SOLUTION BRIEF

Fortinet and Veriti Automated Security Controls Optimization

Proactively monitor and remediate security gaps and misconfigurations across your entire security infrastructure without impacting business

Executive Summary

Maximize your security posture with Fortinet and Veriti integrated solutions. This partnership combines Veriti Security Controls Optimization with the Fortinet Security Fabric, including FortiGate, FortiManager, and FortiAnalyzer. Experience the power of AI-driven solutions to proactively detect and remediate security gaps and misconfigurations while safeguarding your business operations from disruption.

The Challenge

Organizations today face the dual challenge of upholding robust cybersecurity while ensuring uninterrupted business operations. Central to this challenge are the tasks of managing overwhelming data volumes from different sources, including inundation of security alerts. This situation strains resources and complicates the decision-making process, making distinguishing real threats from benign events difficult. Maintaining security defenses amid this overload requires precision and efficiency. Moreover, this overwhelming scenario often hampers the ability to adapt controls to the constantly evolving threat landscape, leading to inadvertent misconfigurations and security gaps. Such gaps can unintentionally obstruct legitimate applications and users, further complicating the security landscape for businesses.

Fortinet and Veriti have established a technology partnership to address these challenges, offering a joint solution that seamlessly integrates into existing organizational frameworks. This collaboration focuses on enhancing cybersecurity measures while minimizing the risk of network downtime and application outages, which are critical for uninterrupted business operations. By leveraging advanced AI-driven technologies, the Veriti Automated Security Controls Optimization solution empowers organizations to swiftly identify and respond to potential and real threats. This approach ensures a resilient and efficient security posture that protects infrastructure and maintains business continuity, bridging the gap between strong cybersecurity and operational agility.

Joint Solution

The innovative integration between Veriti's automated security controls optimization platform and the Fortinet Security Fabric represents a breakthrough in cybersecurity management. This partnership combines the comprehensive network defense capabilities of Fortinet solutions with Veriti's expertise in optimizing security postures, offering organizations a highly efficient and powerful layer of protection.

Solution Components

- Fortinet FortiGate Next-Generation Firewall (NGFW), FortiManager, and FortiAnalyzer
- Veriti Automated Security Controls Optimization

Solution Benefits

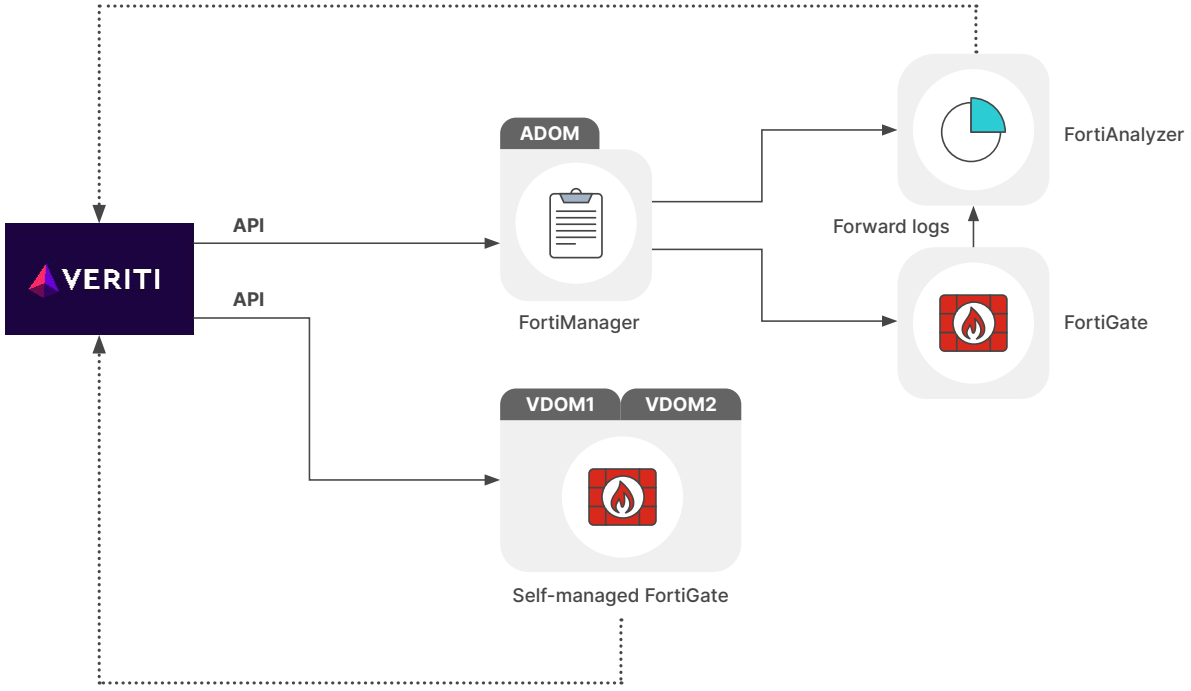
- Close security gaps by leveraging machine learning (ML) and business-impact prediction models
- Maximize security efficiency with automated assessment and root-cause analysis of security alerts and business downtime incidents
- Effectively mitigate threats by facilitating federation of information and accountability
- Simplify investigations and dramatically reduce Mean Time to Respond (MTTR) by continuously analyzing security controls and generating data-driven insights

FORTINET FABRIC-READY

Key Features of Integration

This integrated solution is a comprehensive approach to cybersecurity. It ensures that organizations are equipped with robust defenses and can optimize their security operations for high efficiency and minimal business interruption.

- **One-Click Remediation with Zero Business Impact:** Utilizing advanced ML and predictive models, the solution efficiently addresses security gaps while ensuring zero impact on business operations.
- **Optimize Resources:** The integration automates the assessment and root-cause analysis of security alerts and incidents affecting business continuity. This leads to maximized efficiency in security resource management.
- **Cross-Team Collaboration:** Security teams confidently make informed, threat intelligence–based decisions and orchestrate responses with zero business impact validation through proprietary ML, facilitating rapid reactions to cyberthreats.
- **Save Time:** By continuously analyzing security controls and generating data-driven insights, the solution significantly streamlines investigations and reduces MTTR, saving business time and resources.



Fortinet and Veriti solution integration

Solution Components

- **Fortinet FortiGate:** FortiGate NGFW is the world's most deployed network firewall, delivering unparalleled AI-powered security performance and threat intelligence, complete visibility, and security and networking convergence.
- **Fortinet FortiManager:** FortiManager provides automation-driven centralized management of Fortinet devices from a single console and enables complete administration and visibility of network devices through streamlined provisioning and innovative automation tools.
- **Fortinet FortiAnalyzer:** FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

- **Veriti Automated Security Controls Optimization:** Veriti is a consolidated security platform that proactively monitors and remediates security gaps and misconfigurations from the OS-level and up across the entire security infrastructure without impacting business. It integrates multiple layers of security to deliver an all-encompassing approach to exposure management and remediation.
  - Establishes security baseline from all existing security tools through AI, behavioral analysis, and correlation rules.
  - Security controls assessment provides a deep evaluation with contextualized insights, risk posture validation, cyber-risk prioritization, security gap detection, cyber hygiene, and false positive detection.
  - Imbued with advanced threat intelligence capabilities to stay ahead of potential threats, analyst or intelligence feeds, and Veriti research.
  - The remediation layer ensures that identified security gaps, threats, and exposures are dealt with effectively and efficiently without disrupting business processes, such as non-disruptive remediation, agentless OS-level, and virtual patching.

Joint Use Cases

- **Use Case #1: Security control assessment**
  Facilitate a seamless and agentless evaluation of your security posture. By integrating with your Fortinet Security Fabric and the entire security stack, Veriti's assessment platform proactively monitors for security gaps and misconfigurations that can jeopardize your security posture and disrupt critical business operations.
- **Use Case #2: Eliminating false positives**
  The integrated solution adeptly tackles the challenge of eliminating false positives. Leveraging AI and behavior analysis, it filters out the noise, allowing security teams to focus on true threats. This precision reduces the burden on resources and enables more confident decision-making, ensuring that cybersecurity efforts are strategically focused and more effective.
- **Use Case #3: Remediation without business disruption**
  The solution delivers seamless remediation without business disruption by implementing non-intrusive, agentless security measures directly at the OS level. Virtual patching techniques are used to shield vulnerabilities instantly, ensuring that critical business functions remain operational while the underlying threats are being addressed, thus maintaining business continuity and operational resilience.

About Veriti:

Veriti is a fast-growing cybersecurity innovator that helps organizations maximize their security posture while ensuring business uptime. With Veriti, organizations can eliminate complexity and operational friction in managing multiple cybersecurity solutions with a consolidated, governing platform that proactively monitors and in a single click, remediates security gaps and misconfigurations across the entire security infrastructure.

February 9, 2024 11:31 PM

2562201-0-0-EN