ACIUM

White Paper

The Emergence of Unified Browser Security™

How Unified Browser Security is quietly emerging as a critical concern for security and EUC professionals

© 2025 Acium, Inc. All rights reserved. | Acium.io

In today's rapidly evolving threat landscape, attackers are always one step ahead, exploiting new vulnerabilities in network security, unmanaged browsers, and unsuspecting users. To stay ahead, organizations must adapt and adopt cutting-edge strategies to safeguard against these risks, especially within the unmanaged web browsing environment.

The web browser has emerged as a significant vulnerability point, serving as a launching pad for attackers to execute various exploits, including malware injection, credential theft, and phishing attacks. This is particularly problematic as more organizations have transitioned to a hybrid work model. Employees now frequently shift between office and remote locations, using various devices and mixing work and personal tasks within the same browser sessions. Shockingly, less than 10% of browsers within organizations are currently configured and managed correctly, leaving them susceptible to basic attacks.

As a response to the growing threats, solutions such as 'Enterprise Browsers' or 'Browser Security Platforms' have emerged. However, while acknowledging the need for such solutions, many of the current offerings demand significant operational changes, creating barriers to their full adoption.

The enterprise browser approach: a flawed strategy?

Enterprise browsers aim to rebuild browsers with enhanced security features. Advocates argue that commercial browsers, like Google Chrome and Microsoft Edge, were not originally designed for enterprise use, despite being widely used for productivity today. These commercial browsers share a strong security foundation built on the Chromium open-source project, but some believe they fall short when it comes to enterprise-level security.

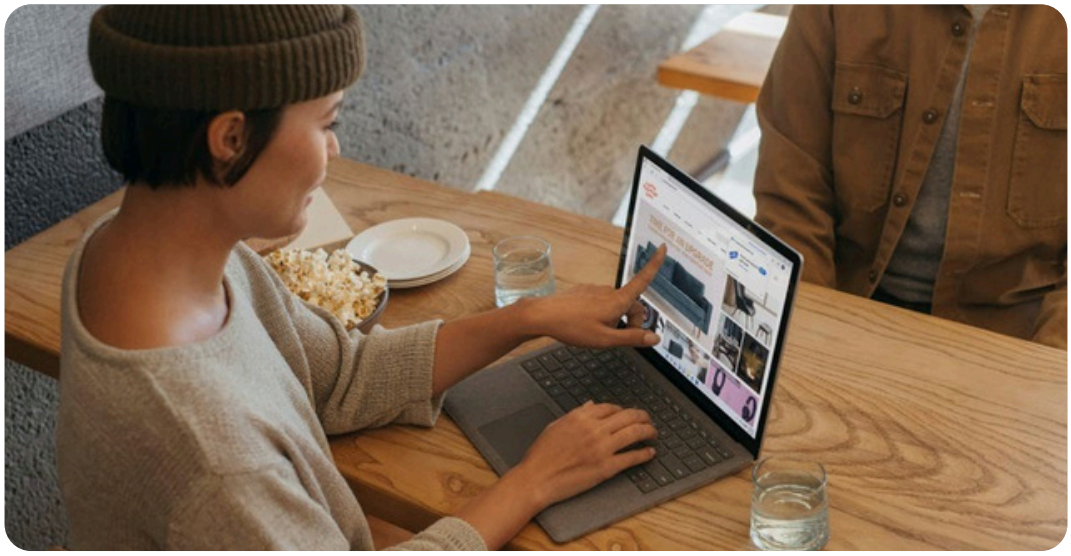
However, forcing customers to replace their preferred browser, slowing innovation, or retraining users does not align with practical business needs. Many enterprise browser solutions have already shifted away from this approach due to poor adoption.

© 2025 Acium, Inc. All rights reserved. | Acium.io

Browser security platforms: a step forward, but not enough

Another approach, Browser Security, enhances security by enforcing policies via a browser extension that works across both managed and unmanaged devices. This solution enables real-time user activity monitoring to prevent web-based threats and other risky or unauthorized behaviors.

While this is a step in the right direction, Browser Security alone does not provide the comprehensive protection organizations need. It is here that Unified Browser Security (UBS) emerges as the more effective, holistic approach.



What is unified browser security?

Unified Browser Security (UBS) offers a browser-agnostic solution that provides organizations with the tools and strategies to manage and secure all their web browsers effectively. Unlike solutions that focus solely on browser replacement or limited browser security features, UBS delivers a comprehensive set of capabilities.

Key benefits of unified browser security:

- **Unified Browser Security:** Streamlined configuration and policy management across all browsers
- **Security:** Enhanced security for existing browsers with a strong security foundation
- **Data Protection**: Real-time safeguarding of in-flight data
- **Visibility:** Deep insights into browser usage, user activity, and potential threats
- **Analytics:** Machine learning-powered reporting for both alerting and incident response

© 2025 Acium, Inc. All rights reserved. | Acium.io

Why unified browser security matters

Unified browser security allows EUC and Security teams to centrally oversee web browser configurations across various operating systems and devices. Our cloud-based approach ensures updates and policies are seamlessly delivered when users open their browsers, enhancing both security and the user experience.

Security measures that focus on web browsers provide an additional layer of protection that network and endpoint security solutions cannot. Local browser security management prevents web-based attacks, including malware and data exfiltration, that can originate from websites, SaaS apps, and unsanctioned applications.

Leveraging AI and machine learning

By harnessing AI and machine learning, UBS provides powerful insights into user behavior and browser sessions. Anomalies in browser usage can be identified, helping teams address potential risks before they escalate. Additionally, UBS allows for automated management of alerts, reducing alert fatigue by prioritizing the most critical events.

Addressing a blind spot: visibility and analytics

One of the most significant challenges faced by EUC and security teams is the lack of visibility into browser usage and security status across an organization. Without a global view of all browsers, keeping track of usage patterns, security configurations, and update statuses becomes over whelming.

With Unified Browser Security, teams can gain full visibility into sanctioned and unsanctioned apps, shadow identities, browser configurations, and usage data. This holistic view significantly reduces response times to business needs, enabling security teams to proactively identify and address potential threats.

Introducing Acium: a comprehensive solution

As organizations seek to enhance their browser management and security, platforms like Acium offer a robust approach to Unified Browser Security. Acium provides organizations with the tools they need to effectively manage and secure their existing browsers while maintaining user familiarity. By focusing on managing and securing their chosen browsers, enterprises can prevent issues such as browser misconfiguration, malware, phishing attacks, and credential theft.

© 2025 Acium, Inc. All rights reserved. | Acium.io

The future of Unified Browser Security

As the browser has firmly established itself as the most widely used productivity tool, and as it evolves into the superapp of the future, it's imperative that EUC and Security professionals prioritize browser protection. Unified Browser Security enables organizations to take control of their browser environments, securing them without impacting user productivity.

Organizations seeking to enhance browser security should take proactive steps to secure the browsers they are already familiar with, rather than being locked into a specific vendor. By focusing on the management and security of their chosen browsers, enterprises can protect themselves against browser misconfiguration, malware, phishing attacks, credential theft, and ensure comprehensive data protection.

Take control of your browsers. Protect your enterprise. Secure the future.

Discover how Acium can transform your security strategy. Schedule a personalized demo today.

© 2025 Acium, Inc. All rights reserved. | Acium.io