Zero Trust Network Access

Vereinfachte Sicherheit für private Anwendungen ohne eine VPN

Anwendungsfälle

- Ersetzen von VPNs für den Zugriff auf private Anwendungen in Rechenzentren und privaten Clouds
- Bereitstellen eines sicheren, agentenlosen Zugriffs auf private Webanwendungen von BYOD- und nicht verwalteten Geräten aus
- Kontrolle des Uploads und Downloads sensibler Daten in jede private Webanwendung
- Abwehr versteckter Malware in geschäftlichen Datendateien, die in oder aus privaten Webanwendungen übertragen werden
- Schutz des Zugriffs auf private Nicht-Webserver von verwalteten Windows- und macOS-Geräten aus

Lösung

- Schutz privater Anwendungen mit Integration in erweiterten Bedrohungsschutz und DLP
- Agentenlose Zero-Trust-Zugriffskontrollen für private Webanwendungen von BYOD- und nicht verwalteten Geräten aus
- Remote-Zugriff auf private Nicht-Webanwendungen von verwalteten Windows- und macOS-Geräten aus
- Bestandteil eines umfassenden, in der Cloud bereitgestellten Dienstes mit SWG, CASB und anderen modernen Sicherheitsfunktionen

Ergebnis

- Höhere Produktivität durch nahtlosen und sicheren Benutzerzugriff auf private Anwendungen von jedem Standort aus
- Niedrigere Kosten durch vereinfachte Sicherheitsmaßnahmen, indem Richtlinien zentral festgelegt werden
- Verringertes Risiko durch Prüfung auf Malware und Kontrolle sensibler Daten, die in und aus privaten Webanwendungen übertragen werden
- Optimierte Compliance mit nachweisbaren Prozessen zur Kontrolle von Informationen

Remote-Arbeitsmodelle haben gezeigt, welche Beschränkungen, Kosten und Risiken Virtual Private Networks (VPNs) mit sich bringen. Wenn Benutzer mit einem VPN verbunden sind, genießen sie ein übermäßiges implizites Vertrauen und können andere IP-Adressen im jeweiligen privaten Rechenzentrum oder in der virtuellen privaten Cloud aufrufen. Sicherheitsverletzungen werden dadurch Tür und Tor geöffnet. Der Wechsel von einem VPN zu einer Zero Trust Network Access (ZTNA)-Lösung sollte jedoch nicht mit noch mehr Komplikationen und weiteren Einzelprodukten verbunden sein. Die Bereitstellung von Zero-Trust-Zugriff muss einfach und unproblematisch sein.

ZTNA von Forcepoint kontrolliert den Zugriff auf private Web- und Nicht-Webanwendungen, für die jeder Mitarbeiter, Auftragnehmer und Partner eine explizite Nutzungsberechtigung hat. Mit Forcepoint ZTNA haben Sie eine wesentlich bessere Kontrolle und somit können Sie Benutzern bedenkenlos die Verwendung ihre bevorzugten Geräte erlauben, selbst nicht verwaltete Geräte und BYOD-Geräte sind kein Problem.

Im Gegensatz zu anderen Lösungen bietet Forcepoint ZTNA kontinuierliche, detaillierte Kontrollmöglichkeiten, eine branchenführende Leistung und einen integrierten Schutz vor Malware und Datenschutz. Trotz der Komplexität moderner Netzwerke bietet ZTNA ein hervorragendes Benutzererlebnis. Bei Bedarf können Sie auch zusätzlich andere Sicherheitslösungen bereitstellen, wie Cloud Access Security Broker (CASB) und Secure Web Gateway (SWG), die vollständig in die Cloud-Plattform Forcepoint ONE integriert werden können.

Ersetzen von VPNs für den Zugriff auf private Anwendungen in Rechenzentren und privaten Clouds
Für den sicheren Zugriff auf private Anwendungen ist eine schnelle, genaue Kontrolle unerlässlich. Sie können den Zugriff auf private Anwendungen wie ERP- oder Lieferkettenserver basierend auf Identität, Gruppenmitgliedschaft, Gerätetyp und Standort beschränken. Bei Nicht-Webanwendungen können Sie Kontrollen individuell pro Port anwenden und den Zugriff von unbekannten Standorten oder Geräten aus schützen. Wenn der Anmeldeversuch verdächtig erscheint, müssen Benutzer ihre Identität über die mehrstufige Authentifizierung nachweisen. All das dauert bei der Hyperscale-Plattform von Forcepoint nur Millisekunden.

Bereitstellen eines sicheren, agentenlosen Zugriffs auf private Webanwendungen von BYOD-Geräten aus
Benutzer können sich sicher und bequem über das Internet mit Webanwendungen verbinden, die hinter einer Firewall gehostet werden, sogar mit BYOD- und nicht verwalteten Geräten. Agenten sind dafür nicht erforderlich.

Kontrolle des Uploads und Downloads sensibler Daten in jede private Webanwendung
Sie müssen nur einen Satz von Sicherheitsrichtlinien verwalten, um sensible Daten zu kontrollieren. Dank integrierten Malware-Scans und DLP haben Hacker und Sicherheitsverletzungen keine Chance. Durch das Zusammenspiel aus Datensicherheit und Richtlinien für Gerätestatus und Standort können Sie einfacher steuern, wie Benutzer Daten von und in private Webanwendungen übertragen, und das für jedes Gerät.

Abwehr versteckter Malware in geschäftlichen Datendateien, die in oder aus privaten Webanwendungen übertragen werden
Forcepoint bremst Ransomware aus. Mithilfe der Scanning-Engines Bitdefender und CrowdStrike können Sie Malware in Daten während der Übertragung zwischen Benutzern und jeder privaten Webanwendung erkennen und blockieren.

Schutz des Zugriffs auf private Nicht-Webserver von verwalteten Geräten aus

ZTNA von Forcepoint ermöglicht den Zugriff auf private Nicht-Webanwendungen wie Secure Shell (SSH) und Remote Desktop von verwalteten PCs und Mac-Computern aus mithilfe des einheitlichen Agenten von Forcepoint ONE.

ZTNA in Forcepoint ONE maximiert Betriebszeit, Verfügbarkeit und Produktivität

Unsere ZTNA-Lösung ist Teil von Forcepoint ONE, unserer Hyperscaler-basierten Cloud-Plattform mit 300 Points-of-Presence (PoPs), globalem Zugriff und einer nachgewiesenen Betriebszeit von 99,99 %, um private Anwendungen nahtlos zu schützen und die Benutzerproduktivität aufrechtzuerhalten. Bei anderen Lösungen wird der Netzwerkverkehr über private Rechenzentren umgeleitet anstatt über Ziele in Benutzernähe. Dies kann die Leistung stark beeinträchtigen. Forcepoint ONE vereint CASB, SWG und ZTNA, um den Zugriff auf unternehmenseigene SaaS-, Web- und private Anwendungen zu schützen – Sicherheit leicht gemacht.

Vereinfachen der Sicherheit für private Anwendungen in der Praxis

Mit der Forcepoint ONE Cloud-Plattform ist die Implementierung von Sicherheit für private Anwendungen denkbar einfach. Administratoren können den Zugriff von einer einzigen Konsole aus verwalten und Datei-Downloads und -Uploads für Benutzer von verwalteten und nicht verwalteten Geräten (wie BYOD-Geräten und Computern von Auftragnehmern und Partnern) kontrollieren.

Absolute Cloud-Sicherheit bei jeder Interaktion

Sehen wir uns am Beispiel von Kris an, wie ZTNA-Funktionen die Sicherheit für private Anwendungen vereinfacht. Kris ist Einkaufsleiter, arbeitet von zu Hause aus und beginnt gerade seinen Arbeitstag.

Kris meldet sich auf seinem firmeneigenen Laptop bei seinem Forcepoint ONE-Konto an.	Da Kris sich von einem verwalteten Gerät und einem zugelassenen Standort aus anmeldet, wird ihm der Zugriff gewährt. Die Anmeldung von einem unbekannten Standort aus erfordert eine mehrstufige Authentifizierung.
Kris kann über das Forcepoint ONE-Benutzerportal mit nur einem Mausklick auf die proprietäre Lieferkettenanwendung des Unternehmens zugreifen.	Im Browser von Kris wird das Forcepoint ONE-Portal mit Kacheln für jede Webanwendung angezeigt, auf die Kris und die Lieferkettenpartner Zugriff haben. (Wenn das Unternehmen von Kris Forcepoint ONE CASB verwendet, kann Kris über dasselbe Benutzerportal auf verwaltete SaaS-Anwendungen zugreifen, wodurch ein einheitliches Benutzererlebnis gewährleistet ist.)
Kris wird der Zugriff auf die verwaltete Anwendung gewährt.	Der Datenverkehr zwischen dem Laptop von Kris und der Lieferkettenanwendung wird automatisch durch den Reverse-Proxy von Forcepoint ONE geleitet. Forcepoint überprüft Datei-Uploads und -Downloads auf Malware und sensible Daten.
Kris lädt einen Lieferantenvertrag als Anhang hoch.	In der Richtlinie für die Verbindung von Kris ist festgelegt, dass Dateien überprüft werden. Der Upload wird erlaubt, wenn die Datei keine Malware enthält. Wenn sie infiziert ist, blockiert der ZTNA-Gateway den Upload, informiert Kris und protokolliert und meldet das Blockierungsereignis.
Kris lädt einen Lieferantenvertrag als Anhang hoch.	In der Richtlinie für die Verbindung von Kris ist festgelegt, dass Dateien überprüft werden. Der Upload wird erlaubt, wenn die Datei keine Malware enthält. Wenn sie infiziert ist, blockiert der ZTNA-Gateway den Upload, informiert Kris und protokolliert und meldet das Blockierungsereignis.

Teil einer einheitlichen Sicherheitslösung für Web-, Cloud- und private Anwendungen

Neben ZTNA schützt die allumfassende Plattform Forcepoint ONE den Zugriff auf Unternehmensinformationen von jeder Website und privaten Anwendung aus:

- → **Web:** SWG überwacht und kontrolliert Interaktionen mit Websites basierend auf Risiko und Kategorie und blockiert das Herunterladen von Schadsoftware und Hochladen sensibler Daten in private File-Sharing- und E-Mail-Konten. Unser geräteinternes SWG setzt Richtlinien für angemessene Nutzung auf verwalteten Geräten an beliebigen Standorten durch.
- → **Cloud:** CASB schützt und erleichtert den Zugriff auf SaaS- und IaaS-Mandanten im Unternehmen und kontrolliert die Übertragung von sensiblen Daten und Malware, ohne dass ein geräteinterner Agent erforderlich ist.
- → **Zusätzliche Funktionen** wie RBI oder die Überprüfung von Cloud-Anbietern auf problematische Konfigurationen (CSPM) sind bei Bedarf verfügbar.

Weitere Informationen erhalten Sie im Lösungsüberblick von Forcepoint ONE.

Möchten Sie Daten in Cloud-Apps von jedem Gerät aus schützen?

Lassen Sie uns mit einer Demo beginnen.

forcepoint.com/contact