Lookout®

DIE SASE-LÖSUNG VON LOOKOUT

PRODUKTIVITÄT VON ÜBERALL AUS DANK SICHERHEIT VON ENDGERÄT BIS HIN ZUR CLOUD

Benutzer, Apps und Daten sind jetzt überall verteilt

Ihre Apps und Daten waren zuvor in Rechenzentren gespeichert und alle Mitarbeiter griffen aus dem Büro darauf zu. Dazu stellten sie über firmeneigene Laptops oder Desktops eine Verbindung zu internen Netzwerken her. Im Sicherheitsperimeter konnten Sie den Datenfluss kontrollieren und Unternehmensdaten schützen. Außerdem wussten Sie immer, was auf den Endgeräten gespeichert wurde, da Sie diese verwalteten.

All das hat sich mit Cloud-Technologie und Remote-Arbeit geändert. Jetzt sind Ihre Daten überall dort abrufbar, wo sie benötigt werden. Mitarbeiter erwarten heute mühelosen Zugriff auf alle erforderlichen Ressourcen, von überall und jedem Gerät aus. Um von diesen unbegrenzten Möglichkeiten der Kollaboration zu profitieren, haben viele Unternehmen ihre Sicherheitsrichtlinien für die Cloud-Nutzung gelockert. Sie sind aber nach wie vor für Ihre Apps und Daten verantwortlich, auch wenn diese jetzt überall verteilt sind.

Von fünf Unternehmensstandorten zu 5.000 Remote-Büros

Die meisten Unternehmen unterstützen ihre Remote-Mitarbeiter über virtuelle private Netzwerke (VPNs). Diese ermöglichen zwar den Remote-Zugriff auf lokale Apps, vertrauen aber auch jedem Benutzer und Gerät. So gewährt ein VPN jedem verbundenem Benutzer uneingeschränkten Zugriff auf interne Netzwerke und gefährdet damit die gesamte Infrastruktur.

Um die Zusammenarbeit zu fördern und gleichzeitig Daten zu sichern, benötigen Sie komplette Transparenz und dynamische Zugriffskontrollen. Hier kommt das neue Framework "Secure Access Service Edge" (SASE) ins Spiel. Damit erhalten Sie einen Schutz in der Cloud wie im Perimeter.

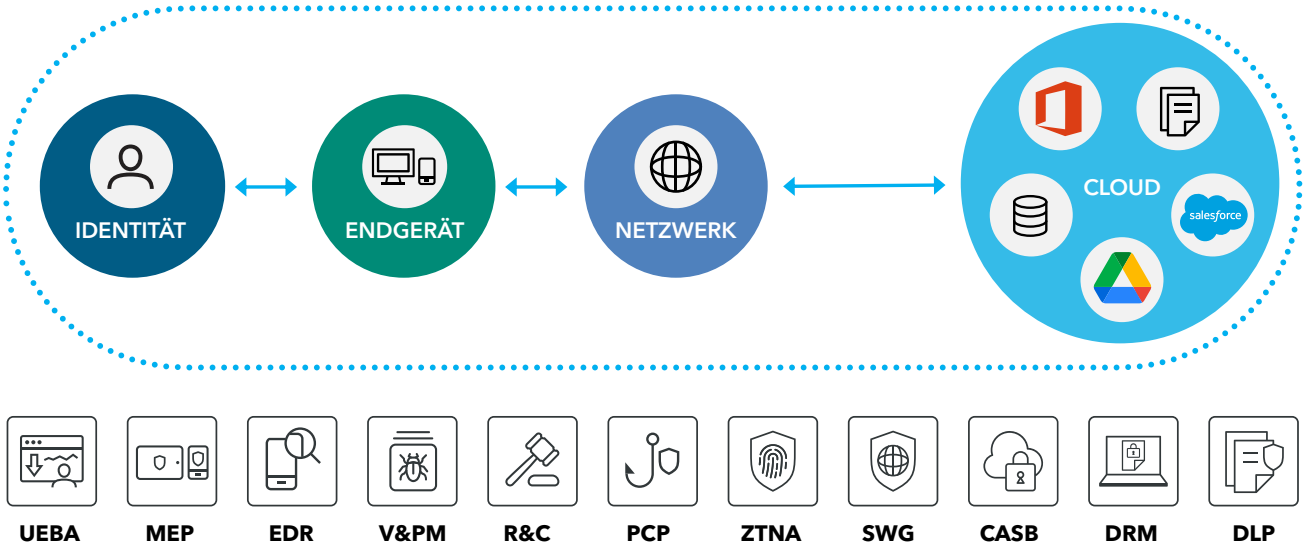
Dedizierte SASE-Anbieter bieten nur netzwerkbasierte Einblicke in Bedrohungen und begrenzte Informationen zur Endgerätesicherheit. Das heißt, sie verfügen nicht über die erforderlichen Endgerätefunktionen und erfüllen nur einen Teil der Voraussetzungen für die effektive Sicherung eines Unternehmens von Endgerät bis in die Cloud. Aktuelle SASE-Technologien sind zudem invasiv und dringen in die Privatsphäre von Benutzern ein, besonders auf ihren privaten Geräten.

Sie benötigen eine integrierte Lösung vom Endgerät bis in die Cloud

Wenn Sie derzeit Sicherheit vom Endgerät bis in die Cloud einrichten möchten, müssen Sie eigenständige Tools kaufen, die jeweils bestimmte Probleme lösen. Das sorgt aber für Komplexität und Ineffizienz. Diese Tools gehen die Datensicherheit auch nicht ganzheitlich an.

Lookout bietet eine einzelne Sicherheitsplattform, die Daten von Endgerät bis Cloud schützt und dabei die Privatsphäre der Anwender respektiert. So sieht unsere integrierte Lösung aus:

1. Präzise Kontrollen, die dynamischen Zugriff basierend auf umfassenden Einblicken bereitstellen
2. Vollständige Einblicke in Benutzer, Endgeräte, Apps und Daten
3. Schutz von Daten an jedem Ort und bei jeder Verarbeitungsweise
4. Zentrale Plattform, in der Sie präzise Richtlinien implementieren, Bedrohungen aufspüren und forensische Untersuchungen durchführen können
5. Achtung der Privatsphäre der Anwender



Transparenz wie innerhalb des Perimeters

Um Daten zu sichern, müssen Sie zunächst einmal wissen, welche Aktivitäten ausgeführt werden. Risiken können nur schwer ermittelt werden, wenn Benutzer von überall aus arbeiten und diese Nutzer mit Netzwerken die außerhalb Ihrer Kontrolle liegen, auf Apps und Daten in der Cloud zugreifen. Wir bieten Ihnen vollständige und zuverlässige Einblicke in alle Aktivitäten – an verwalteten und nicht verwalteten Endgeräten, in der Cloud und überall dazwischen.

Wir erkennen interne Bedrohungen und Cyberangriffe ohne Dateibeteiligung, indem wir das Verhalten analysieren, anstatt Geräte, Apps und Daten genau zu untersuchen.

Wenn Sie ungewöhnliches Benutzerverhalten in der Infrastruktur, wie Freigeben, Herunterladen und Löschen von Daten, erkennen, können Sie die verdächtigen Aktivitäten eines böswilligen Insiders einfach identifizieren. Wir schützen Ihre Daten, unabhängig von ihrem Speicherort: in Rechenzentren, öffentlichen Clouds und Multi-Cloud-Umgebungen. Außerdem überwachen wir kontinuierlich die Risikostufe Ihrer Endgeräte, damit Sie den Zugriff auf Daten dynamisch ändern können. Dank dieser Daten zusammen mit einer integrierten Bedrohungserkennung in Apps, Geräten und Netzwerken erhalten Sie eine umfassende Sicherheit für alle Endgeräte.

Einheitliche Analysen

Eigenständige Tools sorgen dafür, dass die Cybersicherheit unnötig komplex und ineffizient wird. Wenn ein Team mehrere Lösungen verwalten muss, ist die Wahrscheinlichkeit von Fehlern oder dass inkonsistente Sicherheitsrichtlinien übersehen werden, erhöht. In unserer integrierten Plattform erhalten Sie relevante Einblicke in Benutzer, Endgeräte, Apps und Daten.

Jedes Unternehmen unterstützt seine Mitarbeiter heutzutage mit unzähligen Apps und Cloud-Plattformen, von Produktivitätssuites wie Microsoft 365 oder Google Workspace bis hin zu CRM-Lösungen wie Salesforce oder HR-Apps wie Workday. Mit einer zentralen Plattform können Sie konsistente Sicherheitsrichtlinien implementieren und so die komplette Kontrolle behalten. Wir bieten Ihnen Einblicke in alle Aktivitäten aller Cloud-Apps und -Plattformen, sodass Sie ungewöhnliches oder bösartiges Verhalten bzw. Schwachstellen identifizieren können. Dazu können böswillige Drittanbieterintegrationen oder im App-Code verborgene Bibliotheken gehören. Wir wissen auch, wie Ihre Daten verarbeitet, gespeichert und übertragen werden, und ermöglichen so einen dynamischen Schutz.

Außerdem stellen wir Ihnen alle erforderlichen Telemetriedaten zum Aufspüren von Bedrohungen und Durchführen forensischer Untersuchungen komplexer Cyberangriffe bereit. Sie erhalten sofortige Warnungen bei relevanten Problemen. Dabei können Administratoren Benachrichtigungen über ungewöhnliche Ereignisse und verdächtige Aktivitäten anpassen. Mit aggregierten Berichten erhalten Sie umfangreiche Audit-Logs für alle Geräte, Netzwerkverbindungen und Cloud-Services, damit Sie genau feststellen können, wo und wie ein Vorfall stattgefunden hat.

Präzise Kontrollen für dynamischen sicheren Zugriff und Zusammenarbeit

Ihre Mitarbeiter möchten jederzeit von überall aus arbeiten können. Daher birgt der „Alles oder Nichts"-Zugriff auf Unternehmensdaten in der Cloud oder vor Ort unnötige Risiken. Zum Schutz Ihrer Daten müssen Sie jede Interaktion mit Benutzern, Endgeräten und Apps sichern. Wenn Sie über komplette Transparenz, einheitliche Analysen und integrierte einheitliche Kontrollen verfügen, können Sie einen präzisen Zugriff für eine nahtlose und effiziente Verbindung und Zusammenarbeit ins Leben rufen.

Wir bieten eine detaillierte und dynamische Zugriffskontrolle, entsprechend der Risikostufe jedes Benutzers. Dabei wird z. B. beurteilt, ob Malware auf dem Gerät installiert ist oder ob der Benutzer auf sensible Daten zugreift, die nicht mit seiner Rolle im Zusammenhang stehen. Wir wissen, welche Apps und Daten Ihre Mitarbeiter für die Arbeit brauchen. Daher können Mitarbeiter sicher und dynamisch auf die Ressourcen zugreifen, die sie benötigen – in Unternehmensanwendungen innerhalb des Perimeters, in privaten Clouds und in Cloud-Anwendungen.

Sicherheitsfunktionen dürfen auch nicht die Produktivität oder Benutzerfreundlichkeit beeinträchtigen. Wir kennen Ihre Daten ganz genau und können einen nahtlosen Datenschutz auf das ganze Unternehmen erweitern, ohne dass Workflows unterbrochen werden. Außerdem bieten wir eine Datenverschlüsselung im Ruhezustand, bei der Übertragung und bei der Verwendung. So können Sie die höchsten Sicherheitsanforderungen erfüllen und gleichzeitig Online- und Offlinezugriff für Benutzer gewähren. Wir können sogar sensible Daten beim Herunterladen verschlüsseln und ein Digital Rights Management durchsetzen, das einen unautorisierten Zugriff verhindert.

Überall mit Sicherheit arbeiten – vom Endgerät bis in die Cloud

Der digitalen Zusammenarbeit sind keine Grenzen mehr gesetzt und Daten sind nun überall dort abrufbar, wo sie benötigt werden. Um von dieser Produktivitätssteigerung zu profitieren, ohne Daten einem Risiko auszusetzen, müssen Sie jedes Endgerät, jedes Netzwerk und jede Anwendungsverbindung sichern. Lookout integriert die Endgerätesicherheit in SASE, damit Sie Daten vom Endgerät bis hin in die Cloud schützen können und dabei die Privatsphäre der Anwender respektieren.

Über Lookout

Lookout ist ein Anbieter von integrierten Sicherheitslösungen vom Endgerät bis hin zur Cloud. In einer Welt, in der Datenschutz höchste Priorität hat und Mobilität und Cloud bei der Arbeit und in der Freizeit unverzichtbar geworden sind, haben wir es uns zur Aufgabe gemacht, Sie sicher in die digitale Zukunft zu führen. Wir geben Verbrauchern und Mitarbeitern die Möglichkeit, ihre Daten zu schützen und sicher miteinander in Verbindung zu bleiben, ohne ihre Privatsphäre oder ihr Vertrauen zu verletzen. Lookout wird von Millionen Anwendern, den größten Unternehmen und Behörden sowie Partnern wie AT&T, Verizon, Vodafone, Microsoft, Google und Apple genutzt. Lookout hat seinen Hauptsitz in San Francisco und verfügt über Niederlassungen in Amsterdam, Boston, London, Sydney, Tokio, Toronto und Washington, DC. Weitere Informationen finden Sie unter **www.lookout.com/de**. Folgen Sie Lookout auf seinem **Blog**, **LinkedIn** und **Twitter.**

Weitere Informationen finden Sie auf
lookout.com/de

Fordern Sie eine Demo an unter
https://www.lookout.com/de/info/de-enterprise-contact-us

Integrierte Sicherheit von Endgerät zu Cloud

Weitere Informationen finden Sie unter **lookout.com/de**

Lookout®