Cisco Secure Access + Microsoft Edge for Business Integration

Expanding the reach of Zero Trust Security



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Access is now available as an advanced enterprise browser integration for Edge for Business. As a single, deeply integrated connector, it brings secure access, unified data protection, and AI guardrails directly into the browser.

Securing data in the browser era

Organizations have become more distributed, and the browser has become a major workspace for modern business. Employees, contractors, and partners increasingly access private applications, SaaS platforms, and AI-powered tools directly through the browser—often from unmanaged or personal devices.

While many organizations are adopting Zero Trust Network Access (ZTNA) to control who can access private applications, a critical challenge remains: What happens after access is granted?

In many cases sensitive information can still be copied, pasted, downloaded, printed, shared, or exposed. Traditional approaches such as VPNs, Virtual Desktop Infrastructure (VDI), and fragmented security controls add complexity, increase costs, and create inconsistent user experiences.

Security leaders need a simpler way to extend zero trust principles beyond access control and into the browser itself—that is exactly where Cisco Secure Access and Edge for Business now work together to protect sensitve data.

The challenge

Securing private applications on managed and unmanaged devices

Organizations need to provide secure access to private applications for employees, contractors, third parties, and partners—regardless of device ownership.

At the same time, security teams must:

- Prevent data exfiltration from sensitive applications
- Enforce consistent security policies across managed and unmanaged devices
- Enable secure BYOD access without deploying complex infrastructure
- Reduce dependence on VPNs and costly VDI environments
- Govern the use of AI tools and AI-assisted workflows
- Simplify operations while improving user productivity

Now, with more work happening in the browser – where users read, edit, download, and share sensitive data – it has become an important surface where exposure occurs and where protection must be enforced.

© 2026 Cisco and/or its affiliates. All rights reserved.

The solution

Unified Zero Trust Security from browser to cloud

Cisco® Secure Access and Microsoft Edge for Business deliver a unified approach to secure access and data protection.

Cisco Secure Access provides cloud-delivered Security Service Edge (SSE) services including Zero Trust Network Access, Data Loss Prevention (DLP), threat protection, and continuous policy enforcement.

Microsoft Edge for Business extends those protections directly into the browser, enabling local enforcement of data security controls at the point where users interact with sensitive information.

Together, they create a continuous security model that:

- Verifies user identity and device trust
- Grants secure access to authorized applications
- Enforces consistent DLP policies across browser and cloud layers
- Protects sensitive data during active use
- Provides visibility into user activity and security events

This integration allows organizations to extend protected access to unmanaged devices while maintaining strong control over sensitive business information.

Key benefits and capabilities

Extend Zero Trust Access to additional devices

Provide secure access to private applications for employees, contractors, partners, and third parties on a variety of devices. Enable identity verification and device trust assessments to reduce risk and help enforce compliance across a diverse set of users.

Protect sensitive data at the point of use

Apply granular controls directly within Microsoft Edge for Business, including:

- Copy and paste restrictions
- File upload and download controls
- Printing controls
- Screenshot prevention

These controls help prevent data leakage even after access has been granted.

Unify DLP Policy management

Create and manage a single set of DLP policies in Cisco Secure Access and apply them consistently across browser and cloud enforcement points. This unified approach helps to reduce policy fragmentation, simplify administration, and strengthen compliance.

Enable secure BYOD and third-party access

Allow users to securely access private applications from personal devices without requiring VPNs, VDI environments, or complex endpoint deployments. Agentless device trust capabilities help verify device posture while delivering a seamless user experience.

© 2026 Cisco and/or its affiliates. All rights reserved.

Gain deep visibility and compliance reporting

Combine browser telemetry with Cisco Secure Access security insights to deliver visibility into:

- Access events
- Device trust validation
- Data protection violations
- User activity
- Security incidents

Detailed reporting helps accelerate investigations, support compliance initiatives, and reduce operational overhead.

Cisco Secure Access and Edge for Business AI Protections

When unmanaged devices access public AI applications, the Edge for Business browser can enforce Secure Access DLP policies on file uploads, paste content, and local printing.

The use of Secure Access with the Secure Client (managed device) provides visibility and control over end user GenAI activities; visibility and protection for developer downloads of AI models; and visibility and semantic inspection for agentic activities.

Additionally, Edge for Business, through its Copilot control panel in the Edge management service, provides a layered framework for enabling, constraining agentic AI behavior within the enterprise browser.

Security that extends beyond access

Cisco Secure Access enforces policy at the network and application layers, while Microsoft Edge for Business extends protection directly into the browser experience.

Together they deliver:

- Zero Trust access for private applications
- Unified DLP policy enforcement
- Agentless device trust verification
- Browser-native data protection controls
- AI-aware security controls
- Strong protection across managed and unmanaged devices

The result is a modern approach to secure access that reduces complexity, improves user experience, and protects sensitive data throughout browser sessions.

Take the next step

Experience a simpler, more effective way to secure users, applications, and data in distributed environments.

Contact your Cisco account team or partner to learn how Cisco Secure Access and Microsoft Edge for Business can help you extend zero trust security while simplifying operations and reducing risk.

Learn more: Cisco Secure Access and Edge for Business Joint Solution Guide.

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C45-6502254-00 08/26