

Prisma Browser for Business vs Consumer Browsers

The browser is where work happens, with 85% of a worker's day being spent in the browser. It is also vulnerable, with 95% of organizations experiencing a browser-based attack.

For small businesses, the browsers they use for work are not only vulnerable, but they are also a major target for cybercriminals. 46% of small businesses have experienced a cyber attack.

Prisma Browser for Business is built to protect small businesses from advanced cyberthreats with AI-powered protection without the IT complexity. It is also built with data protection features to prevent your sensitive data from being entered into public generative AI apps, risky websites and personal accounts.

Standard browsers and antivirus software leave major gaps when it comes to protecting your employees while they work, ranging from missing sophisticated attacks that use advanced evasion techniques to having no features that protect your data from being exposed to risky apps and sites.

Let's see how it compares to the standard browser and antivirus software you're using today.

	Prisma Browser	Consumer Browser	Antivirus Software
Core Security Engine	✔ Enterprise-Grade AI Powered by the same world-class security intelligence used by the largest global enterprises. This engine analyzes up to 3.8 billion URLs a day and prevents up to 347K new malicious URLs daily.	✘ Consumer Focus, Not Built for Work Built for speed and personal browsing, not for securing businesses that use browsers for work.	✘ Legacy Architecture Built for files on a hard drive, not for the modern web where your team actually works.
Phishing & Malicious Site Protection	✔ Spots New Threats Instantly Analyzes page content in real-time to block the newest AI-generated scams and fake login pages.	✘ Relies On Old "Bad Lists" Only checks URLs against a database of known threats. Blind to new scams created today.	✘ Not Built For The Web Relies on web extensions to inspect live websites which mainly block known malicious URLs. May leave you at risk to new and unknown phishing attacks.
Malware & Ransomware Protection	✔ Stops Threats Before They Land Analyzes files during the download to block brand-new viruses before they touch the device. Catches zero-day malware.	✘ Incomplete Protection Only stops potentially known files of certain types. Lacks the ability to scan popular file types like ZIP and PDF files that may contain malicious content.	✘ Reactive Scanning Usually scans for viruses after the malicious file is already on your computer and potentially active.
Data Protection	✔ Stop Accidental Data Leaks Prevents employees from pasting client info or uploading company files to AI sites like ChatGPT.	✘ Blind To Your Data Lets anyone copy, paste, or upload company data to any website without restriction.	✘ No Data Controls Designed to stop incoming viruses, not to stop outgoing sensitive business data.