MAMMOTH CYBER

DATA SHEET

Enterprise Browsers: A Critical Component of the Cybersecurity Stack

Existing Browsers Are Not Designed for the Enterprise

While many applications within an organization are tailored for enterprise use or have specialized versions designed to meet corporate needs, one critical tool remains largely unchanged: the web browser. Over time, browsers have evolved into the primary gateway for employees and contractors to access enterprise applications, SaaS platforms, and various web-based functions. However, this reliance poses a significant challenge because consumer-oriented browsers lack the robust security and compliance controls essential for organizational use. This makes browsers a prime target for malicious actors, who exploit them in two main ways:

1. **Stealing Sensitive Information:** Attackers target browsers to discover information such as cookies, passwords, and tokens, providing access to the sensitive data on many corporate applications, posing a significant threat to data security.
2. **Installing Malware:** Malicious actors leverage browsers as vectors for malware installation, utilizing techniques like drive-by downloads or malicious browser extensions to infiltrate systems.

Traditional Cybersecurity Approaches Leave Gaps in Visibility and Enforcement

- Solutions like Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) and Secure Service Edge (SSE) are network-based solutions and because they enforce controls far away from the user, they are not able to cover threats like locally installed malware stealing information from the endpoint.
- SSL VPNs, while effective in securing connections, lack visibility into user activities post-authentication due to encryption, limiting their ability to detect and mitigate threats.
- Virtual desktop infrastructure (VDI) may deter malware installation but come with excessive costs, management complexities, and usability issues that drive users towards less secure alternatives.

Enterprise Browsers Emerge as a Critical Component of the Cybersecurity Stack

Recognizing that the browser serves as the primary access point for web activities, SaaS applications and private apps, securing it becomes paramount. This approach offers inherent advantages: browsers possess contextual insight and can proactively intercept threats at the source, enabling real-time protection and analysis impossible with network-centric solutions.

Enterprise Browsers are a new product category that combines a policy engine and a hardened Chromium-based web browser. The Mammoth Cyber solution enforces conditional access and prevents data leakage as users connect to the public cloud, internal applications, and SaaS applications. Integrations with identity providers automate the secure onboarding of remote users, contractors, and partners without the need for VDI or VPN connections. By securing the browser, Mammoth Cyber revolutionizes web security, providing organizations with unparalleled protection and control over their digital assets in an increasingly complex threat landscape.

Key Benefits of the Mammoth Cyber Enterprise Browser:

1. **Enhanced Security:** Enterprise Browsers provide secure access to web resources by providing advanced threat protection and prevent data leakage through granular data access controls
2. **Cost-effective:** Replacing VDI with Enterprise Browsers can lead to massive cost savings by reducing the need for expensive hardware and software infrastructure, as well as ongoing maintenance
3. **Simplified Management:** An Enterprise Browser reduces the complexity of managing remote access, allowing administrators to implement and enforce security policies across multiple platforms, applications and devices all from one place
4. **Improved End User Productivity:** By embedding controls directly into the browser instead of relying on separate virtual environments or proxies, we ensure a superior user experience and maximize productivity for your teams

How it Works

There are several critical components to building an Enterprise Browser – delivering a familiar browser experience users have come to expect, integration with Identity and Access Management (IAM) systems, DLP Capabilities to protect sensitive data, device security posture checking, native productivity enhancers like plug-ins, bookmarks and password vaults, and the flexibility to be deployed alongside other existing security tools like SWGs, CASBs and SSE. The Mammoth browser provides secure access to public cloud infrastructure, private cloud/data centers, public websites and SaaS applications.

While all these foundational elements are required for an Enterprise deployment, one of the capabilities that brings the most value to the security team is the integration with IAM systems. Applying identity information from products like Okta Workforce Identity and Azure AD provides important context to the Mammoth browser. Policies in the browser align to general enterprise principles but go beyond role and application to control permissions within each application. The context acquired through integration with the IdP, in conjunction with a privileged access policy model, allows security administrators to define contextual access policies about who should be allowed to connect to what, with what permissions and user behavior monitoring options enabled.

Why Mammoth Cyber?

Regain Visibility and Control of Internal & SaaS Application Activities

Once the gold standard for secure remote access, VPNs and VDI are widely deployed, but lack the visibility required to implement Zero Trust policies. With the Mammoth Enterprise Browser, users are not granted wholesale access to the network. They are only provided access to the applications they need to do their jobs, and detailed logging maintains a complete audit trail of all user actions.

Enable Conditional Access for Any Web Application on Any Device

The Mammoth Browser enables conditional access for web applications from any device with any identity provider, with policies to enforce access from corporate issued or personal devices. The access policies extend to data access, including copy, paste, print, upload, download and watermarking. This enables you to grant access to sensitive content only if the accessing device passes a certain security threshold. You can also prevent data leakage by restricting access at an application and user level.

Secure Developer Access Without Static Keys

The Mammoth Browser extends secure remote access even further by allowing users focused on dev and engineering roles to utilize their local environments.

These employees often have spent significant effort to customize their local environments and the browser includes capabilities that allow for SSH, RDP, Git, Kubernetes and Database access direct from their own environment.

Static keys are problematic since they can be stolen, reused and constantly need to be rotated. Mammoth provides one-time keys for each login which mitigate risks of key theft and obviate the need for key rotation.

Expand Identity Monitoring to All Web Applications

Integration with identity providers like Okta and Azure AD allows a seamless and automated exchange of role-based access controls. Mammoth's Enterprise Browser expands identity and permission management to applications that are not Single Sign-On enabled and monitor the use of corporate identities for external accounts where identities could be more easily compromised.

Streamline User Experience

The Mammoth Browser helps IT security teams enforce strict access policies while minimizing the impact to the end user. The Enterprise Browser presents a familiar interface for users to access the applications and data they need to do their jobs, and they no longer need to toggle between multiple VPN and ZTNA clients to access different applications.

FEATURE	DETAIL
DLP	• Identity-centric data access controls that monitor and restrict data movement such as copy, paste, print, upload, download, and more • Ability to restrict screenshare and apply dynamic watermarks • Track user activities like file upload to personal accounts • Modern DLP capabilities include scanning content to control access to pre-defined PII data types and Regex patterns • Support for Microsoft Sensitivity labels • Create trusted boundaries between apps to not hinder productivity and prevent data leakage at the same time • Restrict access to personal accounts on a SaaS app while only allowing your corporate accounts to be used • Dynamically mask SSN and credit card numbers without any changes to the web applications
Advanced Threat Protection	• Detect and block malicious sites as well as anti-phishing capabilities • Scan file uploads and downloads to ensure no malware gets on to endpoints
URL Filtering	• Scan billions of web pages and classify them into 80+ categories which are dynamically updated
Shadow IT Discovery	• Detect any unmanaged SaaS applications through deep identity tracking to monitor user activities on unmanaged SaaS applications • Detect shared accounts and impersonated accounts in any web application • Detect data exfiltration
Hardened Browser	• Session cookie, token and password encryption • Monitor and Control browser extensions • Secure credential management • Hardened browser that mandates site isolation • Enforce browser auto-update
Private Access	• Enable connections to internal networks without a VPN • Per application proxy forwarding • Dedicated forwarding proxy • Dedicated ingress/egress IP • Private access for native TCP apps

FEATURE	DETAIL
Developer Access to Key Infrastructure	• Extend conditional access to secure critical infrastructure applications in browsers and native applications – SSH, RDP, K8s, SMB, database, git and more • Certificate based SSH access to eliminate static keys and the need for key rotation, which have been a primary threat vector in recent years
Logging & Reporting	• Comprehensive audit logs for application access with a complete record of user access activities and continued monitoring of risky user activities like excessive file downloads • Policies that include the option to enforce controls as well as audit them • Ability to record SSH, RDP and web sessions • Save file uploads/downloads for auditing or compliance reasons • Detailed config logs for all admin events
Authentication & Authorization	• Integration with identity providers such as Okta, Azure AD, Google workspace, Ping Identity and OneLogin with support for SAML Single Sign-On (SSO) and SCIM to automate user provisioning • Ability to block access from other browsers • Incorporate Muti Factor Authentication (MFA) for all access • Conditional access with device trust and geofencing to prevent unauthorized access, for both managed and BYO devices
Technology Integrations	• SIEM/SOAR integration with Azure Sentinel and Syslog servers • EMM integrations to enforce device compliance policies • Integration with key vaults including HashiCorp Vault, AWS KMS, and Azure Key vault provides centralized key management
Cloud-based Management Console	• Manage policies, monitor data movement, and control browser settings from a central location • Published open APIs for integration with other security solutions as well as for console management functions • Role Based Access Control (RBAC) Controls for admins
Supported Platforms	• Windows 10, 11 • Mac OS 11.x,12.x and 13.x • Android

MAMMOTH CYBER

Contact us to learn more
+1 669 699 1122 | info@mammothcyber.com
mammothcyber.com