NETWITNESS

netwitness.com

WHITEPAPER

Advanced SOC Visibility

SASE Tool Integration with NetWitness®

NetWitness® and SASE
See Everything. Fear Nothing.

OVERVIEW

Secure Access Service Edge (SASE) is quickly becoming the standard network technology that allows modern workforces to interact with corporate resources wherever they are. SASE significantly benefits today's distributed organizations, featuring better security, which includes encryption and zero-trust network access. However, SASE creates blindspots for important security technologies that perform threat analysis, detection, and response. Special integrations can overcome this issue and restore visibility to critical SASE data.

The shortage of qualified security experts is also a significant global challenge in today's market. The security team must have the right information readily available and easily consumable to ensure high confidence in the decisions necessary to protect company and customer assets and services. Many factors drive the complexity of current multicloud environments, including diverse tool stacks and security solutions. This complexity creates significant challenges in sorting through the myriad log and data sets and alerting feeds, leading to delays in identifying and remediating organizational threats.

This paper describes how NetWitness fits in the SASE architecture and how recent NetWitness platform updates aid security analysts, security operations center (SOC) teams, and investigators in detecting, tracking, and remediating various security threats across cloud or hybrid cloud environments. Many companies are migrating quickly to cloud computing to help improve performance, time to market, and reduce costs. As part of these migrations, careful consideration must be made for security throughout the computing environment, especially in multicloud environments.

The Traditional Approach to Cloud and Multicloud Security

Traditional cloud management security concerns are related to the risks and challenges of protecting data and applications in a cloud-based environment. Key considerations include data loss or leakage, data privacy or confidentiality, accidental exposure of credentials, incident response, legal and regulatory compliance, data sovereignty or residence or control, and protecting the cloud infrastructure from attacks.

A recent report by the Cloud Security Alliance (CSA), Cloud Security Alliance's Top Threats to Cloud | CSA, stated that traditional cloud security issues are becoming less concerning as cloud users and providers mature their understanding and cloud security practices become normalized. However, the report identifies new and more nuanced threats focusing on configuration and authentication issues, such as insufficient identity, credential, access, and key management; weak control plane; metastructure and application infrastructure failures; and limited cloud usage visibility. These threats require more attention to the higher layers of the technology stack and the senior management decisions that influence the technology stack and cloud configurations. Therefore, traditional cloud management security concerns are insufficient to address the complex and evolving challenges of securing cloud computing.

Addressing Cloud Security Challenges with SASE

Securing and managing company assets and data becomes more complicated with the migration to cloud computing, especially when multicloud environments are involved. SASE is a network architecture and technology set that combines wide area network (WAN) and other network security functions into a single service. SASE benefits include:

- Significantly improved visibility across hybrid environments.
- Better control of users, data, and apps.
- Reduced network and architectural complexity.
- Consistent data protection across the environments.
- Reduced operating costs.
- Lower administrative time and effort.

Implementing SASE helps IT teams optimize access performance, reduce operational complexity, and enhance security posture on a global scale. This is typically accomplished by moving the network edge to the cloud and leveraging SASE, significantly reducing performance bottlenecks and security gaps associated with traditional hardware-based appliances and VPNs. SASE enables organizations to simplify their network management, which reduces costs and latency while enhancing security and compliance through improved management, detection, and response capabilities. Because it's a cloud-based service, SASE is scalable by design, making it a viable and welcome option during rapidly changing times.

The SASE approach also addresses the problem of providing secure and reliable access to applications and data for distributed and mobile users, devices, and locations. To accomplish this task, the SASE approach leverages networking technology that integrates the WAN capabilities with network security functions consisting of the core SASE architecture elements such as:

- Software-defined wide area network (SW-WAN) and software-defined local area network (SD-LAN)
- Cloud access security broker (CASB)
- Secure web gateway (SWG)
- Cloud-based endpoint security (antivirus/malware inspection)
- Virtual private networking (VPN)
- Firewall as a service (FWaaS)
- Endpoint detection and response (EDR)
- Data loss prevention (DLP)
- Zero-trust network architecture (ZTNA)

(SASE)

Gartner coined the term SASE in 2019, and since then, enterprises have more aggressively adopted various aspects of the SASE architecture for its advantages to the enterprise.

Managing an SASE environment requires the ability to see the complete picture, capture the data that provides the view of security across the environment in real time, and integrate that view into manageable event alerting and remediation. NetWitness' integrated tools and capabilities provide complete security visibility across hybrid environments and event management. This visibility lets organizations see everything happening in their multicloud and hybrid environments, including users, apps, and data. Additionally, SASE control of users, data, and apps helps organizations ensure that their security policies are enforced consistently across all endpoints, leveraging NetWitness for visibility and validation.

NetWitness for SASE

An SASE vendor should include several key security components:

- A cloud-native architecture of the SASE platform, which ensures scalability, agility, and flexibility.
- Networking and security services typically converged on the SASE platform, such as SD-WAN, WAN acceleration, FWaaS, SWG, and intrusion prevention systems (IPS).
- The ZTNA capability of the SASE platform enables granular and policy-based access to applications and resources for cloud and mobile users.
- The SASE platform's global service level agreement (SLA)-backed private backbone guarantees low latency and high availability.
- The management interface of the SASE platform should be easy to use, intuitive, and robust.

NetWitness' suite of products, starting with the XDR (extended detection and response) platform, delivers the industry's most complete integrated solution for SASE through product capabilities developed over the last 25 years. Our extended list of partners' products integrates with NetWitness' XDR to address security threat management and provide comprehensive visibility and threat detection across the network perimeter. These capabilities enable organizations to secure their remote workforce, cloud applications, and internet of things (IoT) devices with a unified platform that integrates network security, endpoint protection, identity management, and threat intelligence. Unlike other vendors that offer fragmented or siloed services, NetWitness provides an integrated security solution, including network detection and response (NDR), (EDR), (CASB), (SWG), (ZTNA), and threat intelligence as a unified platform. This platform-based approach enables capabilities for SASE to deliver superior threat detection and response across the entire attack surface, from endpoints to cloud applications.

NetWitness applies advanced analytics and machine learning to provide actionable insights and automate workflows for faster remediation. This enables enterprises to achieve greater security efficiency and effectiveness for SASE while reducing complexity and cost. By implementing NetWitness' products, organizations can benefit from the following:

- Reduced complexity and cost. This simplifies the deployment and management of security solutions by eliminating the need for multiple vendors, appliances, and licenses. It also reduces bandwidth consumption and latency by applying security policies at the network edge.
- Enhanced visibility and control. By providing granular visibility into all network traffic and user activity across the distributed enterprise, NetWitness XDR also allows organizations to enforce consistent security policies based on user identity, device type, location, and risk level.
- Improved threat detection and response. NetWitness leverages advanced analytics and machine learning to detect known and unknown threats in real time. Integrating NetWitness with other solutions, such as Broadcom (Symantec), Prisma SASE, Zscaler, Netskope, Skyhigh Security, and Cisco provides a holistic view of the threat landscape and enables rapid investigation and remediation.
- Improved performance and user satisfaction with secure access to cloud applications.
- Faster detection and response to advanced threats.

NetWitness, in the SASE environment, provides a comprehensive solution that accelerates threat detection and response by functioning as a single platform for *all* your security data across the multiple IT environments included in multicloud and SASE architectures. It features an advanced analyst workbench for triaging alerts and incidents and orchestrates security operations programs end-to-end. NetWitness also provides real-time visibility into all network traffic — on-premises, in the cloud, and across virtual environments — enabling an integrated view. Figure 1 below shows how we fit in an SASE and multicloud environment.

Through a unique combination of behavioral analytics, data science techniques, and threat intelligence, NetWitness, in the SASE environment, quickly detects known and unknown attacks that put organizations at risk, facilitating fast, actionable responses to address the identified attacks. This comprehensive security orchestration and automation is designed to improve the efficiency and effectiveness of the SOC and cyber incident response team.

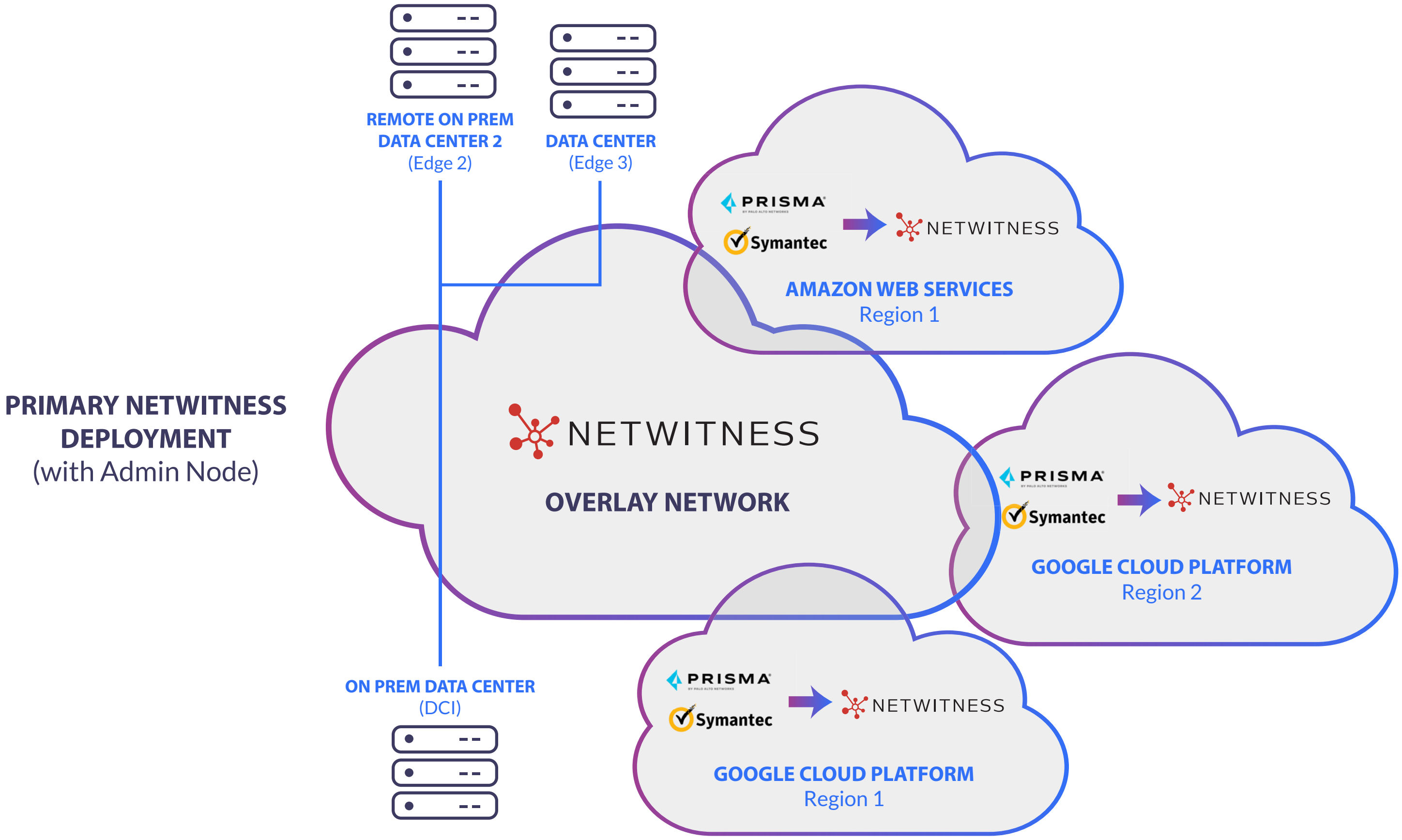

FIGURE 1 — NETWITNESS IN SASE MULTICLOUD ENVIRONMENTS

NetWitness empowers security teams to detect and understand the full scope of a compromise because it analyzes data and behavior across an organization. The integrated platform transforms the data into more useful information through real-time enrichment with business context and threat intelligence delivered from various sources. Utilizing a standardized taxonomy across all data sources accelerates the detection of known and unknown threats, thereby improving resiliency and reducing risks through faster detection and response.

The common taxonomy also facilitates a better understanding of the impact on the organization by the CISO, CIO, and their senior staff, which ensures resources are aligned and prioritized to address the organizational risks. The taxonomy also assists security executives in communicating with business leaders and senior executives to build a common understanding of events and the path to remediate. This approach also provides the baseline for communications with customers and partners based on specific events.

NetWitness has been specially designed for analysts who protect valuable assets and networks. The user interface provides easy access to business and security context, which enables prioritization and faster response to detected threats. This context can include asset criticality, user information from identity solutions, and threat intelligence. We also provide business-context-related reporting to the CISO, technology partners, and business partners on the state of security in the SASE environment and throughout investigation and event response.

As mentioned previously, NetWitness has built-in, direct SASE integration with market-leading SASE partners to deliver unparalleled network visibility across the enterprise. By performing full-packet capture and log monitoring directly on SASE nodes and combining them with all on-prem, cloud, and SaaS sources, enterprise-grade security is maintained, no matter where the data originates.

By incorporating quality network detection, response, and orchestration capabilities that NetWitness provides, enterprises can enhance their detection, management, and response across the MITRE ATT&CK framework. Many enterprises have found the MITRE ATT&CK framework to be useful for evaluating the overall performance of their technology and security stack. Enterprises can validate detection across their attack surface by mapping ATT&CK coverage with NetWitness visibility, detection, and response capabilities.

NetWitness Integration in SASE: The Industry-Leading Cloud-Based Security Solution

NetWitness' approach to integration in SASE provides the industry-leading cloud-based security solution with comprehensive visibility and protection for on-premises, cloud, and multicloud enterprise architectures.

Unlike other vendors that offer fragmented or siloed services, the key components are included to enable the detection, response, and management of threats in the cloud environment using specific capabilities, including NDR, EDR, CASB, SWG, ZTNA, and threat intelligence.

As a result, NetWitness' superior threat detection and response management across the entire attack surface, from endpoints to cloud applications, ensures the high-quality capabilities needed to meet today's threats and minimize risk to your organization. The platform is designed to evolve with your systems and track emerging threats to protect you well into the future. In addition, by leveraging advanced analytics and machine learning, NetWitness provides industry-leading actionable insights and automates workflows for faster remediation.

NetWitness ensures that enterprises gain high-quality, relevant, and focused information provided promptly, facilitating executive awareness, decision-making, remediation, and response. This facilitates more efficient and effective decision-making and focused communication with customers, partners, and regulators.

If you are looking for a cloud security solution that can provide comprehensive visibility and protection for your enterprise, NetWitness integration in SASE is the right choice. Contact us today to learn how we can help you secure your organization.

NETWITNESS

netwitness.com