Lookout

LOOKOUT SECURE WEB GATEWAY

PROTECT YOUR ORGANIZATION AND DATA FROM INTERNET THREATS

In an effort to support hybrid work and boost productivity, organizations are moving away from traditional on-premises solutions to cloud-based services. A major effect of this shift is the increased reliance on the internet as the corporate network. This transformation, however, increases the risk to employees and organizations as users and data circumvent perimeter-based security controls. Without those controls, organizations have lost visibility into internet-based threats, such as malicious websites and insecure web apps, thereby increasing the risk of cyberattacks for every organization.

Challenges

The concept of network and security perimeter has turned inside out. With apps and data residing in the cloud and users connecting from anywhere, IT has lost the visibility and control they had with legacy tools. Below are the challenges IT organizations are facing as a result.

Online collaboration and remote work increase data security risk

More than ever, employees are using the internet and web apps to get work done. They are bypassing perimeter-based security to connect directly to whatever they need, from any device and location. With traditional tools rendered obsolete, company data is spread across unsanctioned apps, websites and cloud vendors. This creates countless places for attackers to steal data or distribute malware by using malicious websites.

BENEFITS

- Protect hybrid workforce from internet-based threats
- Enforce effective cloud governance and help achieve compliance
- Monitor and assess risk with web and cloud usage
- Protect corporate data stored in unsanctioned SaaS and cloud apps
- Improve end user experience with direct access to internet

Lack of protection against modern-day threats like ransomware

Organizations with highly sensitive information are attractive targets of ransomware attacks. Bad actors typically leverage phishing attacks to trick users into providing login credentials to the corporate environment. With credentials in hand, attackers can penetrate an organization's network and execute malicious code to encrypt or exfiltrate sensitive data.

Unsanctioned apps add hard-to-detect Shadow IT risk

The risk of Shadow IT and unsanctioned apps has never been greater. Cloud services such as file storage, messaging and video solutions, while designed for consumers, offer a convenient option for work tasks. Unfortunately, on-premises web gateway solutions are unable to detect them.

Legacy gateways are inefficient and have limited visibility into the modern environment

Organizations using on-premises secure web gateway (SWG) solutions must backhaul traffic through a data center. Excessive latency not only creates poor end user experiences, it also limits the range of security that can be applied to a data stream in real-time. For example, to block the upload of sensitive data to a website, a SWG needs to inspect data, apply policies, and take protection action, all in one motion. A lag in throughput degrades effective detection and response, exposing the organization to increased risk of data leakage.

On-premises SWG appliances also require more maintenance, labor and logistics to scale to geographically-dispersed locations. An upgrade of physical hardware across several data centers would require technicians to go onsite, perform the upgrade, test it and ensure all appliances are functioning properly.

Benefits of the Lookout Secure Web Gateway

Lookout SWG is cloud delivered and built on the principles of Zero Trust to protect users, underlying networks and corporate data from Internet based threats. With a single proxy architecture and inline controls, Lookout can efficiently inspect all incoming and outgoing web traffic for malicious content. This enables always-on security, simplified IT, and a seamless user experience.

As organizations transition from on-premises security solutions to cloud-delivered services, they need a platform that enables them to pace their migration to the cloud. A platform-centric approach ensures that policies can be applied consistently across all workloads and use cases. This provides organizations with a much simpler way to manage and deploy security tools, monitor end user activity and enforce organizational policies such as Shadow IT.

Protect hybrid workforce from internet-based threats

The single proxy architecture allows Lookout to get complete visibility of all end-user traffic whether accessing Internet, SaaS apps, or private enterprise apps. With this end-to-end visibility, IT can enforce policy controls on both sanctioned and unsanctioned apps to prevent unauthorized traffic from entering the corporate network.

URL filtering enables admins to control which websites their employees and guest users can access based on threat intelligence from hundreds of millions of websites, domains and apps in the Lookout Security Graph. Lookout also integrates with multiple threat-intelligence engines to provide the latest threat signatures and information. This allows Lookout SWG to detect and stop any internet-based attacks like ransomware, phishing, zero day and browser-based threats.

Enforce effective cloud governance and help achieve compliance

The ability to differentiate between corporate versus personal instances of cloud apps feeds Data Loss Prevention (DLP) policies that can apply different actions depending on which instance data is being sent to. These actions include encrypting, watermarking, masking, redacting, highlighting, setting expiration times or allowing offline access. By detecting the destination of the data, Lookout prevents it from being sent to unauthorized locations, apps or users that could put the organization in violation of compliance or data privacy laws.

Lookout SWG also offers adaptive access controls that are based on a user's risk score, device posture and location for automatic enforcement of security policies that ensure compliance with local and industry regulations.

Monitor and assess risk with web and cloud usage

Lookout allows complete consolidation of IT security infrastructure with a unified platform delivering a single proxy, a single end user agent and a single policy infrastructure. This eliminates the need for multiple IT security tools from different vendors, thereby reducing the risk of human errors and inconsistent policies. Lookout performs TLS/SSL inspection on all inbound and outbound traffic passing through the SWG proxy so that packet decryption and encryption only needs to happen once. This not only provides the visibility needed to apply protection policies but it also results in a smoother, faster end-user experience.

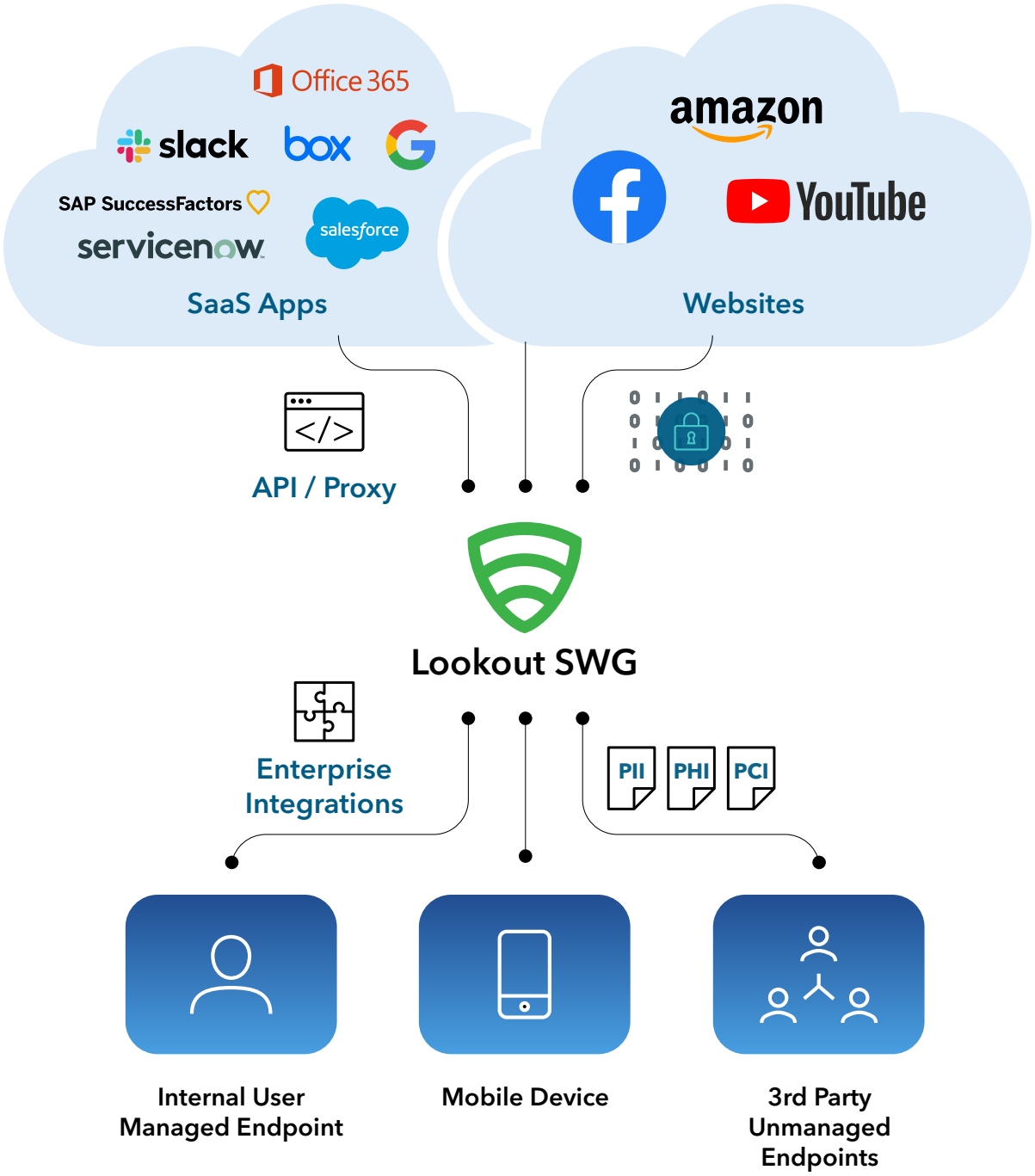
Protect corporate data stored in unsanctioned SaaS and cloud apps

By supporting both managed and unmanaged devices, admins can provide secure access for contractors and supply-chain partners, allowing IT teams to monitor activity across any device. This provides IT with complete end-to-end visibility to ensure proper enforcement of security policies for protecting sensitive information.

Lookout SWG leverages industry-leading intelligence gathered from over 20,000 apps, enabling it to identify Shadow IT as users are connecting to unauthorized apps or personal accounts. This ensures real-time threat protection.

Improve end user experience with direct access to Internet

Unlike traditional solutions that backhaul traffic, Lookout SWG provides security controls closer to the users and apps by being delivered from the cloud. This proximity enables it to efficiently enforce security inline or via API, ensuring the end user has a seamless experience.


Office 365
slack
box
SAP SuccessFactors
servicenow
salesforce
SaaS Apps
amazon
YouTube
Websites
API / Proxy
Lookout SWG
Enterprise Integrations
PII
PHI
PCI
Internal User Managed Endpoint
Mobile Device
3rd Party Unmanaged Endpoints

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.**

For more information visit
lookout.com

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

Data-Centric Cloud Security

Learn more at **lookout.com**

Lookout®