

# Zero Trust, umfassende Sicherheit und Schutz vor Datenabfluss direkt im Browser

Der Prisma Access Browser von Palo Alto Networks löst Sicherheitsprobleme hybrider Arbeitsumgebungen auf elegante, kosteneffiziente Art und schützt bei der Nutzung von Webapplikationen wirksam vor Cyberangriffen und Datenabfluss.

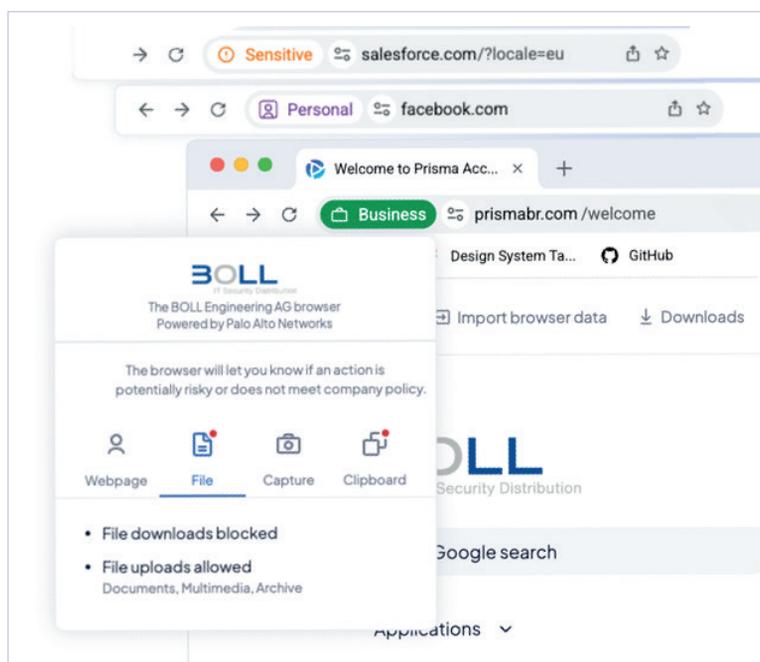
Hybride Arbeitsmodelle, Bring Your Own Device (BYOD), externe Dienstleister und Partner – in der digitalen Welt von heute können sich Cybersicherheitsmassnahmen nicht mehr auf das Firmennetzwerk selbst beschränken. Hinzu kommt, dass ein Grossteil der benötigten Software mehrheitlich in Form von Webapps via Browser genutzt wird. Konventionelle Webbrowser sind jedoch nur mangelhaft auf Sicherheit ausgelegt. Ausser der SSL-Verschlüsselung zwischen Browser und Webserver verfügen sie über wenig Sicherheitsfeatures. Demgegenüber erfolgen vier Fünftel aller Data Breaches über Webapplikationen und E-Mail, wie Studien zeigen.

## Traditionelle Absicherung teuer und kompliziert

Um mehr Sicherheit in hybride Nutzungsszenarien und die Anwendung von Webapplikationen zu bringen, bediente man sich bisher kostspieliger und komplexer Lösungen, darunter die Abgabe gemanagter Laptops an eigene Mitarbeitende und Contractors wie etwa externe Dienstleister oder Servicetechniker. Eine weitere Möglichkeit waren umfangreiche VDI-Infrastrukturen (Virtual Desktop Infrastructure), die hohe Kosten und einen ebenso hohen Verwaltungsaufwand mit sich bringen. Diesen Lösungen ist zudem gemeinsam, dass sie nicht das beste Nutzererlebnis bieten.

## Ein sicherer Browser für alle Fälle

Mit dem Prisma Access Browser hält Palo Alto Networks eine kosteneffiziente, benutzerfreundliche und durch und durch sichere Alternative zu den konventionel-



len Sicherheitsoptionen bereit. Der Prisma Access Browser ist Teil der SASE-Plattform des Cybersicherheitsanbieters, kann aber auch separat bezogen und eingesetzt werden.

Der Browser basiert auf der Chromium-Engine und sichert sowohl gemanagte als auch nicht gemanagte Geräte ab. Auf dieser Basis ermöglicht er sichere Zugänge für externe Dienstleister und den flexiblen Einsatz eigener Geräte durch die Mitarbeitenden nach dem BYOD-Modell. Vor allem aber bietet die Lösung umfassenden Schutz bei der Nutzung von Webapplikationen, indem sie Zero Trust Network Access (ZTNA) direkt in den Browser integriert und damit eine fein granulierte, identitätsbasierte und laufend aktualisierte Zugriffs-

kontrolle durch Continuous Trust Verification gewährleistet.

Dazu kommen weitere Sicherheitsfeatures wie integrierter Schutz vor Keyloggern und manipulierten Gerätezertifikaten sowie volle Kontrolle über die installierten Browsererweiterungen, über verwundbare Komponenten des Browsers sowie nicht vertrauenswürdige Websites. Mit all diesen Massnahmen macht der Prisma Access Browser jedes Gerät nativ zu einem sicheren Arbeitsinstrument.

## Schutz vor Datenabfluss inklusive

Darüber hinaus bietet die Lösung browserbasierten Schutz vor Datenabfluss (Data Loss Prevention) und löst damit eines der gerade bei der Nutzung von

Webapplikationen meistgefürchteten Cybersecurity-Probleme direkt an der Quelle – Schluss mit Datenklau! Sensible Daten werden aufgrund von Inhalt und Kontext dynamisch maskiert, der Abgriff von Screenshots, Copy-and-Paste-Operationen und Drucken je nach Vorgabe des Unternehmens verhindert. Des Weiteren lässt sich der Upload von Dateien auf persönliche Cloud-Speicher und lokal angeschlossene Datenträger unterbinden. Auch Sicherheitsmassnahmen zum Schutz vor Spoofing sind mit an Bord. Und eine zusätzliche, vom Betriebssystem unabhängige Verschlüsselungsschicht schützt sämtliche Assets des Browsers.

Untersuchungen von Palo Alto Networks zeigen zudem erhebliche Möglichkeiten zur Kostenoptimierung. Im Vergleich zur Ausgabe gemanagter Laptops an Mitarbeitende und Dritte lassen sich demnach bis zu 85 Prozent an Kosten sparen. Gegenüber Installation und Betrieb einer VDI-Infrastruktur hilft der Prisma Access Browser, die Gesamtkosten (TCO) um bis zu 79 Prozent zu senken – dies alles verbunden mit der Tatsache, dass praktisch 100 Prozent der mit dem Browser ausgestatteten Geräte umfassend geschützt sind.

**BOLL**  
IT Security Distribution

**BOLL Engineering AG**

Jurastrasse 58 | 5430 Wettingen  
056 437 60 60 | info@boll.ch | boll.ch