Lookout®

WHITEPAPER

Strengthening cloud security with SASE

The journey of data

Businesses are no longer constrained to a single location, network, or cloud. What gives meaning to the infinite channels, clouds, devices, users, and transactions in the enterprise landscape is data. With new devices, a mobile workforce, and global partnerships, data is the common denominator that enables businesses to function and governments to run, almost seamlessly.

Keeping this diverse data environment secure across all touchpoints can no longer be just addressed through siloed traditional measures. In the current business environment, security organizations should be ready to flex their muscles, adapt and scale to accommodate this natural evolution from endpoints to the cloud.

Echoing this evolution, Gartner in 2019 introduced the Secure Access Service Edge (SASE) cloud architecture. It is touted as the future of cloud architectures as organizations continue their cloud journey, including application adoption as well as infrastructure migrations. SASE might prove to be the security solution that's needed in these changing times.

The current security crisis

Most organizations today have added cloud security to on-premises protection to address rising concerns about vulnerabilities. However, other security and network solutions are still required beyond the cloud – at headquarters and branch offices, and for the remote workforce - to ensure continuity of operations.

Consider these scenarios that highlight the lack of a centralized security strategy:

- A Latin America business unit of a U.S. corporation signs an agreement with a European distributor and bundles its software for resale in several European Union countries. The business unit extends a third-party CRM application to the distributor to place orders that include some regulated data under GDPR. U.S. corporate legal, governance and compliance teams are unaware of this GDPR violation.
- A sensitive document in your cloud is downloaded to an employee's personal mobile device and emailed to an outside party. Or a former employee downloads cloud data and takes it to a new employer. You have no way to restrict or control the transfer of your sensitive data.
- Unintentional misconfigurations leave cloud data exposed and allow unauthorized access. In 2017, Accenture reportedly left unsecured a massive store of private data across four cloud servers, exposing passwords and decryption keys that could have caused considerable damage.

Most organizations support several disparate network and security solutions – firewalls, VPNs, secure web gateways, DNS and cloud security coupled with WANs and other tools that are meant to improve network performance.

Unfortunately, this creates multiple, independently operated siloes. With zero visibility into what the other is doing, this lack of seamless, systematic control weakens an organization's security posture. The formidable complexity of managing multiple security systems often leads to misconfigurations, excessive operating costs and increased vulnerabilities.

The perils of a mobile workforce

In a mobile workforce, the number of security vulnerabilities increases by orders of magnitude due to the sheer volume of endpoint devices. Although unintentional, this creates a massive attack surface of exposed endpoints that cybercriminals will exploit.

Most employees who work remotely each use multiple managed and unmanaged personal devices that connect to enterprise cloud apps and other highly sensitive data from unsecured networks.

And as enterprises extend collaboration to more employees, suppliers and customers, the lack of visibility and control to the edge increases the risk of data loss, noncompliance and devastating breaches.

Burdened with imminent crisis, security and risk management leaders are now asking:

- What's the right mix of access controls and policies to ensure data is secure? What are the risks of using multiple personal devices? Who are the users, what devices do they use and where are they located?
- Do we enforce data privacy and compliance regulations across all office locations worldwide? What are the local penalties for noncompliance?
- With a burgeoning mobile workforce, are we prepared to face emerging cyber threats, vulnerabilities and data loss due to the expanding attack surface?

Key tenets of SASE

Professionals who are immersed in cloud security often utilize three key metrics to avert data breaches and ensure compliance with regulatory mandates.

- How is access to data controlled?
- How is data protected and encrypted to prevent breaches?
- What data protection policies are in place to monitor risks, assess threats and track compliance?

Step away from the data center and into the cloud

Because no physical perimeter exists in the cloud, SASE calls for a dynamic perimeter. It is a mesh of network and security capabilities that are applied when and where they are needed. This dynamic perimeter ensures that employees can only access the enterprise apps and services they are authorized to use.

Other differentiating characteristics of the SASE model include:

Identity-aware architecture – Security context and access decisions are based on the identity of the connection source, such as user, device, branch office, IoT device, or location.

Scalable services and policies – Enforcement of required services and policies on-demand occur independent of the location of the connection source.

Key benefits of SASE

SASE brings digital transformation across cloud access security, network, and network security services, and mobile endpoints used by today's remote workforce.

- **Reduced complexity and increased cost savings:** Disparate legacy solutions are replaced with a consolidated extendable security solution that strengthens security posture, removes overlapping security silos, and reduces overheads. You can easily scale security policies in response to new threats and traffic inspection mechanisms.
- **Stronger security with unified policy enforcement:** Cloud-based policy management lets you easily control access to cloud apps by users, devices, and networks, irrespective of perimeters. Policies can enforce geo-anomalies, local compliance rules, and access protection for managed and unmanaged devices in real-time.
- **Improved visibility, protection and user experience:** Consistent access control policies provide a secure and uniform user experience across all users, devices, networks, and locations. Real-time content inspection, control and remediation measures can be applied to ensure readiness against any security violations.

Risk monitoring and trust assessment – Active sessions and user behaviors are continuously monitored to assess trust levels and identify potential risks.

In summary, integrated SASE capabilities are delivered as a service based on identity awareness, real-time context, enterprise security policies, and the nonstop assessment of risk and trust factors for the duration of a session.

Implementing SASE in the current cloud scenario

Most enterprises currently rely on some type of on-premises, cloud or hybrid security and want to protect their legacy investments. To consolidate and centralize the security posture based on SASE principles, an organization would need to consider best-of-breed integrations and solutions that can be brought to scale.

The Lookout suite of cloud-native endpoint-to-cloud security provides a strong foundation for organizations that are ready to rollout SASE. Architected for scale and centrally managed and controlled, Lookout protects data from endpoint to the cloud and dramatically reduces business risk by delivering:

- Full visibility into users, devices, apps, networks, and data.
- Protection against zero-day threats, ransomware and other malware, data breaches, and malicious insiders.
- Safeguards for data at rest and data in motion.

However, the real power of Lookout is its ability to protect your previous investments in on-premises legacy apps and security by protecting your previous investments in on-premises solutions.

Lookout also provides seamless API integration to send telemetry data from your unified security platform to cloud productivity suites like Microsoft Office 365, Google Workspace, VMWare Workspace ONE Intelligence, and other third-party solutions.

In the example above, continuous security telemetry from the Lookout SASE-based security platform is shared with Microsoft Enterprise Mobility + Security (EMS) and Google Cloud Identity to enhance security. And by sharing telemetry data with VMware Carbon Black, you can consolidate mobile security intelligence with fixed endpoint security.

Enabling a unified security and management experience, these integrations together provide unprecedented security insights into users, devices, apps, networks, and cyberthreats and enforces conditional access based acceptable risk levels.

Key considerations before launching SASE

As today's most viable architecture for building a holistic security strategy, it's important to consider what you will require from SASE before you get started:

Cloud access security broker (CASB)

- Use data loss prevention (DLP) to discover and protect structured and unstructured data that is sensitive.
- Use encryption to obfuscate, protect and apply enterprise digital rights management (EDRM).
- Use data discovery and classification to monitor data access.

Mobile endpoint security

- Nonstop assessment of user, device and app security posture to reduce risk
- Dynamic access controls and policy enforcement for users and devices.
- Stop mobile threats using AI-driven, cloud-powered detection and response.
- Protect iOS, Android and Chrome OS.
- Secure company-owned (managed) and employee-owned (unmanaged) devices.

- Meet compliance requirements while protecting user privacy.
- Scale to protect mobile fleets with hundreds of thousands of endpoints.

Apply access controls

- Centralized identity- and context-aware protection with secure sign-on (SSO) and multifactor authentication (MFA) everywhere.
- Use advanced behavior monitoring, such as user and entity behavior analytics (UEBA), to augment data and user security.

Simplify operations

- Centralized management and unified control from endpoints to the cloud protects data and reduces risk along the entire enterprise data path.
- Leverage APIs to integrate SASE with cloud productivity suites, fixed endpoint security and other third-party security solutions.
- Operationalize your enterprise security infrastructure from mobile endpoints and personal devices to the cloud.

Secure against the biggest threat vector first

SASE will continue to evolve as it is driven by newly emerging security requirements. As your remote workforce continues to flourish, it is imperative to protect data and reduce risk by securing users, devices, apps, networks, and the cloud as one cohesive entity.

The optimal way to secure this mobile-to-SaaS environment

Lookout delivers a centralized security platform for SASE that integrates endpoint security, CASB, zero-trust network access (ZTNA), and other siloed security solutions. This enables you to centrally manage and dynamically control your entire security infrastructure.

The Lookout approach to SASE protects all your data from endpoints to the cloud by providing all-important visibility into users, devices, apps, access privileges, networks, and the cloud.

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

To learn more, visit www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.