

Solution Brief

Visibility and Control for Corporate Data and SaaS Access with the Mammoth Extension

Enterprise Browser Capabilities in an Easy-to-Deploy Form Factor

The browser has become the defacto interface for enterprise users to access the applications and data they need to do their jobs effectively and efficiently.

While the Mammoth Extension does not provide every capability included in the Mammoth Browser, it does provide a core set of functionality that provides visibility and control when users are able to select their own browser.

Securing access to key company data has been a long-standing security risk that requires a modern solution. Companies are looking for more visibility around who has access to sensitive information and need answers to questions around who has access to their data, and what can they do with it. The Mammoth Extension brings a new approach that answers these questions by providing the context, visibility and controls to tailor permissions, control user actions and maintain detailed audit logs for company employees and contractors.



Key capabilities of the Mammoth Extension include:

- ✓ Enforcing strict access control to company resources without sacrificing user productivity
- ✓ Integrating with existing security ecosystem (Identity management, infrastructure, logging)
- ✓ Preventing data loss by implementing least privileged access across all
- ✓ Meeting compliance requirements with verbose user activity logging

Traditional Approaches Have Hit the Wall

Traditional approaches to providing secure access to company resources have reached their limits in the new world where web user interfaces dominate the Enterprise workspace with remote access to resources on-prem and in the cloud. The same encryption that makes SSL VPNs effective for securing connections prevents them from allowing deeper visibility to what users are doing once they are authenticated. Remote desktop approaches like VDI are costly, difficult to manage and typically have a user experience challenge that leads employees to look for ways to bypass them altogether. A new approach to securing company resources is clearly in order.

A New Approach

The browser has evolved over the years into the primary access point for employees to reach key enterprise and SaaS applications. The position of the browser in this remote network architecture, with its view of the source of so many transactions, eliminates the need to proxy and decrypt network traffic, provides significantly more context, and allows the real-time analysis of web browser sessions for security monitoring.

The Mammoth Extension solution combines a policy engine and a corporate controlled browser extension that works with any standard browser. Users get the freedom to choose their browser, and Enterprise IT teams get the visibility and control they need to secure company resources. The Mammoth Extension allows Enterprises to implement centralized controls for functions like enforcing least privilege access, requiring multi-factor authentication, alerting on risky usage and more. A complete audit log of user actions enables and simplifies compliance reporting for key industry mandates.



Ease of Deployment

No need to mandate a particular browser for users. The Mammoth Extension works with any standard browser like Chrome or Edge to give users the choice they demand. The Extension can be deployed via MDM solutions like Intune for seamless corporate control.

User Experience

The Mammoth Extension helps IT security teams monitor web use while minimizing the impact to end users. With no impact to the browser, all functions remain the same for corporate users.

Technology Intergrations

Integration with Identity Providers like Okta or Azure AD allows a seamless and automated exchange of role based permissions. Identity and permission management flags the use of corporate identities for external accounts where identities can be more easily compromised.

The Mammoth Difference

Our Mammoth Extension solution solves critical access problems while improving security posture, driving compliance, accelerating deployment and simplifying policy management.

- ✓ Prevent data theft with control over the access and actions of remote employees, 3rd party contractors and partners
- ✓ Drive compliance to industry mandates with visibility and audit logs for user behavior
- ✓ Enhance productivity with a seamless end user experience and simple deployment
- ✓ Enable the shift to a zero-trust security architecture with visibility and control at a critical access point



Schedule a self-start from your mobile device at mammothcyber.com or contact demo@mammothcyber.com to secure your LLM-Centric AI with Zero Trust on Zero Day!

Get Started