



Lookout cybersecurity software provides Customers with an integrated endpoint to cloud security solution that can protect the Customer's data wherever it goes whether in the data center, public cloud or end user mobile device. This end-to-end protection enables users the flexibility to work anywhere, anytime while still helping to provide the same high level of data security required in today's hybrid work environments.

Lookout software falls into one of two portfolios. The first is **Mobile Endpoint Security (MES)**.

**Mobile Endpoint Security (MES)** is a cloud-delivered security platform and a lightweight app that protects iOS, Android and Chrome OS devices. MES can secure company-owned and employee-owned devices from phishing risks, application risks, network risks and device-based risks. MES helps companies meet compliance requirements while preserving end user privacy by providing deep insights into mobile application and operating system vulnerabilities. MES also provides endpoint detection and response tools that work to prevent breaches and respond to incidents.

The second portfolio is **Secure Service Edge (SSE)** which is a suite of software to help safeguard SaaS and private apps, as well as, Internet Access. Secure Service Edge solutions are:

**Cloud Access Secure Broker (CASB)** simplifies security governance on cloud-hosted web applications. Lookout CASB readily integrates with SaaS applications such as Google Workspace and Microsoft Office 365 to help a) deliver extensive data discovery capabilities across multi-cloud deployments, b) protect data with advanced classification and data loss prevention (DLP) capabilities, c) secure and control data shared externally with encryption and data rights management, d) detect insider threats with user and entity behavior analytics (UEBA), and e) manage security posture of cloud infrastructure and applications. Lookout CASB skus are available in 1, 2 and 3-year terms and can be purchased in bundles which cover different numbers of SaaS applications. Add on features are also available for specific use cases.

**Zero Trust Network Access (ZTNA)** provides granular identity and context-aware access controls for enterprise applications in private data centers or IaaS infrastructure. ZTNA application-centric control limits access only to those who need it. Application cloaking prevents discovery on the public internet. ZTNA also extends advanced security to legacy applications with identity and access management. ZTNA uses the Lookout platform's data loss prevention (DLP) and protection capabilities to secure data. Lookout ZTNA skus are available in 1, 2 and 3-year terms.

**Secure Web Gateway (SWG)** works to protect hybrid workforces from internet-based threats and enforces effective cloud governance to help achieve compliance. SWG can a) monitor and

cloud apps and c) improve end user experience with direct access to the internet without backhauling traffic

In addition to the above software subscription licenses, Lookout also offers optional:

**Support and Deployment** SKUS that provide Customers with access to Lookout technical support engineers via the Lookout Enterprise Support Portal. Customer can purchase the level of desired support as either Standard, Premium, or Premium Plus. The Standard and Premium service leverages a shared pool of support resources with the primary difference being that the Premium service is available 24x7x365, whereas the Standard service is only available during local business hours. Premium Plus service provides a white glove level of service with a dedicated support and deployment services team available through the lifecycle of the product deployment.

**Threat Intelligence reporting** SKUs that provide Customer with monthly reports containing the latest threat encounter rates, trends, and top threat families globally.