



ULTIMATE GUIDE TO SECURITY CONTROLS OPTIMIZATION

How to reduce risk exposure and get away with it

TABLE OF CONTENTS

Introduction: Some Things Never Change.....	3
The Typical Security Stack.....	5
Building Automated Security Controls Assessments into Your Cybersecurity Strategy	6
The Key is Automating Exposure Identification and Response	7
The Difference with Security Controls Optimization (or The Veriti Difference)	7
How To Reduce Risk and Get Away with It	9

INTRODUCTION

SOME THINGS NEVER CHANGE

Companies continue to face security breaches, and while some security vendors tout 100% protection and detection rates, the reality is more complex. The devil lies in the details. What many vendors fail to disclose, but organizations like MITRE reveal, is that achieving such results often hinges on configuration changes or delayed detections. The ideal scenario would involve everything functioning exactly as intended, seamlessly integrated with the infrastructure to ensure comprehensive protection. However, experience has shown that this is not the case.

In today's landscape of widespread remote work, expanding attack surfaces, and the AI-powered realm of cyber threats, where some malicious actors only need a few seconds to make you the next headline in a cyber breach story, the luxury of making additional configuration changes or waiting for delayed detections is a risky proposition. When the complexity and exceptions within security solutions become too costly to navigate, the solution becomes apparent.

To adapt to this ever-evolving landscape, leaders in security and risk management must develop strategies that prioritize business risk over the mere refinement of existing methods.

LET'S EXPLORE THE CURRENT REALITY

The average organization, spanning from SMBs to large enterprises, is laden with over 70 security tools.

Vendors may claim their security tools "pass" evaluations.

Various security controls are in place but often misconfigured.

NOW, THE TRUTH:

It's challenging to fortify security defenses without jeopardizing business operations.

Achieving better results often requires configuration changes or delayed detections.

Companies are still susceptible to breaches.

Dealing with intricate configuration demands remains a significant challenge in both cloud and on-premises environments, and the most effective approach lies in automation. As a result, Automated Security Control Assessment (ASCA) tools are emerging to validate product configurations in hybrid environments. Facts emphasize the need for change.

60%

OF ORGANIZATIONS ANALYZE AND TRIAGE LESS THAN 40% OF THEIR LOG DATA

(McKinsey).

10%

OF KNOWN VULNERABILITIES ARE REMEDIATED ON A MONTHLY BASIS

(The Cyentia Institute).

60%

OF FUTURE SECURITY BREACHES ARE EXPECTED TO RESULT FROM MISCONFIGURATIONS

(Gartner)

ASCA processes and technologies play a pivotal role in addressing these pressing challenges. They zero in on the analysis and rectification of misconfigurations within a spectrum of security controls, spanning endpoint protection, network firewall, identity management, email security, and security information and event management. This dedicated focus on misconfigurations serves as a linchpin in fortifying an enterprise's overall security posture.

Furthermore, these cutting-edge technologies take on a crucial role in optimizing security controls by identifying vulnerabilities, threats, and risks that have the potential to lead to system, application, or data breaches. They also automate responses, encompassing tasks like software patching and orchestrating dynamic configuration changes whenever outdated, insecure, or exploitable systems are detected. This proactive approach not only counters both known and unknown cyber threats but also minimizes the organization's exposed attack surface.

Automated security control assessment technologies are instrumental in cultivating a more secure environment. They effectively combat security configuration drift, reduce the occurrence of false positives, and maintain consistent configurations. Rather than merely confirming the existence of security controls, they ensure these controls are correctly and consistently configured.

In addition to enhancing security, ASCA processes and technologies also bring numerous benefits to the organization. They enhance staff efficiency, minimize the impact of human errors, and increase resilience in the face of organizational churn. By closing security control configuration gaps, they help prevent preventable attacks.

KEY BUSINESS DRIVERS FOR IMPLEMENTING AUTOMATED SECURITY CONTROLS ASSESSMENTS



The growing complexity of environments, the emergence of new threat vectors, the proliferation of innovative security tools, and the frequent turnover of staff have resulted in an escalating number of misconfigurations within security controls, rendering the attack surface more vulnerable.




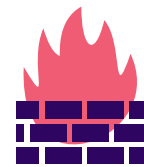



Some organizations prioritize the preservation of intricate, heterogeneous infrastructure and security architectures to meet specific use cases and objectives, instead of simplifying through vendor consolidation.



Relying exclusively on manual periodic configuration reviews, tool-centric approaches, or occasional penetration tests for optimizing enterprise security control configurations falls short of the mark.

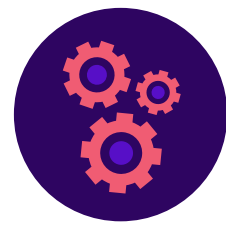
THE TYPICAL SECURITY STACK

Let's briefly delve beneath the surface and uncover the tools and protection measures an organization typically employs to ensure security. In addition, we will examine the key factors contributing to a successful attack and what ultimately leads to these breaches within organizations.

SECURITY LAYER	PROTECTION/ CAPABILITY	RISK
 MAIL SECURITY	Sandbox (email) CDR Antivirus	Sandbox (email) - Detection only CDR - turned off on XLS files (understandable why) Antivirus - no knowledge on the hash
 FIREWALL	IPS Antivirus Sandbox (SSL)	IPS - no SSL inspection (signature is turned on) Antivirus - no knowledge on the hash Sandbox (no SSL inspection)
 EDR	Behavioral Signature-based HIPS Sandbox	Behavioral - license is not valid Signature based - no knowledge on the hash HIPS - no signature for the specific vulnerability used in the attack Sandbox - license is not valid
 OPERATING SYSTEM (OS)	Prompt for unauthorized apps and process User Role access	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 MOVEMENT	Micro segmentation East-West network detection	No policy enforcement in the OS-Level for not allowing SMBv1 Hosts allows SMBv1 inside the LAN and between micro-segmentation that was conducted on the network

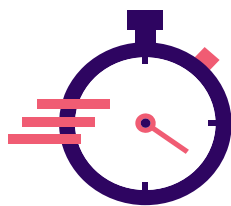
BUILDING AUTOMATED SECURITY CONTROLS ASSESSMENTS INTO YOUR CYBERSECURITY STRATEGY

To effectively integrate ASCA into your defense strategy, consider the following factors:



VENDOR CONSOLIDATION

Begin by evaluating the potential for vendor consolidation. The presence of numerous security tools can lead to increased data management, individual maintenance responsibilities, and a higher likelihood of misconfigurations. To address this, it's crucial to assess the array of tools deployed across your organization. Conduct ongoing scans to identify opportunities for tool consolidation, and, more importantly, approach security solutions with a unified perspective. Even minor misconfigurations can trigger a cascade of issues.



OPTIMIZATION CAPABILITIES

When evaluating vendors, inquire about their optimization capabilities. Seek answers to questions regarding monitoring and alerting speed, the potential impact on your business operations, and the extent and nature of support for your organization's security controls.



IMMEDIATE REMEDIATION

Ensure that the tools you select can deliver immediate remediation. Solutions leveraging machine learning and predictive models have the capacity to close security gaps exponentially faster. They achieve this by swiftly implementing remediation actions, which are designed to avoid any disruption to critical business functions.

Adhering to these considerations will enhance your ability to seamlessly incorporate ASCA into your overall security infrastructure.

"ASCA processes and technologies focus on the analysis and remediation of misconfigurations in security controls (e.g., endpoint protection, network firewall, identity, email security, and security information and event management), which improves enterprise security posture. ASCA can be a stand-alone tool or a capability of other security products, such as firewalls, identity threat detection and response, network security policy management, and cloud infrastructure entitlement management."

Gartner, Analysis By: Evgeny Mirolyubov, Jeremy D'Hoinne

THE KEY IS AUTOMATING EXPOSURE IDENTIFICATION AND RESPONSE

The cornerstone of automating exposure identification and response hinges on an integrated platform characterized by the following attributes:

Utilizes Existing Security Stack

It optimally integrates with your existing security infrastructure.

Continually Monitoring for potential risk

Proactively identify all security gaps, vulnerabilities, and misconfigurations across the hybrid environment.

Automatic Remediation and Mitigation

It enables automated remediation and mitigation of vulnerabilities.

Without Business Disruption

It accomplishes these tasks without causing disruptions to business operations.

The introduction of ASCA technology stands as a game-changer in security operations. It orchestrates continuous monitoring and alerts, enabling organizations to proactively identify and address potential risks. By taking proactive, AI-driven measures, threats can be mitigated swiftly, well before they inflict harm. As cyber attackers grow increasingly sophisticated and aggressive in their tactics, the capability to promptly detect and respond to exposures becomes ever more critical.

THE DIFFERENCE WITH SECURITY CONTROLS OPTIMIZATION (OR THE VERITI DIFFERENCE)

In the realm of security controls optimization, Veriti introduces a transformative approach characterized by comprehensive insight. This approach encompasses gaining a holistic understanding of an enterprise's traditional configurations and the critical ability to pinpoint misconfigurations or gaps in protection that could expose vulnerabilities.

Veriti also provides real-time threat visibility across a complex, dispersed network while capitalizing on existing security assets. This approach enables organizations to make informed, threat intelligence-based decisions and orchestrates automated responses through machine learning (ML)-generated playbooks, facilitating rapid reactions to cyber threats.

THE VERITI DIFFERENCE IS QUANTIFIABLE

3

Delivering an average of 3 impactful insights to business operations every week

12 sec

To proactively remediate Veriti Insights (MTR)

164

Non-disruptive remediations handled per session on avg. every month to ensure operational continuity.

DEFRAGMENTING SECURITY

Veriti consolidates security configurations – NGFWs, WAFs, Intrusion Prevention Systems, endpoint protection, EDRs, vulnerability scanners, BAS tools and much more. We defragment the security tools to eliminate silos and providing crystal clear view of both security and risk posture.

ONE-CLICK REMEDIATION. ZERO BUSINESS IMPACT

Leveraging machine learning and business-impact prediction models to close security gaps with zero business downtime.

ACTIONABLE INSIGHTS WITHIN MINUTES

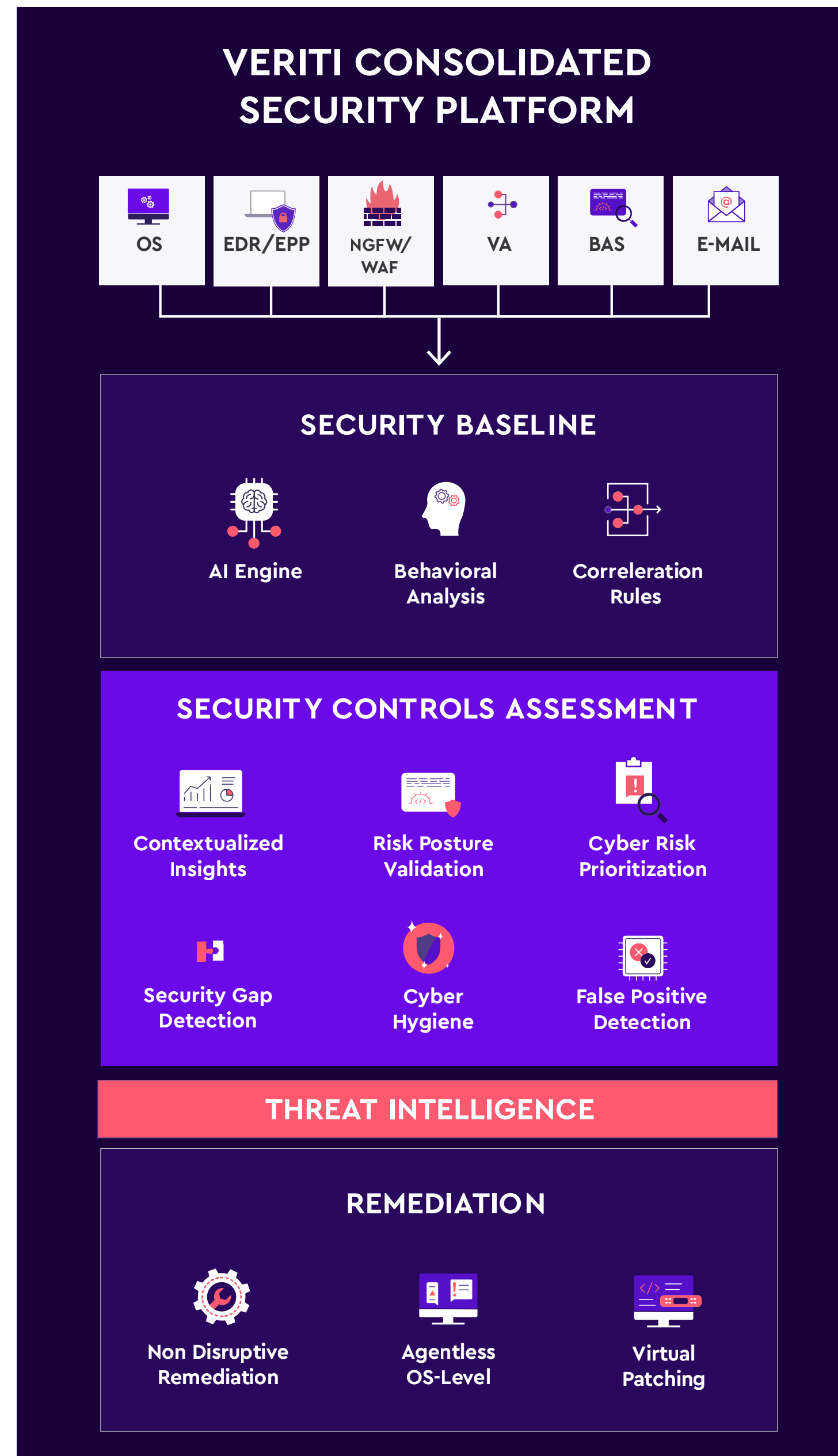
Continuously analyzing security controls and generate data-driven insights that simplify investigations and dramatically reduce MTTR.

OPTIMIZE RESOURCES

Maximize security efficiency with automated assessment and root cause analysis of security alerts and business downtime incidents.

CROSS-TEAM COLLABORATION

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



HOW TO REDUCE RISK AND GET AWAY WITH IT

The key to risk reduction lies in the proactive implementation of Automated Security Control Assessments (ASCA) and the diligent execution of remediation efforts. Effective leaders should embrace an exposure-driven approach to operations, placing a premium on business relevance. This entails maintaining comprehensive visibility across technology estates to monitor and swiftly respond to potential threat activity, with a focus on proactive risk reduction through the careful orchestration of security controls.

KEY FRAMEWORKS TO ACHIEVE THIS VISION:

- 1. Continuous Threat Exposure Management (CTEM) and Automated Exposure Identification and Response (AEIR):** These concepts serve as foundational pillars, facilitating ongoing assessment and automated response to exposures.
- 2. Business-Relevant Approach:** By adopting a business-centric perspective, organizations can significantly enhance the breadth and relevance of their detection and response capabilities.
- 3. Maximized Automation:** The incorporation of automation leads to a reduction in response times, enhancing the organization's overall agility and responsiveness.
- 4. Leveraging Generative Cybersecurity AI:** The utilization of AI-driven solutions not only boosts operational efficiency but also augments the skills of security teams.

These strategic objectives can be effectively realized through a series of concrete steps:

- 1. Simplify Operations:** One key step is streamlining operations through security vendor consolidation, reducing complexity, and enhancing efficiency.
- 2. Institute Comprehensive Security Control Evaluation Processes:** Develop a robust framework for evaluating enterprise security controls. This should cover the planning, assessment, remediation, and validation of intended configurations to ensure comprehensive coverage.
- 3. Continuous Configuration Monitoring:** Maintain unwavering vigilance through continuous configuration monitoring, which offers immediate insights into the impact of configuration changes on security, operational integrity, and productivity.

To get you started, at Veriti, we provide a no-cost Security Controls Assessment that facilitates a seamless and agentless evaluation of your security posture. Our non-intrusive assessment process empowers you to easily identify misconfigurations, understand their root causes, and fortify your defenses in a continuous and proactive manner.

EASY AND SHORT PROCESS



CYBERSECURITY EFFICIENCY WITH VERITI

30%

reduction in false positives resulting in improved time to respond and operationalization of the security posture

66%

improvement in enterprise security posture using the security solutions already in place

42%

increase in active vulnerability protections implemented without disrupting business operations

11%

fewer logs sent to SIEM due to Veriti's exclusion creation, reducing operational friction posture

50%

improvement in penetration testing achieved by Veriti's continuous security controls optimization



Veriti's mission is to eliminate complexity and operational friction in managing multiple cybersecurity solutions by providing a consolidated, governing platform that proactively monitors and in a single click, remediates security gaps and misconfigurations across the entire security infrastructure.

VERITI.AI