

The Browser Risk Gap



Your most-used tool is your biggest blind spot

Your browser is the least governed yet most-used layer of IT operations. Let’s look at some telling statistics about the gaps in browser management that open your IT infrastructure to threats.

The new threat battlefield

99% of businesses run at least 1 browser-based app; the average is

87 browser-based apps

Source: [TechTarget/Omdia, October 2025](#), [Omdia/Parallels Report, March 2026](#)

55%

of organizations experienced a browser-related security incident in the last 12 months

Source: [Omdia/Parallels Report, March 2026](#)

Credential theft and phishing

Browser-based credential theft accounts for

41% of all observed browser attacks

Source: [Verizon DBIR 2026](#)

46%

of all browser attacks are due to phishing and social engineering

Source: [Verizon DBIR 2026](#)

The extension problem

54%

of organizations have installed extensions that can access cookies, passwords, and browsing data

Source: [LayerX, April 2025](#)

26%

of enterprise extensions were sideloaded, bypassing app stores entirely

Source: [LayerX/The Hacker News, November 2025](#)

Shadow AI is leaking data

67%

of users access AI services on corporate devices through personal, non-corporate accounts

Source: [Verizon 2026 DBIR](#)

77%

of employees paste data into GenAI prompts; 82% of those pastes come from personal accounts

Source: [LayerX Browser Security Report 2025 via The Hacker News](#)

The identity gap

68%

of corporate logins happen without SSO

Source: [LayerX Browser Security Report 2025 via The Hacker News](#)

43%

of SaaS logins use personal accounts, outside IT’s visibility

Source: [LayerX Browser Security Report 2025 via The Hacker News](#)

Enterprises are paying attention

85%

of organizations are increasing investments in browser security

Source: [Omdia/Parallels Report, March 2026](#)

62%

of IT/security professionals rank browser security as a top 5 security priority

Source: [Omdia/Parallels Report, March 2026](#)

The data is clear. The browser is now the primary attack surface of IT environments, yet it remains the least managed layer. Browser management changes that. Gain visibility into extensions, enforce identity policies at the point of access, and control what data is shared with AI tools, and configure every browser across your infrastructure consistently.

Learn more.