WHITE PAPER

October 2025

Versa Networks NIS2 Compliance

Disclaimer

This material includes confidential and proprietary information of Versa Networks. It may not be replicated or distributed without the written consent of Versa Networks. This document may include forward-looking roadmap and product strategy information from Versa Networks. It is intended for informational purposes only and should not be interpreted as a commitment on the part of Versa Networks. Versa Networks makes no warranties, expressed or implied, on future functionality and timelines in this document.

Contents

Introduction

The Network and Information Systems Directive (NIS2) is a critical regulatory framework established and adopted by the European Union in November 2022 to enhance cybersecurity across member states. It aims to increase the level of security of critical network and information systems infrastructure, to protect against cyber threats, and ensure the continuity of essential services, across the EU. Starting from the 2016 NIS directive, NIS2 includes stricter obligations, and enforcement requirements for a broader scope of organizations. NIS2 provides for increased security requirements, including:

- Incident Response and crisis management
- Vulnerability management and disclosure
- Software and hardware Supply Chain Security
- Policies and procedures for effective cybersecurity risk management
- Cryptography
- Human Resources security
- Asset Management
- Authentication and Access Control

In 2018, GDPR directive became effective, to safeguard Personally Identifiable Information (PII). Like GDPR, NIS2 also mandates reporting obligations and administrative sanctions for non-compliance and failure to report incidents. Sanctions under NIS2 include recommendations of security audit to ensure compliance with NIS2, and administrative fines of up to 10 million Euros or 2% of the worldwide turnover of an organization.

Versa Unified SASE

This whitepaper will provide a summary and explanation of how Versa Unified SASE addresses NIS2 compliance and enables business organizations to adhere to its requirements.

Versa Unified SASE is a cloud-native multi-tenant software platform that delivers software-defined network/security capabilities for all layers of the network stack – ranging from Layer 2 [switching], Layer 3 [routing] to Layer 7 [application] with full programmability and automation. The Versa Unified SASE addresses SD-WAN, SD-Security, and SD-Branch use-cases for the WAN Edge. This unique approach delivers multiple functions in a single unified software platform that consists of the following software components:

- **Versa Operating System (VOS™):** The multiservice (network, security, SDWAN) software which is deployed at the business edge (branch, cloud).
- **Versa Director:** The single-pane-of-glass management software component responsible for configuration, monitoring, and provisioning.
- **Versa Analytics:** The big data analytics software engine responsible for historical and real-time collection of network, security, and application analytics to deliver insights into SD-WAN fabric policy adherence and performance.
- **Versa Concerto:** The single-pane-of-glass management software component that orchestrates the configuration, monitoring and provisioning that spans one or more horizontally scaled Versa Director instances, and provides a simplified user experience.
- **Versa Messaging Server:** The real time message bus for the Versa solution that propagates network/security intelligence to the VOS instances for real time network/security policy enforcement.

NIS2 Compliance with Versa Unified SASE

NIS2 Requirement	Summary of Versa Capabilities to Meet Compliance
Security of Supply Chains	Versa ensures secure supply chain management through its rigorous vendor assessment and management processes. The platform's multitenant architecture allows secure and isolated environments for different users.
Incident Reporting	Versa Analytics provides comprehensive logging and monitoring capabilities, ensuring that all security incidents are recorded and can be reported as required by NIS2.
Risk Management Measures	Versa Secure SDWAN incorporates robust risk management measures through its integrated security features, including NGFW, IPS, and antivirus capabilities. The platform supports real-time threat detection and automated responses.
Security in Network and Information Systems	VOS provides state of the art security features, including IPsec for encryption and advanced firewalls for network protection. Versa Director centralizes the management of these security features, ensuring consistent application across the network.
Operational Security	Versa Secure SDWAN supports continuous monitoring and maintenance of security measures, ensuring that all components are updated and secure against known vulnerabilities.
Crisis Management and Response	Versa's integrated incident response capabilities ensure that any cybersecurity incidents are quickly identified and mitigated, with detailed logs available for post incident analysis.

Details of NIS2 Compliance with Versa Unified SASE

Security of Supply Chains

NIS2 requires that companies enforce strong protection against risks associated with supply chain of the information and communication technology. Versa Networks associates the highest level of security measures to tackle risks associated with supply chain attacks, by incorporating strong security measures throughout the Software Development Life Cycle (SDLC). This is also demonstrated by the fact that Versa Networks achieved the Common Criteria EAL4+ certification. EAL4+ is the highest security standard achieved by any security vendor, which means that the products delivered by Versa Networks are secure by design and secure by default, including how we build, evaluate, and protect our software. Versa Networks' VOS appliances also support the following security features which provide the maximum protection against hardware and software supply chain attacks:

- **Secure Boot:** The VOS appliances will only load the kernel images that are digitally signed by the Versa build process
- **Verified Execution:** The VOS appliances will allow the execution of only those binaries and libraries that are digitally signed by the Versa build process

Versa Networks regularly conducts vulnerability analysis and penetration testing of the products and services offered by Versa Networks, by both internal and external teams that are experts in security analysis and penetration testing. Versa Networks is also certified for security standards such as ISO 27001, HIPAA, and SOC 2 Type II, whereby all the Versa networks processes are audited annually by accredited security certification companies. Versa Networks is also compliant with the strictest data security and data privacy standards and regulations, including GDPR and PCI-DSS.

Incident Reporting

NIS2 requires that businesses submit a report within 24 hours of becoming aware of security incidents that are confirmed to be critical severity.

Versa Analytics plays a crucial role in incident reporting by:

- Logging all security events and network activities.
- Providing real-time alerts and detailed reports on any detected incidents.
- Facilitating compliance with NIS2's requirement for timely incident reporting to relevant authorities.

Risk Management Measures

Versa Unified SASE provides comprehensive risk management features, including:

- **Next Generation Firewall (NGFW):** Protects against a wide range of threats with advanced visibility, filtering, inspection and enforcement capabilities.
- **Intrusion Prevention System (IPS):** Detects and prevents intrusion attempts in real time.
- **Anti-Virus and Advanced Threat Prevention (ATP):** Integrated antivirus capabilities ensure that all network traffic is scanned for malicious content.
- **Data Loss Prevention (DLP):** Integrated content scanning for identification and protection of sensitive/confidential information.

Security in Network and Information Systems

Versa Unified SASE ensures the security of network and information systems through:

- **IPsec Encryption:** Protects data in transit with AES256 encryption.
- **Advanced Firewall Capabilities:** Prevents unauthorized access and secures network perimeters.
- **Centralized Management:** Versa Director provides a unified platform for managing all security policies and configurations.

Operational Security

Operational security is maintained through:

- Continuous monitoring of network and security systems.
- Regular updates and patches to address vulnerabilities.
- Automated responses to detected threats, minimizing the risk of successful attacks.

Crisis Management and Response

Versa's incident response capabilities include:

- Real-Time threat detection and mitigation.
- Detailed logging and analysis tools for post incident review.
- Support for creating and executing crisis management plans in compliance with NIS2 requirements.

Summary

Versa Networks is the innovator of Unified SASE architecture, delivering integrated cloud, networking, and security services. Versa's leading solution enables enterprises to achieve superior business agility, branch modernization, and compliance with regulatory standards like NIS2. For more information, visit versa-networks.com.

VERSA

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054, +1 408.385.7660, info@versa-networks.com, www.versa-networks.com

© 2025 Versa Networks, Inc. All rights reserved. Portions of Versa products are protected under Versa patents, as well as patents pending. Versa Networks and VOS are trademarks or registered trademarks of Versa Networks, Inc. All other trademarks used or mentioned herein belong to their respective owners. Part# WP_NIS2COMPLY-01