

INSIGHTS | TECH BRIEF

Close The Last Mile: Secure User Activity In SaaS & Web Applications

Enterprise security strategies have matured across identity, network, and endpoint controls. However, a critical gap remains inside the user session. As work shifts to SaaS and browser-based applications, organizations lack control over how data is accessed, used, and shared after login.

The enterprise browser introduces a new control layer that enforces policy where risk actually occurs. It provides governance at the point where users interact with applications and sensitive data.

The Business Problem: Security Stops at Login

Most security investments focus on granting access securely. Few control what happens after access is granted.

This creates measurable risk:

- Sensitive data can be copied, downloaded, or shared from SaaS applications
- Contractors and third parties access systems from unmanaged devices
- Security teams lack visibility into user actions within applications
- Organizations rely on VDI and VPN to compensate for missing controls

These gaps directly impact:

- Regulatory compliance across PCI, HIPAA, and SOX
- Third-party and supply chain risk
- Insider threat exposure
- Business continuity during security incidents

The result is a fragmented model where access is controlled, but data usage is not.

The WEI Approach:

Practical, Proactive & Proven

WEI takes a holistic, risk-based approach to cybersecurity, integrating people, processes, and technology to build a defense strategy that addresses every layer of risk. Our methodology ensures proactive, adaptable security measures tailored to your organization's unique challenges.

STRATEGIC SECURITY SERVICES

- Strategy Development & Analysis
- Maturity Assessments

SECURITY COMPETENCIES

- Cyber Security Strategy
- Cloud Security
- SIEM & SOAR Orchestration
- Policy Framework
- Incident Response
- Vulnerability Management

Learn more about WEI Cybersecurity

Island

The Security Gap: No Control Inside the Session

Today's enterprise security stack is strong at the perimeter and identity layer:

- Identity and access management verifies users
- SASE and ZTNA secure connectivity
- Endpoint tools validate device posture

However, none of these controls govern user behavior inside an active session. Once a user is authenticated, organizations often lose visibility and control over how data is handled.

You have now entered the last mile of security!

Introducing the Enterprise Browser

An enterprise browser embeds security, governance, and policy enforcement directly into the user's primary workspace.

Unlike traditional browsers, it enables organizations to:

- Control user actions such as copy, paste, upload, and download
- Enforce data protection policies within SaaS and web applications
- Monitor user behavior in real time
- Apply consistent controls across managed and unmanaged devices

Where the Enterprise Browser Fits

The enterprise browser complements existing security investments by closing a persistent gap. Below, we walk through common use cases.

Security Layer	Primary Function	Limitation
Identity (IAM)	Authenticates users	Does not control data usage
SASE / ZTNA	Secures connectivity	Limited visibility inside sessions
Endpoint	Validates device posture	No control over SaaS interactions
Enterprise Browser	Governs user behavior and data	Extends control into the session

1. Solve The SaaS Data Leakage Problem: The shift to SaaS and web applications has exposed critical data and workflows to consumer browser vulnerabilities. To mitigate these risks, organizations have traditionally relied on a patchwork of tools which is often ineffective and complicated.

An enterprise browser offers a fundamentally different approach to cybersecurity. By securing data directly within SaaS and web applications, it eliminates the need for multiple, and often contrasting, security solutions. Businesses can benefit from the following capabilities:

- **Granular Access Control:** Protect any application's specific pages, workflows, and data through seamless IdP integration. For example, secure legacy in-house web applications with multi-factor authentication (MFA) without requiring code modifications.
- **Comprehensive Data Protection:** Control how data moves within and outside applications. Prevent sensitive information, such as customer records, from being inadvertently shared or copied.
- **Conditional Access:** Ensure devices meet stringent security requirements before granting access to critical SaaS applications. Continuously assess devices for factors like patch levels, disk encryption, and endpoint protection status to enforce a strong security posture.

2. A Radical (And Sensible) Departure From VDI: Many organizations have turned to virtual desktop infrastructure (VDI) to provide remote access to critical applications. However, VDI often introduces substantial costs and user frustration.

An enterprise browser offers a modern, secure, and efficient alternative. Organizations can significantly reduce VDI reliance, thereby reducing costs, and enhancing user experience. Key features of include:

- **Data segregation and application isolation:** Enterprise browsers protect sensitive data by isolating it from the device. For example, when used on unmanaged devices, it can prevent data from being saved, downloaded, or copied from enterprise applications.
- **Remote access capabilities:** Enterprise browsers enable secure remote access to internal enterprise resources without requiring a separate virtual private network (VPN) client, supporting hybrid and remote workforces.

3. Zero Trust Integration: Zero trust is a critical security model that shifts focus from static network perimeters to user identity, device health, and restricted resource access.

Unlike consumer browsers, an enterprise browser actively incorporates zero trust practices directly into the browser environment, where most application and data access occurs. This approach strengthens enterprise browser security and aligns with the overall cybersecurity strategy.

To effectively implement an end-to-end zero trust experience, an enterprise browser must possess the capabilities of user identity verification, device posture assessment, and ZTNA enablement.

4. Third-Party Access Management: As organizations expand their workforce through contractors or business process outsourcing (BPOs), ensuring efficient and secure access becomes a critical challenge. Managed laptops or virtual desktops are usually the solutions, but these often introduce significant costs, delays, and user frustrations.

With the enterprise browser, organizations rapidly grant access by enabling contractors to use their existing devices while maintaining complete control over enterprise browser security and data. Unlike virtual desktops, these eliminate performance bottlenecks.

5. Building Data Loss Prevention: Modern work environments extend beyond the office, involving unmanaged devices, networks, and a growing array of SaaS and web applications. However, legacy data loss prevention (DLP) platforms are not equipped for these conditions.

The enterprise browser embeds data loss protection within the platform, creating a more effective and efficient cybersecurity strategy tailored to diverse work settings and businesses.

6. Integrating Apps From Mergers, Acquisitions and Divestitures: Merging or acquiring another company is complex, as integrating IT systems alone can take months or even years. This hinders communication and collaboration precisely when they are most crucial.

An enterprise browser accelerates this integration by addressing key pain points during a merger and acquisition:

- Providing immediate and extensive access to all private and internal applications, resources, and communication tools across diverse networks – all while enforcing consistent IT and security policies such as ZTNA, thus bypassing VPN or infrastructure changes
- Allows new employees to use their personal laptops or other devices to connect with their colleagues.

7. Adaptable With Various Devices: With the rise of remote work, enterprise browsers have become essential for enabling secure access to applications from any location. Additionally, these offer a flexible solution for employees who frequently use personal devices at work to enable secure access to company resources while keeping personal data separate. This capability provides a more user-friendly and cost-effective alternative to traditional VPN or VDI solutions, making enterprise browsers a key component of a modern cybersecurity strategy.

8. Support Continued Operations During Security Incidents: To contain cyber threats, IT teams often shut down endpoints and disable network segments during incident response. This forces employees to halt work or use alternative devices, causing significant business disruptions.

The enterprise browser empowers staff to maintain uninterrupted operations during severe cybersecurity incidents by enabling self-service installation on personal devices or other hardware. This allows employees to access critical communications and business applications instantly, strengthening the overall cybersecurity strategy.

Moreover, the security features of an enterprise browser automatically adapt to device conditions, which is important in safeguarding against data breaches. This centralized management also accelerates incident response and facilitates a gradual restoration of business operations.

Business Outcomes

Risk Reduction

- Reduced SaaS data exposure
- Controlled third-party access
- Limited insider threat risk

Financial Impact

- Reduced reliance on VDI infrastructure
- Consolidation of overlapping security tools

Compliance and Governance

- Audit-ready visibility into user activity
- Consistent enforcement of data handling policies
- Improved alignment with regulatory requirements

When to Consider an Enterprise Browser

Enterprises have made significant progress securing identities, networks, and endpoints. However, the point where users interact with data remains exposed.

Organizations should evaluate this approach when they experience:

- Increasing exposure of sensitive data in SaaS applications
- Growing reliance on contractors, partners, or BPOs
- Challenges securing BYOD environments
- High operational cost from VDI or VPN usage
- Limited visibility into user activity within applications

Contact WEI Today

WEI takes a risk-based, advisory-led approach to enterprise security, helping organizations identify gaps in SaaS data protection, third-party access, and Zero Trust enforcement. By aligning enterprise browser capabilities with broader security architecture, WEI enables organizations to reduce exposure, simplify overlapping tools, and strengthen compliance posture. The focus is on delivering measurable outcomes, including improved control over user activity, stronger governance, and a more resilient security framework.

Contact WEI's cybersecurity experts to start your enterprise browser journey.

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.