MAMMOTH CYBER

SOLUTION BRIEF

Preventing Data Loss from Remote Employees with an Enterprise Access Browser

Preventing Data Loss with a Secure Access Approach for Remote Employees

Intellectual Property theft and data loss results in hundreds of billions of dollars of losses every year. The growing number of employees working from home and other remote locations is shaping up to be a permanent change in how work is done in the modern enterprise. This puts considerable pressure on existing approaches to secure remote access, where problems that were merely annoying a few years ago have now become critical security issues. The large number of remote employees opens a substantial attack surface that requires a more scalable approach to provide visibility and control into the actions of remote employees.

Traditional Approaches Have Hit the Wall

Traditional approaches to providing secure access for remote employees have reached their limits in the new world of distributed remote employees accessing 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 user experience challenges that lead employees to look for ways to bypass them altogether. A new approach to secure remote access is clearly in order.

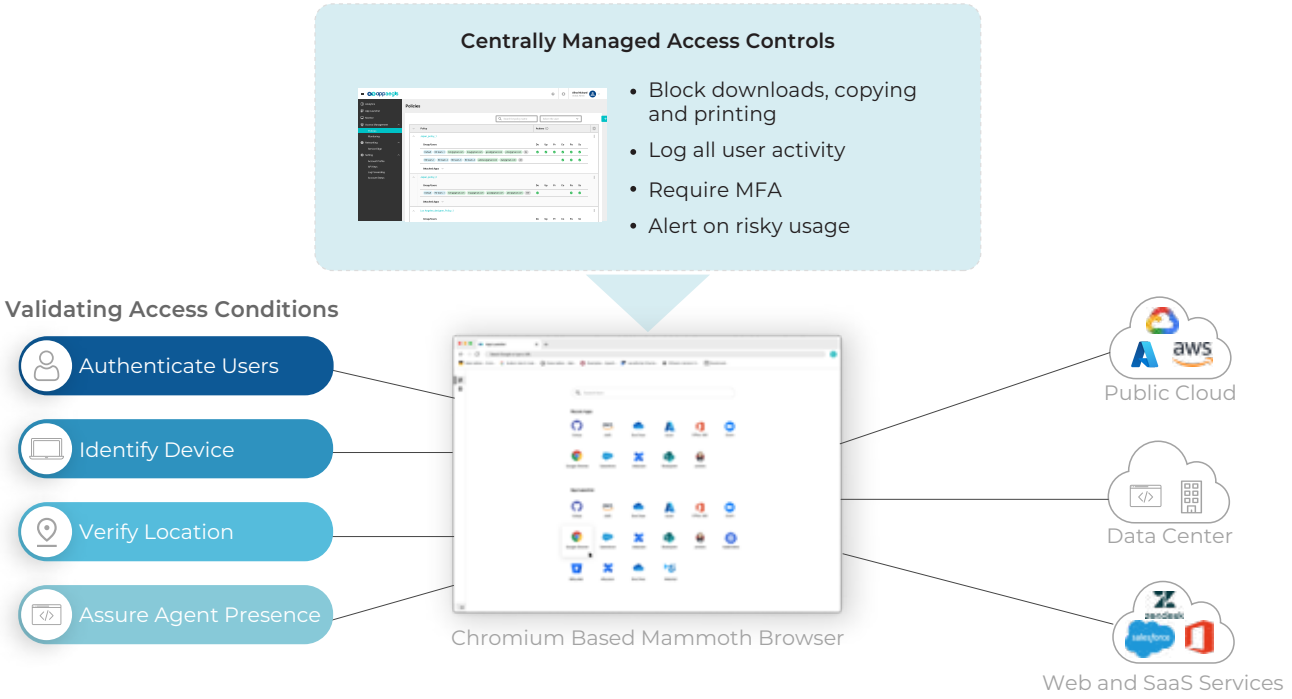
Four Ways to Prevent Data Loss

1. Implement conditional access policies to stop access with stolen credentials
2. Block user downloads of key intellectual property
3. Maintain detailed audit logs of any access to sensitive files or data
4. Watermark sensitive documents to deter file sharing and photography

A New Approach

The browser has evolved over the years into the primary access point for employees to reach enterprise applications, SaaS applications, and a multitude of other web-based functions needed to perform their jobs. 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 browser is also the ideal location to govern conditional access to a broad range of destinations including internal data centers and applications, public cloud access, SaaS Applications and websites. The Enterprise Access Browser (EAB) is a new product category that combines a policy engine and a Chromium based web browser to create a new solution for secure remote access. The Mammoth EAB provides the visibility needed 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.

Combining Conditional Access with Centrally Managed Access Controls



The Mammoth Difference

Our Enterprise Access Browser solves critical access problems while improving security posture, driving compliance, accelerating deployment and simplifying policy management.

- Block access with stolen credentials through conditional access policies
- Prevent data loss with complete control over remote employee access and actions
- Discourage intellectual property theft with visibility and audit logs for user behavior
- Watermark sensitive documents to deter sharing and photography
- Enable the shift to a zero-trust security architecture with visibility and control at a critical access point

MAMMOTH CYBER

Schedule a Demo
info@mammothcyber.com