HPE ARUBA EDGECONNECT SD-WAN AND THE LOOKOUT SSE PLATFORM

ACHIEVE A MODERN SASE ARCHITECTURE THAT SAFEGUARDS DATA ACROSS DEVICES, APPS, NETWORKS AND CLOUDS

Hybrid workforce and cloud adoption drive the convergence of SD-WAN and Security Service Edge solutions

When everyone worked from an office and data and apps were in data centers, your security perimeter protected your data. All applications and security services were hosted in your data centers and network traffic from your branch offices was backhauled over expensive MPLS circuits for security enforcement. Today, this model is less relevant as many business applications are now delivered as SaaS from the cloud, and users connect to applications using both personal and managed devices over networks that are outside your perimeter security. Meanwhile, employees expect to work seamlessly from anywhere at full speed knowing a comprehensive security stack is protecting their devices and data.

Security architectures need to adapt to today's increasingly cloud-based business models and accommodate a perimeter that is now constantly on the move. Visibility and control of valuable and often irreplaceable enterprise resources can be easily lost when users, devices, and data are created and stored virtually anywhere.

This transformation has forced an evolution of how network and security services are delivered, ensuring the most direct and secure access to cloud applications. It no longer makes sense to backhaul traffic across expensive MPLS networks to a centralized data center for security enforcement. Rather, a Secure Access Service

Benefits

- Protect access to data and applications from internal or external cyber threats
- Simplified management of branch office WAN connectivity
- Enhanced visibility of all end user activity
- Better performance for accessing cloud and SaaS apps across the enterprise
- Delivers extensive data discovery capabilities across multi-cloud deployments
- Protects data with advanced classification and Data Loss Prevention (DLP)
- Manages security posture of cloud infrastructure and applications
- Broad integrations with productivity, business and IT applications

Edge (SASE) solution transforms legacy perimeter security into a set of cloud-delivered, converged network and security capabilities that are available when and where they are needed.

By combining the core network component, a Software-defined Wide Area Network (SD-WAN), with the core security components, commonly referred to as Security Service Edge (SSE), enterprises gain full cloud and data security across internet, SaaS applications, and private enterprise applications for any user and branch office regardless of location.

Lookout SSE and HPE-Aruba SD-WAN

To address these security and cost challenges, the integration of the Lookout SSE platform with Aruba SD-WAN provides customers with a best-of-breed secure access service edge (SASE) architecture that blends network security with an integrated security stack delivering secure web gateway (SWG), cloud access security broker (CASB), zero trust network access (ZTNA), and data loss protection (DLP). This integrated solution helps existing Aruba customers protect corporate data stored across any app, any device and any cloud delivering zero trust outcomes.

Customer benefits of the integrated Lookout/HPE Aruba SASE solution include:

Protected access to data and applications from anywhere: Lookout provides secure access to internet, cloud, SaaS and private applications and protects data stored in these apps from unauthorized access and misuse. By using adaptive access policies with continuous monitoring of the user and the device risk, Lookout SSE protects any app, any cloud, any user and any device from internal and external cyber threats.

Simplified management of branch office connectivity: Using Aruba EdgeConnect and the Service Orchestration workflow within Aruba Orchestrator, network administrators can automatically create secure IPSec tunnels between branch locations and Lookout SSE platform enforcement points. This avoids the need to manually create tunnels every time a new branch or a new app is onboarded and simplifies the management of site connectivity.

Enhanced visibility of all end user activity: Aruba customers can use the Lookout SSE user and entity behavior analytics (UEBA) to to understand device posture, IP addresses and user context when users access corporate apps and data, or the internet in general, from any branch or remote location. This allows customers to monitor end user activity, gain control and visibility into usage of shadow IT/unsanctioned apps, and monitor internal and external cyber threats.

Better performance for accessing cloud and SaaS apps: Legacy architectures force customers are forced to backhaul traffic for cloud and SaaS apps to enforce inline security policies and get complete visibility of the traffic. However, backhauling the traffic increases latency and affects the performance of these apps. With the joint Lookout/HPE Aruba solution, existing EdgeConnect SD-WAN customers can avoid backhauling traffic for cloud and SaaS apps, enforce inline policies and maintain complete visibility – all without compromising on performance.

Best-of-breed secure access service edge (SASE)

HPE (Aruba) has been named an SD-WAN Magic Quadrant Leader five years in a row. Aruba EdgeConnect Enterprise is an advanced, secure SD-WAN platform that supports the necessary WAN Edge functions needed for SASE including SD-WAN, firewall, segmentation, routing, WAN optimization and application visibility and control in one centrally managed platform designed to protect the branch from incoming security threats. The platform enables customers to build a unified WAN edge that is business-driven, delivers the highest quality of experience, and continuously adapts to changing business needs and network conditions. HPE Aruba integration with Lookout, enables enterprises to fully and securely embrace digital transformation.

The Lookout Security Service Edge platform delivers a full endpoint to cloud security solution including secure web gateway (SWG), cloud access security broker (CASB), and zero trust network access (ZTNA). These integrated solutions include advanced data and threat protection capabilities within a single console and with unified policy enforcement. With centralized data loss prevention (DLP) policies, you can detect, classify and protect sensitive data across any cloud deployment, email and applications in a consistent manner. With user and entity behavior analytics (UEBA), enterprise customers can detect and respond to insider threats and advanced cyberattacks.

- **CASB:** Gain visibility and control over your SaaS applications, including Office 365, Google Workspace, Box, Salesforce and others, and ensure your sensitive data is protected wherever it goes. With automated data protection policies, such as rights management and encryption, empower secure collaboration by protecting data shared internally and externally. Automated assessment of all your cloud apps and infrastructure ensures they are properly configured.

- **SWG:** With a single proxy architecture and inline controls, Lookout not only inspects all incoming and outgoing web traffic fr malicious content but also prevents sensitive data from leaking to the public internet. This safeguards the enterprise hybrid workforce from internet-based threats and enables always-on security, simplified IT, and a seamless user experience.

- **ZTNA:** Continuously monitors users requesting access to your on-premises enterprise applications and applies dynamic access controls to authorize secure access. By leveraging the risk context of users, devices, applications and data, Lookout delivers zero trust outcomes for securing private applications and data.

Built from the ground up, the platform is powered by unified protection policies that can be applied across all users, devices, applications, and data to ensure consistent policy enforcement across hundreds or even thousands of branches – without buying, deploying or managing any physical security appliances.

Together Aruba and Lookout, leaders in WAN edge and security infrastructure solutions, enable customers to implement zero trust and SASE frameworks that uniquely addresses the evolving business needs faced by cloud-first enterprises today.

HPE Aruba and Lookout deliver better business outcomes

To enable cloud-delivered security and deliver the best cloud application performance, Aruba EdgeConnect Enterprise provides seamless connectivity to Lookout using integrated service orchestration. With integrated service orchestration, secure IPsec tunnels are established between branch locations and the Lookout cloud security enforcement points. To meet global enterprise scalability and performance requirements, Lookout SSE solution connectivity is available from global datacenters with high-availability services to ensure the highest level of performance. Together, this joint solution delivers the following outcomes:

- Protected access to data and applications from anywhere

- Simplified management of branch office connectivity

- Enhanced visibility of all end user activity

- Better performance for accessing cloud and SaaS apps

Lookout®

Deployment Architecture
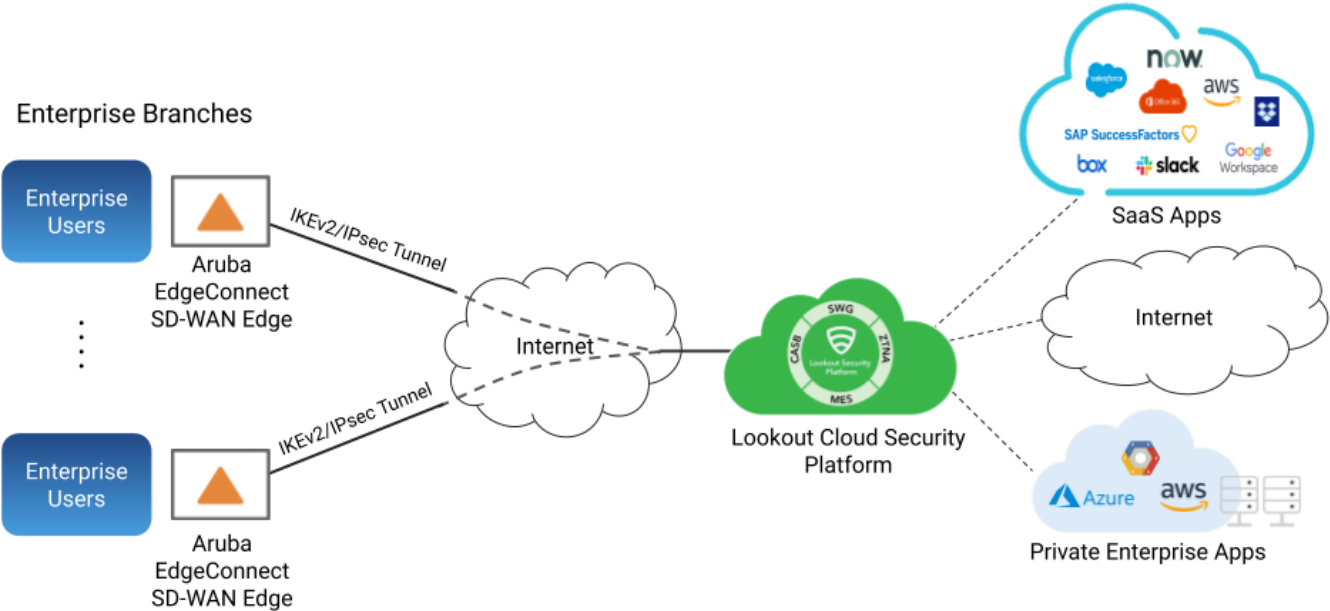
About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely. To learn more about the Lookout Security Platform, visit **www.lookout.com** and follow Lookout on its **blog**, **LinkedIn**, and **Twitter**.