

Understanding Prisma Browser for Business: A Secure Guide for Small Business

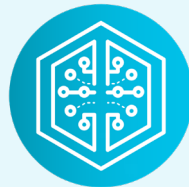
Introducing [Prisma Browser for Business](#), where enterprise-grade security is made simple for small businesses. In today's digital landscape, the browser is where most of your work happens, but it's also where your business is most vulnerable. Our solution is designed to protect your work, your data,

Key Takeaways



Proactive Defense

Stop **8.95M** unique daily attacks.



GenAI Guardrails

Prevent sensitive data leaks in tools like ChatGPT.



Zero-IT Setup

Go from "unprotected" to "secure" in **under 5 minutes**.

Frequently Asked Questions

What is Prisma Browser for Business? Prisma Browser for Business is a secure web browser designed specifically to protect small businesses. It replaces standard browsers to actively defend your team from phishing, scams, and malware while keeping sensitive data safe from accidental leaks. It provides the same best-in-class security used by the world's largest enterprises, but is built to be simple enough for businesses without a dedicated IT team.

Is it difficult for my team to adopt and use? Not at all. Prisma Browser for Business requires zero effort to set up and is ready to use out of the box with pre-configured security settings. You can onboard your entire team via email in minutes, requiring no technical expertise or complex tools like VPNs.

Why is cybersecurity so important for my small business? Small businesses are often seen as easier, more vulnerable targets by cybercriminals. In fact, small businesses can experience up to 3.5x more attacks than large enterprises, and over half of those attacked go out of business shortly after. Strong security is essential to protect your revenue, your customers, and your survival.

Why do I need to secure the browser specifically? The browser is the modern workplace, with employees spending roughly 85% of their day there. Because of this, it is a primary target—95% of security incidents originate in the browser through web-based phishing, ransomware, or malware.

What are the most common threats targeting my business? Cybercriminals use advanced strategies like fake login pop-ups, malicious tools disguised as helpful browser extensions, and malware built to bypass traditional scanners. Many of these sophisticated threats easily evade standard browser security and traditional antivirus software.

How does this protect my business data and reputation? Data is often lost when employees accidentally paste sensitive information into public GenAI tools or upload files to personal cloud storage. Prisma Browser for Business has built-in features to prevent these leaks. This is critical because 7 out of 10 consumers are likely to take their business elsewhere following a data leak.

How is this different from standard browsers like Chrome or Edge? Standard browsers prioritize personal convenience over security. Prisma Browser for Business is built to secure the entire organization. It features real-time AI-powered threat scanning and centralized management that provides visibility across your entire team.

What security engine powers this browser? Prisma Browser for Business is backed by Palo Alto Networks, the global leader in cybersecurity. It uses Cloud-Delivered Security Services (CDSS) powered by Precision AI®, which blocks over 30 billion threats daily for the world's largest companies. This shared intelligence allows us to stop new and unknown threats 180x faster than other solutions.

Can my remote employees and contractors use it safely? Yes. Prisma Browser for Business is an ideal solution for remote or hybrid teams and third-party contractors. It allows you to enforce consistent security and data protection policies on any device, anywhere, without the need for complex management.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.