Prisma Access Browser

Der Browser ist der Ort, an dem die Arbeit stattfindet. Die Abhängigkeit vom Browser für den Zugriff auf geschäftskritische Anwendungen, in Kombination mit der Zunahme von hybridem Arbeiten, mobilem Arbeiten, BYOD und unabhängigen Mitarbeitern, stellt ein erhebliches Sicherheitsrisiko dar. Schützen Sie den browserbasierten Arbeitsbereich mit Prisma® Access Browser und bieten Sie sicheren Zugriff auf Web-, SaaS-, GenAI- und private Anwendungen auf jedem Gerät, ob verwaltet oder nicht verwaltet.

Die unbequeme Wahrheit über Unternehmenssicherheit

Im heutigen digitalen Zeitalter liegt die primäre Sicherheitsherausforderung nicht mehr im Unternehmensnetzwerk selbst, sondern in den nicht verwalteten Geräten, die von der hybrid arbeitenden Belegschaft genutzt werden. Diese Geräte, ob sie nun Auftragnehmern gehören oder Teil einer BYOD-Richtlinie (Bring Your Own Device) für Mitarbeiter sind, stellen ein erhebliches Risiko beim Zugriff auf SaaS- und sensible, geschäftskritische Anwendungen dar. Tatsächlich erfolgen 80 % der Datenschutzverletzungen über Webanwendungen und E-Mails,[1] auf die in erster Linie über anfällige private Webbrowser zugegriffen wird. Zudem gibt die große Mehrheit der Unternehmen an, dass mehr als die Hälfte der mobilen Mitarbeiter über nicht verwaltete Geräte auf Unternehmensanwendungen zugreifen.[2]

Herkömmliche Lösungen wie die Auslieferung von verwalteten Laptops und große VDI-Implementierungen sind kostspielig in der Implementierung, schwierig zu verwalten und bieten den Mitarbeitern oft eine schlechte Benutzererfahrung. Die Cyber-Bedrohungen, mit denen viele Unternehmen konfrontiert sind, erfordern eine Lösung, die es ermöglicht, die moderne, verteilt arbeitende Belegschaft zu schützen, ohne die Produktivität zu beeinträchtigen.

Was wäre, wenn eine Sicherheitslösung Ihr Unternehmen unterstützen würde, anstatt es einzuschränken?

Wir stellen vor: Prisma Access Browser

Palo Alto Networks bietet Ihnen eine branchenweit einzigartige SASE-Lösung, die mit einem nativ integrierten, sicheren Browser eine sichere Arbeitsumgebung für verwaltete und nicht verwaltete Geräte schafft. Benutzer profitieren nun auf allen Geräten von einem konsistenten, reibungslosen Zero-Trust-Zugriff auf SaaS- und private Anwendungen.

Prisma Access Browser sichert sowohl verwaltete als auch nicht verwaltete Geräte und wird den sich wandelnden Sicherheitsanforderungen moderner Organisationen und ihrer hybriden Belegschaften gerecht. Durch die Ausweitung der Schutzreichweite von SASE auf jedes beliebige Gerät in Minutenschnelle schützt Prisma Access Browser Geschäftsanwendungen und -daten vor einem breiten Spektrum von Bedrohungen.

Einzigartige, reibungslose Sicherheit

- **Agilität**: Schützen Sie jedes Gerät in Minutenschnelle mit Prisma SASE, der einzigartigen SASE-Lösung mit einem integrierten, sicheren Browser. Diese Funktion gewährleistet umfassenden Schutz für Unternehmensanwendungen und -daten auf allen Geräten.
- **Zuverlässigkeit**: Schützen Sie sich zuverlässig mit Prisma SASE, der einzigen Plattform mit integrierter KI, um Bedrohungen im Handumdrehen in allen Browsern und Anwendungen abzuwehren. Die Lösung erkennt täglich über 1,5 Millionen Angriffe unterschiedlichster Art und bietet damit ein unübertroffenes Maß an Sicherheit.
- **Effizienz**: Erleben Sie unübertroffene Effizienz mit Prisma SASE, der einzigen Plattform, die eine zentrale Verwaltung für alle Geräte bietet. Mit vereinfachten Prozessen, verringertem Aufwand und automatisierten IT-Aufgaben wird Ihre digitale Umgebung durchgängig gesichert.

1. *Data Breach Investigations Report 2023*, Verizon, 6. Juni 2023.
2. „Stimmungsumfrage: Bedenken und Anforderungen zur Netzwerksicherheit angesichts der dauerhaften Homeoffice-Realität“ (unveröffentlichte Studie), ESG, August 2022.

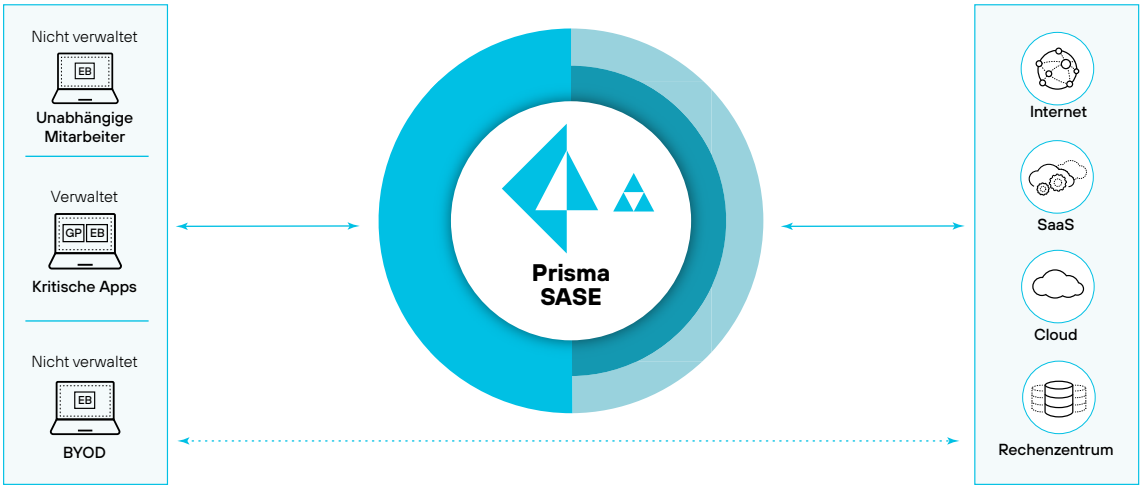

Abbildung 1. SASE erstreckt sich mit Prisma Access Browser auf alle Geräte

Anwendungsszenarien

Prisma Access Browser unterstützt eine Vielzahl von Szenarien, von der Sicherung des Zugriffs von Auftragnehmern und Dritten über die Ermöglichung von BYOD für Mitarbeiter bis hin zur Bereitstellung eines sicheren Zugriffs auf kritische Webanwendungen für all diese verschiedenen Mitarbeiter.

Sicherung des Zugriffs von Dritten und Auftragnehmern

Prisma Access Browser bietet Auftragnehmern Sicherheit auf Unternehmensniveau und ermöglicht die Kontrolle und Transparenz externer Interaktionen mit Anwendungen und Daten. Die Ausweitung der umfassenden Sicherheitskontrollen von SASE auf nicht verwaltete Geräte über den Browser gewährleistet nicht nur die Einhaltung der Sicherheitsrichtlinien des Unternehmens, sondern reduziert auch die Kosten und Komplexität der Bereitstellung herkömmlicher Lösungen. Dieser Ansatz bietet zuverlässigen Schutz für sensible Daten und Ressourcen und ermöglicht eine nahtlose Zusammenarbeit mit externen Partnern bei gleichzeitiger Einhaltung strenger Sicherheitsstandards.

BYOD für Mitarbeiter

Mit Prisma Access Browser können Mitarbeiter mühelos von persönlichen Geräten aus auf Unternehmensanwendungen zugreifen, ohne ihr Unternehmen einem Risiko auszusetzen. Durch die Nutzung der Leistungsfähigkeit von SASE wird sichergestellt, dass jedes persönliche Gerät in einem sicheren, konformen Rahmen betrieben wird. Dies ermöglicht die Flexibilität von BYOD, jedoch mit kompromissloser Sicherheit. Dieser innovative Ansatz macht herkömmliche Geräteverwaltungslösungen überflüssig und schafft ein ideales Gleichgewicht zwischen Benutzerfreiheit und Gerätewahl, ohne die Sicherheit des Unternehmens zu beeinträchtigen.

> „Bis 2030 werden Browser die Kernplattform für die Mitarbeiterproduktivität und die Bereitstellung von Sicherheitssoftware auf verwalteten und nicht verwalteten Geräten sein – für eine nahtlose hybride Arbeitserfahrung.“[3]
>
> – Gartner

Sicherer Zugriff auf kritische Webanwendungen

In einer Umgebung, in der sensible Webanwendungen für den Geschäftsbetrieb von zentraler Bedeutung sind, schützt Prisma Access Browser diese Anwendungen vor webbasierten und internen Angriffen sowie vor infiltrierten Endpunkten auf allen Geräten. Durch die Einbettung der starken Sicherheitsfunktionen von SASE direkt in das Browsing-Erlebnis können Unternehmen ihre Betriebsprozesse optimieren und eine hohe Produktivität aufrechterhalten, indem sie ihre Daten bei kritischen Anwendungen auf allen Geräten zuverlässig schützen.

3. Dan Ayoub et al., *Emerging Tech: Security — The Future of Enterprise Browsers*, Gartner, 14. April 2023.

Die wichtigsten Vorteile

Um die messbaren Vorteile von Prisma Access Browser zu demonstrieren, haben wir eine interne Analyse mittels einer unabhängigen Prüfung durch Dritte durchgeführt, die folgende Erkenntnisse aufdeckte:

- **85 % günstiger als die Bereitstellung von Laptops**: Sie müssen keine Unternehmenslaptops für mobile Mitarbeiter und Auftragnehmer bereitstellen, da diese dieselbe Funktionalität sicher und kosteneffizient in Prisma Access Browser nutzen können.
- **79 % niedrigere Gesamtbetriebskosten als VDI**: Dank seiner effizienten, cloudnativen Architektur und Benutzerfreundlichkeit punktet Prisma Access Browser mit deutlich günstigeren Gesamtbetriebskosten als herkömmliche VDI-Lösungen.
- **Schutz von bis zu 100 % der Geräte**: Eine umfassende Abdeckung aller verwalteten und nicht verwalteten Geräte schließt Lücken in vorhandenen Sicherheitsprogrammen. Prisma Access Browser bietet starke Sicherheitsmaßnahmen für alle Endpunkte und schützt Unternehmensdaten zuverlässig – unabhängig von der Herkunft des Geräts und dem Standort des Benutzers.

Für die Kundenpräsentation mit Berechnungen und Anwendungsszenarien wenden Sie sich bitte an einen Vertriebsmitarbeiter von Palo Alto Networks.

Innovative Sicherheitsfunktionen von Prisma Access Browser

Zero Trust auch für den Browser

Prisma Access Browser umfasst Zero Trust Network Access (ZTNA) – das heißt, im Unterschied zu herkömmlichen Sicherheitsansätzen wird kein Benutzer oder Gerät als von Haus aus vertrauenswürdig angesehen. Diese ZTNA 2.0-Funktionalität erlaubt eine granulare, identitätsbasierte Zugriffskontrolle direkt im Browser, um die Sicherheit zu erhöhen und das Risiko durch Bedrohungen zu minimieren.

Tabelle 1. Zero Trust – Prisma Access Browser vs. private Browser

Privater Browser	Prisma Access Browser
Keine Kontrolle der Gerätesicherheit, wodurch das Risiko besteht, dass infiltrierte Geräte Zugriff auf sensible Informationen erhalten.	Erzwingung strenger Geräteprüfungen, bevor der Zugriff gewährt wird, und Nutzung der kontinuierlichen Prüfung der Vertrauenswürdigkeit und Sicherheit, um die Einhaltung von Vorschriften zu gewährleisten und Risiken zu minimieren.
Keine Bestätigung der Benutzeridentität für Aktionen, sodass die Anfälligkeit für identitätsbasierte Angriffe steigt.	Integration von Just-in-Time-MFA für zusätzlichen Schutz bei extrem sensiblen Aktionen.

Prisma Access Browser nutzt die kontinuierliche Prüfung der Vertrauenswürdigkeit von Prisma Access für detaillierten Least-Privilege-Zugriff sowie tiefgreifende und fortlaufende Sicherheitsprüfungen. Darüber hinaus wird mit der kontinuierlichen Sicherheitsprüfung von Prisma Access ein umfassendes Spektrum an Sicherheitsservices bereitgestellt, z. B. Advanced Threat Prevention, Advanced URL Filtering, DNS Security und Sandboxing.

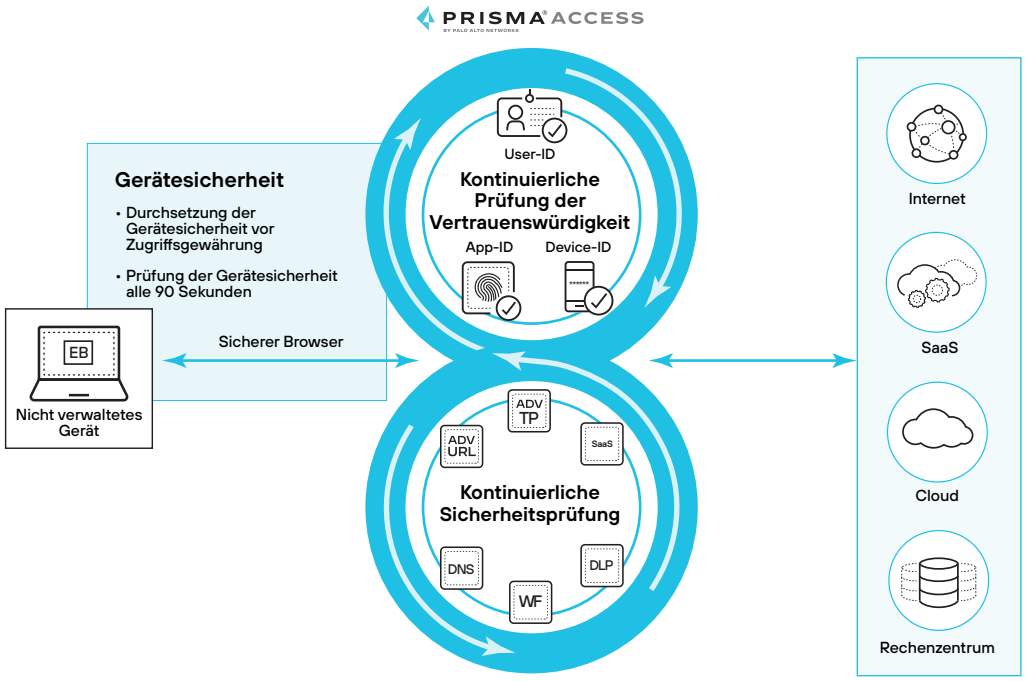

Abbildung 2. Prisma Access Browser ermöglicht die kontinuierliche Prüfung der Vertrauenswürdigkeit und Sicherheit von nicht verwalteten Geräten

Sichere Arbeitsumgebung auf jedem Gerät

Durch den umfassenden Schutz von Browserassets, -laufzeit und -angriffsflächen gegen Schwachstellen und Angriffe schafft Prisma Access Browser eine sichere Umgebung für webbasierte Aktivitäten. Damit werden alle Onlineaktivitäten und Daten im Browser vor webbasierten Bedrohungen und Bedrohungen durch infiltrierte Endpunkte geschützt.

Tabelle 2. Sichere Arbeitsumgebung – Prisma Access Browser vs. private Browser

Privater Browser	Prisma Access Browser
Browserassets	
Nicht alle Browserassets sind verschlüsselt und die verschlüsselten lassen sich einfach umgehen.	Eine zusätzliche Verschlüsselungsebene schützt alle Browserassets mit einer vertrauenswürdigen, vom Betriebssystem unabhängigen Verschlüsselungskette.
Angreifer können das Betriebssystem spoofen, um Browserassets zu entschlüsseln.	Spezielle Sicherheitsmechanismen wirken Spoofing-Versuchen entgegen, um unbefugten Zugriff auf verschlüsselte Browserassets zu verhindern.
Browserlaufzeit	
Fehlender Schutz vor Endpunktmalware, die auf den Browser abzielt.	Integrierter Schutz vor Keyloggern und Abwehrmaßnahmen gegen Screen Scraper.
Keine Möglichkeit, Risiken aufgrund einer Insidermanipulation des Browserspeichers zu minimieren.	Kontrollmaßnahmen zum Schutz des Browserspeichers vor Manipulation, um die Laufzeitintegrität zu wahren.
Zu große Abhängigkeit vom Endpunktzertifikatsspeicher, sodass der Browser anfällig für zertifikatsbasierte Angriffe ist.	Erhöhte Sicherheit durch den Schutz vor der Manipulation von Gerätezertifikaten und weniger Abhängigkeit vom Zertifikatsspeicher des Endpunkts.
Browserangriffsfläche	
Komponenten sind anfällig für Schwachstellen.	Deaktivierung oder Kontrolle von anfälligen Browserkomponenten auf nicht vertrauenswürdigen Websites möglich, um die Gefährdung durch gängige Sicherheitslücken zu minimieren.
Nur minimale Sicherheitskontrollen zum Schutz vor schädlichen Erweiterungen.	Vollständige Kontrolle über installierte Erweiterungen und deren Berechtigungen. Erweiterungen, die auf sensible Informationen zugreifen könnten, werden streng verwaltet und kontrolliert.

Schützen Sie sensible Daten direkt dort, wo auf sie zugegriffen wird

Prisma Access Browser integriert browserbasierte Data Loss Prevention zum Schutz sensibler Informationen innerhalb der Browserumgebung. Diese Funktion verhindert proaktiv die unbefugte gemeinsame Nutzung, Übertragung oder Weitergabe sensibler Daten und entspricht damit den Compliance-Anforderungen und den Datenrichtlinien des Unternehmens.

Tabelle 3. Datenschutz – Prisma Access Browser vs. private Browser

Privater Browser	Prisma Access Browser
Keine Möglichkeit zur Maskierung sensibler Daten.	Tarnung sensibler Daten auf dynamische Weise – basierend auf Inhalt und Kontext – und Sicherstellung, dass vertrauliche Informationen geschützt werden.
Anfällig für Datenausschleusung durch Screenshots, gemeinsame Nutzung, Copy/Paste und Drucken.	Kein Erstellen von Screenshots, Freigeben über Zusammenarbeitstools, Kopieren/Einfügen sowie Drucken mit konfigurierbaren Firmenwasserzeichen auf sensiblen Bildschirmen, um eine unbefugte Erfassung zu verhindern.
Nur minimale Kontrolle über Dateiübertragungen und damit möglicherweise unbefugte Datentransfers.	Steuerung von Dateiübertragungen durch Verschlüsselung von Downloads aus Unternehmensanwendungen und Blockierung von Uploads auf private Laufwerke. Einschränkung von Download/Upload von Dateien abhängig von Inhalt und Quelle und Sicherstellung, dass Dateien nur innerhalb genehmigter Kanäle übertragen werden.

Prisma Access Browser ermöglicht detaillierte(n) Verschlüsselung und Dateizugriff basierend auf Benutzer, Anwendung und Dateityp. Dadurch können sensible Daten einfach geschützt und das Risiko eines unbefugten Zugriffs und Datenverlusts minimiert werden.

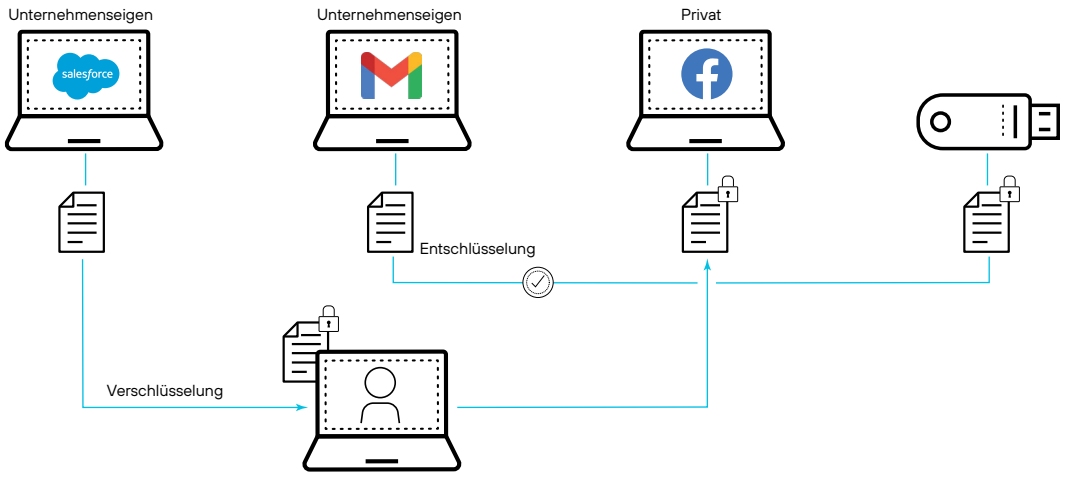

Abbildung 3. Schutz sensibler Daten durch benutzer-, anwendungs- und zielabhängigen Dateizugriff

Sonderaktionen für Prisma Access Browser

Bestandskunden mit Prisma Access Enterprise Mobile User (Stand 31. Januar 2024) bieten wir beim Kauf von Professional Services für die Implementierung ein kostenloses Upgrade auf den sicheren Browser. Dieses Upgrade ist bis zu Ihrer nächsten Vertragsverlängerung oder bis zum 31. Juli 2025 erhältlich, je nachdem, was zuerst eintritt.

Über Palo Alto Networks

Palo Alto Networks ist der globale Leader für Cyber-Sicherheit, der sich zum Ziel gesetzt hat, jeden Tag sicherer zu machen als den Tag zuvor – mit branchenführenden, KI-gestützten Lösungen für Netzwerksicherheit, Cloud-Sicherheit und Sicherheitsprozesse. Unsere Technologien, die auf Precision AI® basieren, ermöglichen eine präzise Erkennung von Bedrohungen und eine schnelle Reaktion, wodurch Fehlalarme minimiert werden und die Sicherheitseffektivität erhöht wird. Unser Plattformansatz integriert verschiedene Sicherheitslösungen in eine einheitliche, skalierbare Plattform, die die Verwaltung vereinfacht und betriebliche Effizienz mit umfassendem Schutz verbindet. Weitere Informationen finden Sie unter www.paloaltonetworks.de.

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Zentrale: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de

prisma_sb_prisma-access-browser_041725