
 Azure - D8s v5 or DC8as v5



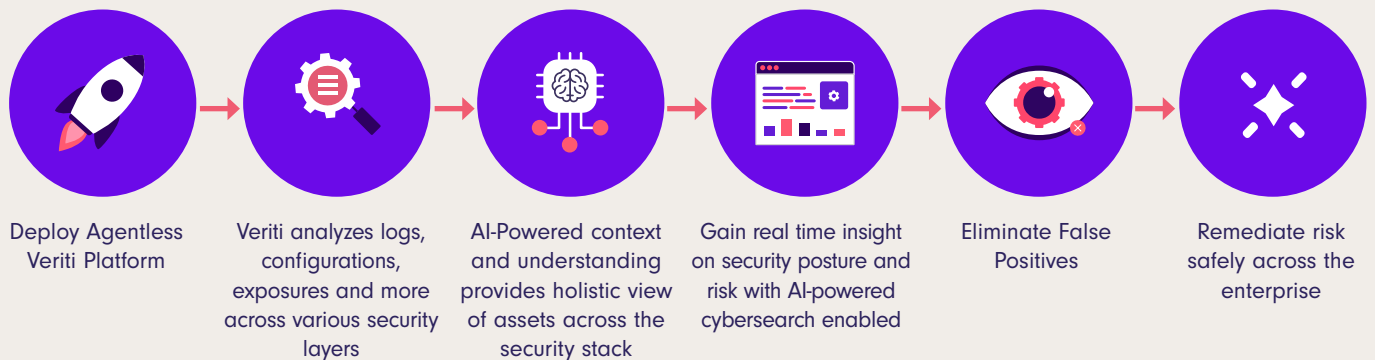
## SEAMLESS AND AGENTLESS ASSESSMENT

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.



## FROM INSTALLATION TO REMEDIATION

Continuously analyze security controls and generate data-driven insights that simplify investigations and dramatically reduce MTR enabling a unified cross-team collaboration platform that facilitates the federation of information and accountability to effectively mitigate cybersecurity threats.



# VERITI ARCHITECTURE



## 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

## 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

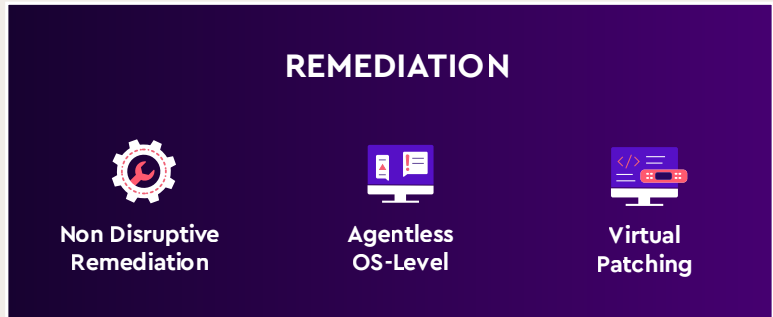
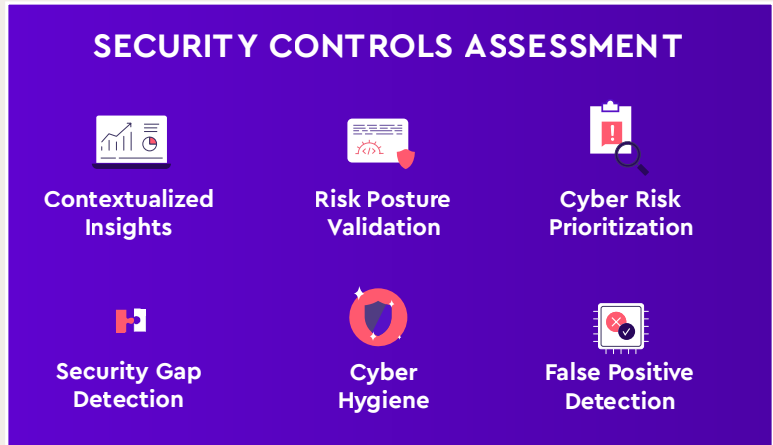
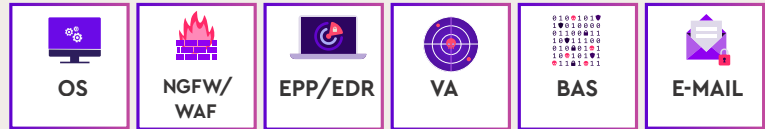
Identify and stop zero-day indicators of attacks

### Vulnerability Remediation

Prioritize and remediate vulnerabilities without business impact

### Maintain Cyber Hygiene

Continuously monitoring the health of the security apparatus



# ACTIONABLE INSIGHTS FOR DIRECT EXPOSURE REMEDIATION

By continuously analyzing and correlating all configurations with security logs, telemetries, and intelligence feeds, Veriti generates actionable insights with the admissible evidence followed by the actionable safe remediation that does not impact the business.

The screenshot displays a user interface for security remediation. At the top, it shows 'CP Firewall | Protection Hardening' and a 'Remediate' button. The main message states: 'You are not protected against multiple Remote Code Execution CVEs, including a CISA known exploited vulnerability CVE-2019-17621'. Below this, there are tags for 'High' severity and 'CISA', along with an '+ Add Tag' option.

The next section, 'Threat Intelligence', indicates that the activity is documented in the 'CISA Known Exploited Vulnerabilities Catalog', accompanied by the CISA logo.

The 'Highlights' section is divided into three columns: 'Root Cause' (2 protections are in 'Detect' mode), 'Remediation' (Change action to 'Prevent'), and 'Posture Gain' (0.26%). A note below highlights that no false positive detections were recorded for this protection in the past seven days.

The 'Protections' section features a search bar, a 'Group by Severity' dropdown, and a table of 4 items. The table lists the following protections:

SEVERITY	PROTECTION NAME	CVES	CVE YEAR	CREATED BY
Critical	Oracle Weblogic Insecure Deseriali...	CVE-2020-2551	2020	Check Point
High	D-Link DIR-859 Remote Code Exec...	CVE-2019-17621	2019	Check Point

Identified Risk Details

Threat Intelligence

Actual mitigation that will be done in one click

Protections that are affected

## KEY FEATURES

### Eliminate False Positives

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

### Safe Remediation in One Click

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.