

# Unified Browser Security™: Safeguarding the Modern Workforce

Empowering organizations with flexible, scalable  
browser security for the modern workforce

As organizations adapt to the dynamics of hybrid work models, BYOD initiatives, third-party business services, business process outsourcing, and contractor engagement, the landscape of digital operations is evolving rapidly. These modern workforce use cases bring significant advantages but also introduce risks, including the rise of unmanaged or distributed devices and unsanctioned applications. This results in security blind spots for End User Computing (EUC) and security teams.

The solution? Unified Browser Security (UBS), which provides organizations with the visibility and control they need to mitigate these risks while streamlining management operations.



## The role of browsers in modern business operations

The browser has evolved from a simple tool for accessing the web into the modern "super app," a gateway for users to access nearly every critical business service. Workers use browsers across a variety of devices—some managed, others unmanaged—ranging from corporate-issued laptops to personal mobile devices used by contractors or third parties.

Yet, despite the growing importance of browsers in today's work environment, fewer than 10% of browsers are currently managed, according to Gartner. This represents a huge security gap that enterprises need to address. By utilizing the browser as a security and management layer, organizations can deliver secure access, protect sensitive data, and gain much-needed visibility into user behavior across devices.



## Key use cases for Unified Browser Security

### Third-party and contractor workers

Organizations frequently employ third-party contractors and outsource business processes, increasing the number of unmanaged devices accessing corporate resources. By implementing Acium's UBS, security and EUC teams can enforce access policies that require the use of protected browsers. This ensures consistent protection on any device while providing the necessary visibility to reduce risk.

### Supplementing VDI and RBI deployments

For organizations using Virtual Desktop Infrastructure (VDI) or Remote Browser Isolation (RBI), Acium's UBS offers a cost-effective supplement. By securing browsers directly, UBS enhances VDI setups by applying security controls at the browser level, reducing the strain on VDI systems. This approach improves user experience and lowers overall costs while ensuring consistent browser security across both managed and unmanaged devices.

### BYOD programs

For businesses with robust BYOD programs, Acium's UBS allows employees to use their preferred browsers while ensuring corporate security policies are seamlessly enforced. This approach maintains user privacy, protects corporate data, and reduces the need for complex network infrastructure.

## Unified Browser Security: a simple, scalable solution

Acium's UBS is designed to provide secure and seamless access across all browsers, regardless of the device being used. Our solution simplifies access and data control measures, allowing IT teams to implement policies without adding complexity for end users or disrupting productivity. Users continue to enjoy their familiar browsing experience, but with the added protection of UBS.

Unlike legacy solutions such as secure web gateways or complex network-based tools, Acium's browser-based approach is remarkably easy to deploy. IT teams can integrate our extension across any browser within minutes, gaining unparalleled visibility into browser activities and eliminating security blind spots. Customer's will have the option to deploy Acium's control plane in a hyper-scale cloud, Co-Lo data center or on-prem.



## Strengthening zero trust architectures

Acium's UBS is designed to integrate with and enhance existing security infrastructures, including zero trust architectures. By adding granular security controls at the browser level, UBS allows organizations to conduct continuous device posture checks for all users, whether they're using managed or unmanaged devices.

Through API integrations with XDR and SIEM platforms, our solution provides visibility and telemetry data that extend the effectiveness of existing security stacks. This creates a stronger zero trust framework and ensures that no user or device is a weak link in the security chain.

## The future of work, secured

As work models continue to evolve, so too must the methods for securing the workforce. Browsers are now at the center of the modern work experience, and as such, they represent both a valuable tool and a potential vulnerability. Acium's UBS empowers organizations to protect their users, data, and digital environments with a solution that is both simple to implement and highly effective at reducing risk.

## Modern work, secured and simplified

The way we work has changed, and so must our approach to security. Acium's Unified Browser Security offers a solution that improves user productivity, reduces IT costs, and enhances cybersecurity across the board. By leveraging the browser as a key security layer, organizations can manage modern workforce use cases with confidence, efficiency, and ease.

Ready to secure your workforce with Acium's Unified Browser Security? Discover how we can help you achieve unparalleled visibility, control, and security. Visit [Acium.io](https://Acium.io) to learn more or [contact our team for a personalized demo today!](#)