VERITI

10 Questions to Ask Before Investing in an Exposure Management Platform

A Strategic Guide to Help You Evaluate Solutions That Actually Reduce Risk

Introduction

Security tools have mastered detection - but visibility without action still leaves you exposed.

Exposure management platforms promise to bridge the gap between alerts and real risk reduction. But not all platforms deliver. Use this guide to ask the 10 questions that separate real exposure remediation from just another dashboard.

CTEM Stage 1

Visibility

Question 1

Can the platform integrate across all security controls – on-prem and cloud – without deploying agents?

Modern infrastructures are hybrid. Agentless integration ensures low-friction, high-coverage visibility into misconfigurations, vulnerabilities, and control gaps across firewalls, endpoints, cloud services, and more.

Question 2

Does it unify all exposures and security telemetry into a single source of truth?

Fragmented visibility leads to missed risk. A true platform should aggregate, normalize, and deduplicate data from your existing security stack to create one comprehensive view of your attack surface.

VA CNAPP EDR NGFW SIEM

CTEM Stage 2

Assessment

Question 3

Does it continuously validate the effectiveness of your security controls?

Misconfigured or ineffective controls can leave critical gaps. Choose a platform that assesses real-world protections and maps security configurations to actual exposures—not just vulnerabilities.

Question 4

Can the platform identify the root cause of each exposure and correlate with active threat activity?

Assessment must go beyond point-in-time findings. Look for solutions that tie exposures to MITRE ATT&CK tactics, identify which tools failed to prevent them, and highlight whether threats are actively targeting the gap.

CTEM Stage 3

Prioritization

Question 5

Does it incorporate threat intelligence and exploitability into risk scoring?

Not all vulnerabilities matter equally. Ensure the platform prioritizes based on threat actor activity, EPSS scores, number of affected assets, and existing compensating controls.

Question 6

Can it deduplicate and normalize vulnerabilities across tools?

If your vulnerability scanner and CNAPP report the same issue differently, can the platform consolidate it into one actionable exposure?

Question 7

Does it factor in business context to avoid false positives and operational disruption?

Security doesn’t exist in a vacuum. Prioritization should reflect business-critical assets, compliance requirements, and operational impact to avoid unnecessary escalations.

CTEM Stage 4

Remediation (Mobilization)

Question 8

Can it remediate directly—or just recommend?

Detection without action is just documentation. The platform should let you remediate via APIs, ITSM workflows, or playbooks—without disruption.

Question 9

Does it validate remediation actions before deploying?

To protect business continuity, remediation must be safe. That means predicting operational impact and confirming nothing breaks.

Question 10

Can it apply compensating controls when patching isn't possible?

When a patch isn't available, you're not helpless. Your platform should enforce IoCs, adjust control configurations, and harden security posture instantly.

Real-world results

Veriti Customer Case Studies

Exposure assessment platforms are essential for organizations looking to stay ahead of cyber threats. By offering visibility, prioritization, and active remediation, these platforms empower businesses to reduce risk and maintain resilience.

1

Vulnerability Remediation

Industry: Financial Services

Challenge

A critical vulnerability exposed to the internet was detected by Tenable, but the Check Point IPS protection was disabled.

Solution

Veriti identified the issue and remediated over 440 vulnerabilities using the organization's existing security tools while maintaining business continuity.

2

OS-Level Remediation

Industry: Healthcare

Challenge

Patch management tools failed to detect OS-level misconfigurations, leaving 25 hosts vulnerable to credential harvesting attacks.

Solution

Veriti agentlessly identified and fixed registry and OS issues, ensuring the vulnerabilities were remediated. This led to a Pen Tester failing their follow-up attempts.

3

Cross-Platform Threat Enforcement

Industry: Manufacturing

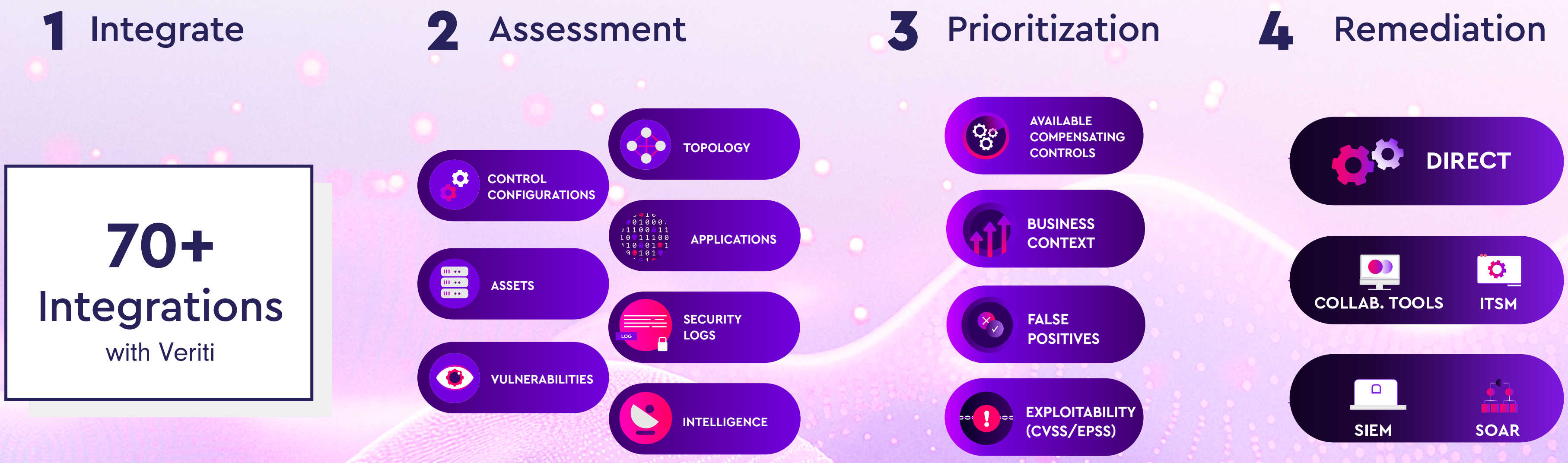
Challenge

F5 prevented an attack, but the incident wasn't shared across other security products, creating a gap in protections.

Solution:

Veriti enriched attack data and enforced protections across all security controls, establishing a cohesive and effective threat prevention system.

Exposure Assessment Platform



1 Integrate

70+ Integrations

with Veriti

2 Assessment

- CONTROL CONFIGURATIONS
- ASSETS
- VULNERABILITIES
- TOPOLOGY
- APPLICATIONS
- SECURITY LOGS
- INTELLIGENCE

3 Prioritization

- AVAILABLE COMPENSATING CONTROLS
- BUSINESS CONTEXT
- FALSE POSITIVES
- EXPLOITABILITY (CVSS/EPSS)

4 Remediation

- DIRECT
- COLLAB. TOOLS
- ITSM
- SIEM
- SOAR

Your Final Checklist

Agentless integration across hybrid environments

Unified view of exposures from all security tools

Continuous validation of security control effectiveness

Exposure-to-threat correlation

Threat and exploitability informed prioritization

Business aware risk modeling

Real-time dynamic risk scoring

Apply compensating controls when patching isn't possible

One-click safe remediation across tools

Business impact analysis before change

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