Enterprise Strategy Group

SHOWCASE

SEPTEMBER 2025

Endpoint Security Evolution: Threat Detection and Response in the Web Browser

Todd Thiemann, Principal Analyst

Abstract: The workforce web browser is where much of today's work is done. Adversaries are increasingly targeting users in the browser to steal credentials and sessions, then use that information to break into business apps and compromise the corporate environment. While protective security layers cover the network and the endpoint, they need to also address web browsers to protect against internal and external threats. However, existing solutions typically only have a vague understanding of external threat vectors that exist in the browser. Push Security brings real-time detection and response into this layer, shining a light on browser activity to counter today's threats.

The Web Browser Blind Spot

Today's web browser is integral to workforce productivity. While it originated as a way to view websites, the enterprise workforce now depends on web browsers to access nearly all work applications, analyze sensitive data, and enable secure collaboration regardless of location or device. The browser is where employees work and where attackers are increasingly focusing their malicious efforts to target them.

According to Enterprise Strategy Group research, the top reason why securing endpoints has become more difficult in the past two years is that the threat landscape has become more complex.[1] Enterprises have deployed a variety of endpoint security tools because of the recognition that the endpoint is a large portion of the enterprise attack surface and provides a reliable control point (see Figure 1).

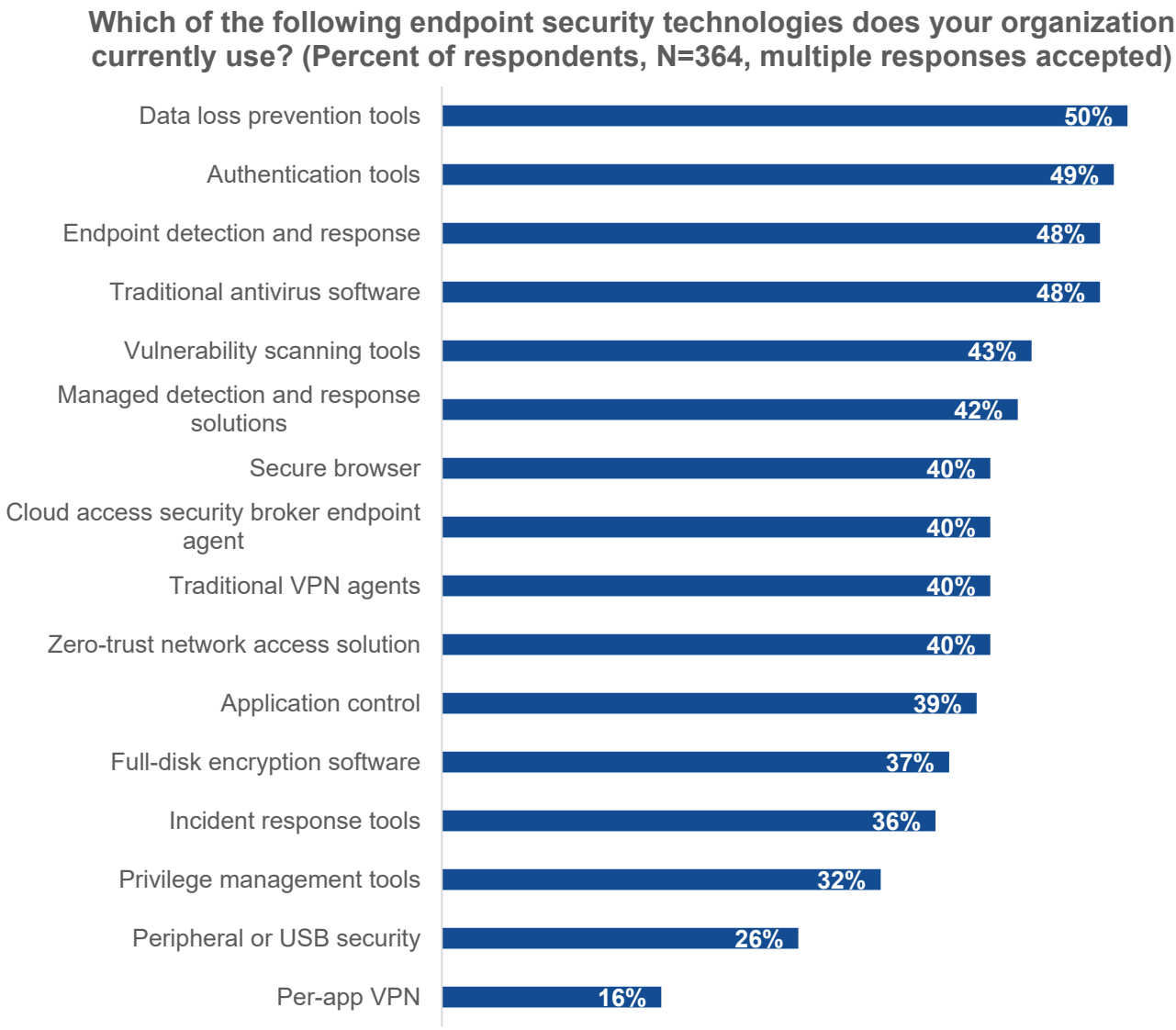
[1] Source: Enterprise Strategy Group Research Report, *The Growing Role of AI in Endpoint Management and Security Convergence*, June 2025. All research references and charts in this Showcase have been taken from this research report.

This Showcase from Enterprise Strategy Group was commissioned by Push Security and is distributed under license from TechTarget, Inc.

© 2025 TechTarget, Inc. All Rights Reserved

Information Classification: General

Figure 1. Endpoint Security Technology Usage



Source: Enterprise Strategy Group, now part of Omdia

While some enterprises have deployed secure enterprise browsers, those tools have been focused predominately on insider risk management and data loss prevention. Such tools can restrict copy-paste, mask sensitive information, and reduce accidental data leakage to address insider threats but seldom focus on external threats attempting to compromise the enterprise.

Adversaries understand that the browser provides a key entry point from which they can expand a foothold. As endpoint and network layers have become more hardened, attackers have been quick to develop and exploit a growing number of threat vectors in the browser. While browsers themselves are rarely the target, the identities and sessions used within them are the prize that adversaries seek. Threats such as phishing, credential theft, session hijacking, and even malicious extensions or app integrations all offer paths to compromise.

The browser is an underappreciated piece of the attack surface that needs improved defenses, but it's also one of the richest sources of threat telemetry for modern attacks. The browser provides visibility into how phishing pages

load and behave, when users attempt to submit stolen credentials, or when attackers hijack active sessions. It also reveals risky behaviors like shadow app usage or unvetted extensions. These are signals that many traditional endpoint and network tools struggle to capture.

Enterprises face multiple challenges when it comes to controlling risk around browser-based threats, and the browser blind spot affects multiple security teams in the enterprise:

- **SOC analysts** are blind to activity in the browser and struggle to detect or hunt for threats targeting SaaS or identities.
- **Security operations teams** suffer from slow investigations and gaps in incident response.
- **Identity security teams** have no way to see or enforce policy across shadow apps and unmanaged accounts.
- **Third-party risk management teams** often lack visibility into all the external services being trusted with corporate data.
- **Compliance and GRC teams** cannot confidently demonstrate SaaS account controls or password hygiene.

While work has moved into the browser, security has not followed for many organizations. As a result, security teams lack both the visibility and controls to defend their organizations against the majority of modern attacks.

Protecting Against Browser-borne Threats With Push Security

The Push Security team combines offensive and defensive cybersecurity expertise and experience to counter external threats at the browser layer. This brings the power of endpoint detection and response tooling to the browser.

Push uses a browser extension as a security agent inside every users' browser to provide real-time visibility, precision detection, and in-browser controls to stop attacks at the earliest point in the kill chain.

Push Security solves for key use cases:

- **Real-time detection of browser-based attack techniques:** Includes zero-day phishing, MFA-bypass toolkits, password-based attacks, session hijacking, clickfix attacks, etc.
- **Account takeover detection:** Stop account takeover activity with stolen credential and compromised token detection.
- **Incident response:** Leverage comprehensive browser telemetry to inform and accelerate incident response.
- **Proactive attack path hardening**: Identify and close off viable attack paths, including unsecure identities, malicious browser extensions, and risky app integrations.
- **Secure shadow SaaS:** Identify and control shadow SaaS in the browser.

Push's dedicated offensive research into browser attack techniques and vectors directly drives the development of new telemetry, detections, and response actions. This research-led approach helps defenders anticipate and counter new adversary techniques, continuously adapting to the evolving tactics attackers use in the browser.

Conclusion

Enterprises face a shifting threat landscape, and the browser is becoming the new endpoint. Enterprise security teams need the visibility and control that they expect at the endpoint layer to also be available at the browser layer where many attacks now happen. Existing tooling does not provide adequate visibility into threats originating in the browser, particularly identity-based threats such as phishing, credential theft, and session hijacking.

Push Security provides this essential security layer with real-time threat detection and response capability to stop attackers where they now operate. Push Security enables organizations to identify, analyze, and counter those threats, and the Push platform and the browser telemetry it provides will lend itself to a broader set of security use cases in the future.

©2025 TechTarget, Inc. All rights reserved. The Informa TechTarget name and logo are subject to license. All other logos are trademarks of their respective owners. Informa TechTarget reserves the right to make changes in specifications and other information contained in this document without prior notice.

Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of Informa TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com