Lookout

THE LOOKOUT SASE SOLUTION

SECURITY FROM ENDPOINT TO CLOUD, ENABLING PRODUCTIVITY FROM ANYWHERE

Your users, apps, and data have left the building

Your apps and data used to reside in data centers, and everyone worked from an office. To gain access, your workforce connected to internal networks using company-issued laptops or desktops. With a security perimeter, you were able to control data flow and protect your organization's data. You also knew what was stored on your endpoints as they were managed by you.

All that changed with cloud technology and remote work. Today, your data goes wherever it is needed. Employees now expect effortless access to whatever they requireneed from anywhere and on any device. To tap into the skyrocketing collaboration, organizations felt they had to relax their security stance as they embraced the cloud. But just because your apps and data left the building, it doesn't mean you're no longer their custodian.

From five corporate locations to five thousand remotes offices

Investing in virtual private networks (VPNs) is how many organizations are supporting their remote workers. While it enables access to on-premise apps from anywhere, it also assumes that every user and device is trustworthy. And because VPN provides whoever is connected unrestricted access to your internal networks, it puts your entire infrastructure at risk.

To promote collaboration while keeping your data secure, you need complete visibility and dynamic access controls. This is where a new framework called secure access service edge (SASE), comes in, delivering protection in the cloud like you still have a perimeter.

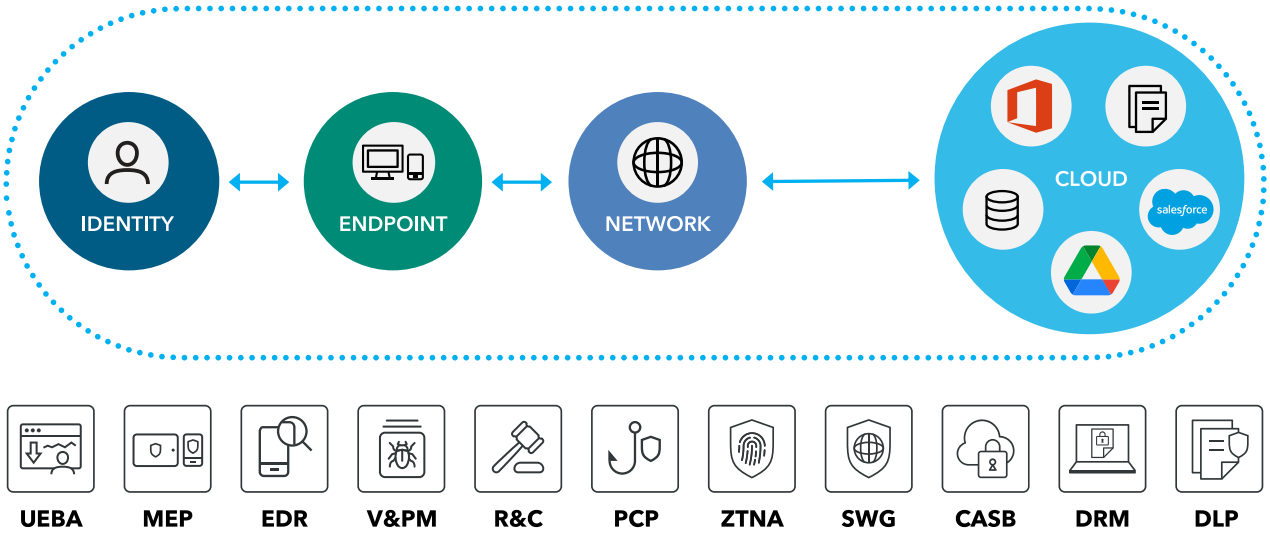
Dedicated SASE vendors only provide network-based insight into threats and have limited visibility into the security posture of the endpoint. This means they lack the endpoint capabilities and only have a fraction of what is required to effectively secure an organization from endpoint to cloud. Existing SASE technologies are also invasive and clash with the users expectation of privacy, especially on their personal devices.

You need an integrated endpoint-to-cloud solution

Right now, if you want security from endpoint to cloud, you need to buy standalone tools that solve specific problems. But that creates complexity and inefficiency. They also don't address data security holistically.

Lookout delivers a single security platform that protects your data from endpoint to cloud in a manner that respects personal privacy. Here's what our integrated solution looks like:

1. Precise controls that provides dynamic access based on full insights
2. Full visibility into your users, endpoints, apps and data
3. Protect your data regardless of where it goes or how it's being handled
4. A single place to implement precise policies, hunt for threats and conduct investigations
5. Respect personal privacy



Visibility like you still have a perimeter

The first step of securing data is knowing what's going on. It's hard to see the risks you're up against when your users are everywhere, using networks you don't control to access your apps and data in the cloud. We eliminate the guesswork by providing visibility into what's happening – on managed and unmanaged endpoints, in the cloud and everywhere in between.

We detect insider threats and file-less cyberattacks by analyzing behaviors rather than performing deep inspection of devices, apps and data.

By understanding anomalous user behavior within your infrastructure, such as sharing, downloading, and deleting data, we make it easy to spot the suspicious activity of a malicious insider. We have deep knowledge of your data regardless of where you store them – in data centers, public cloud and multi-cloud environments. We also continuously monitor the risk level of your endpoints so you can dynamically modify access to protect your data. This data combined with app, device and network threat detections delivers the most comprehensive security posture across your endpoints.

Unified insights to make sense of everything

Standalone tools make cybersecurity unnecessarily complex and inefficient. Your team may make mistakes and glance over security policy inconsistencies if they have to manage multiple solutions. Our integrated platform gives you actionable insights across users, endpoints, apps and data.

Every organization now uses countless apps and cloud platforms to support their employees – whether it's productivity suites such as Microsoft 365 or Google Workspace, customer relationship management like Salesforce or HR related apps like Workday. With everything in one place, you can implement consistent security policies that ensure you stay in total control. We give you visibility into what's happening on all your cloud apps and platforms so you can identify anomalous, malicious behavior or vulnerabilities. These could include malicious third-party integrations or libraries buried deep in the app's code. We also know how your data is being handled, stored and transferred so you can protect your data dynamically.

We also provide all the telemetry data you need to hunt for threats and conduct forensic investigations into advanced cyberattacks. You receive instant alerts to bring attention to issues of interest, and administrators can customize notifications for anomalous events and suspicious activities. With aggregated reporting, you have extensive audit trails across all devices, network connections and cloud services to help you pinpoint exactly where and how an incident took place.

Precise controls for dynamic secure access and collaboration

Your employees want to work from anywhere at any time, so all-or-nothing access to corporate data in the cloud or on-premises creates unnecessary risk. To protect your data, you need to secure every interaction with users, endpoints and apps. With complete visibility into everything, unified insights and integratedunified controls, you can dial-in precise access to provide seamless and efficient connection and collaboration.

We provide granular and dynamic access that matches each user's risk posture, such as whether the device has malware installed or if the user is accessing sensitive data unrelated to their role. We understand what apps and data your employees need for work. As a result, we enable your employees to securely and dynamically access what they need – whether it's stored in enterprise applications within your perimeter, private cloud or cloud applications.

Security also should not interrupt productivity or impair the user's experience. We have deep knowledge of your data and can extend seamless data protections across your entire organization, ensuring that workflows are not interrupted. We provide encryption of data at rest, in-flight, and in-use, enabling you to address the strongest security requirements while still providing users access online and offline. We can even encrypt sensitive data as it's being downloaded to enforce digital rights management that prevent unauthorized access.

Work anywhere with endpoint-to-cloud security

With digital collaboration skyrocketing, data now goes wherever it's needed. To tap into this boosted productivity without risking your data, you need to be able to secure any endpoint, using any network, connecting to any application. Lookout integrates endpoint security with SASE so you can protect your data from endpoint to cloud in a manner that respects personal privacy.

About Lookout

Lookout is a 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.**

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo

Integrated endpoint-to-cloud security

Learn more at **lookout.com**

© 2021 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT®, and PROTECTED BY LOOKOUT®, are registered trademarks of Lookout, Inc. in the United States; and POST PERIMETER SECURITY ALLIANCE™ is a trademark of Lookout, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders. 20210415-Lookout-USv1.0

Lookout®