WHITE PAPER

Secure Remote Access

MAMMOTH CYBER

Introduction

Enterprises around the world are relying on remote employees, contract workers and partner organizations to meet their staffing needs on an unprecedented scale. In some of the world's largest technology companies, contract workers are now outnumbering direct employees for the first time. In the US, 36% of the workforce is now freelancing across a variety of roles from sales and marketing to building applications and managing IT infrastructure. Though companies have tried to sequester contract workers and remote employees for obvious security reasons, the modern digital economy dictates that these workers need access to corporate cloud infrastructure, SaaS and internal applications, and sensitive business data in order to do their jobs.

A key consequence of this increased reliance on contract workers and partners is the increased security risk from allowing external users and unknown devices into trusted corporate environments. The Verizon Data Breach Investigation Report (DBIR) found that enterprise business partner access was responsible for 39% of the data breaches they investigated.

Securing access for external contractors and partners has been a long-standing security risk that requires a modern solution. Legacy VPN and VDI solutions provide the needed access, but their security controls are not only ineffective against escalating and stealthy attack methods, but worse in that hackers have effectively targeted and exploited their limitations to gain unauthorized access and infiltrate corporate applications, data and operating environments.

The Problem – Securing Access from Any Location on Any Device

As security practitioners worldwide look to improve their security posture with regards to 3rd party contractor and partner access, they have encountered numerous security and deployment limitations attributed to the legacy security products and architectures that assumed remote workers could be trusted once they had authenticated when connecting to a corporate network. These days we know better, and after countless incidents of compromised credentials that led to data theft and business disruptions, the industry shift to a adopt a zero-trust model needs to accelerate.

IT Security Teams designing, deploying and adopting a zero-trust access model that specifically targets remote contractor and partner access need to consider a number of important requirements for a successful deployment.

Key Requirements for Secure Remote Access for Contractors and Partners

- Secure identities and credentials with conditional access
- Integrate with existing security ecosystem (Identity management, infrastructure, logging)
- Prevent data theft by implementing least privileged access
- Meet compliance requirements with verbose user activity logging
- Enforce strict secure access without sacrificing user productivity

The issue at hand for those charged with security around Identity and Access Management and Privileged Access Management is the lack of visibility and control with legacy solutions such as Virtual Private Networks (VPNs) and Virtual Desktop Infrastructure (VDI). Trying to bolt on visibility and control capabilities to VPN solutions typically requires a man in the middle approach with a proxy that decrypts the tunnel, performs deep packet inspection and then re-encrypts the traffic. While technically possible, the implementation and certificate management required with this approach are quite cumbersome in practice and do not scale well when looking at hundreds or even thousands of employee connections. Similarly, taking a VDI approach has limitations when it comes to management complexity and cost. Managing policy controls on a per user basis adds strain to perennially understaffed IT and security teams. In practice, a 100% deployment of a VDI solution at scale is rarely achieved.

Limitations in Current Secure Remote Access Products

No easy way to monitor user actions post authentication
Network level access provides broad access that enables lateral movement
Complex to monitor user actions post authentication
Lack of privileged access controls for data protection
Negative user experience from bandwidth restrictions when having to hairpin traffic

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 browser's central position in the workflow of the modern enterprise provides a compelling opportunity for a new approach to implementing security controls at the source of the majority of connections and transactions.

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, web sites and more.

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 EAB provides the visibility that was the missing link needed to implement centralized controls for functions like data upload and download, copy and paste, printing, watermarking screenshot images, and more. A complete audit log of user actions enables and simplifies compliance reporting for key industry mandates.

The position of the policy engine in the EAB allows it to do more than just monitor web traffic and user actions. Companies are outsourcing everything from IT support, call centers and help desks, and software development and testing. These different job functions all need access to slightly different, yet sensitive applications. Software developers, for example, can still customize their environments to optimize efficiency with libraries and scripts that align with their tech stacks. The EAB is an ideal point to control functions outside of traditional web traffic and can be used to provide visibility and control for native SSH and RDP access for outsourced IT support contractors.

How it Works

There are several critical components to building an Enterprise Access Browser, including broad support for web-based applications to deliver the browser experience users have come to expect, integration with Identity and Access Management (IAM) systems, native productivity enhancers like plug-ins, bookmarks and password vaults, and the flexibility to be deployed alongside other existing security tools like secure web gateways and CASBs. The EAB provides access to public cloud infrastructure, private cloud/data centers, public websites and SaaS applications.

While all of these foundational elements are required for an Enterprise deployment, one of the capabilities that brings the most differentiated 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 EAB. Policies in the EAB 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 with which user behavior monitoring options enabled.

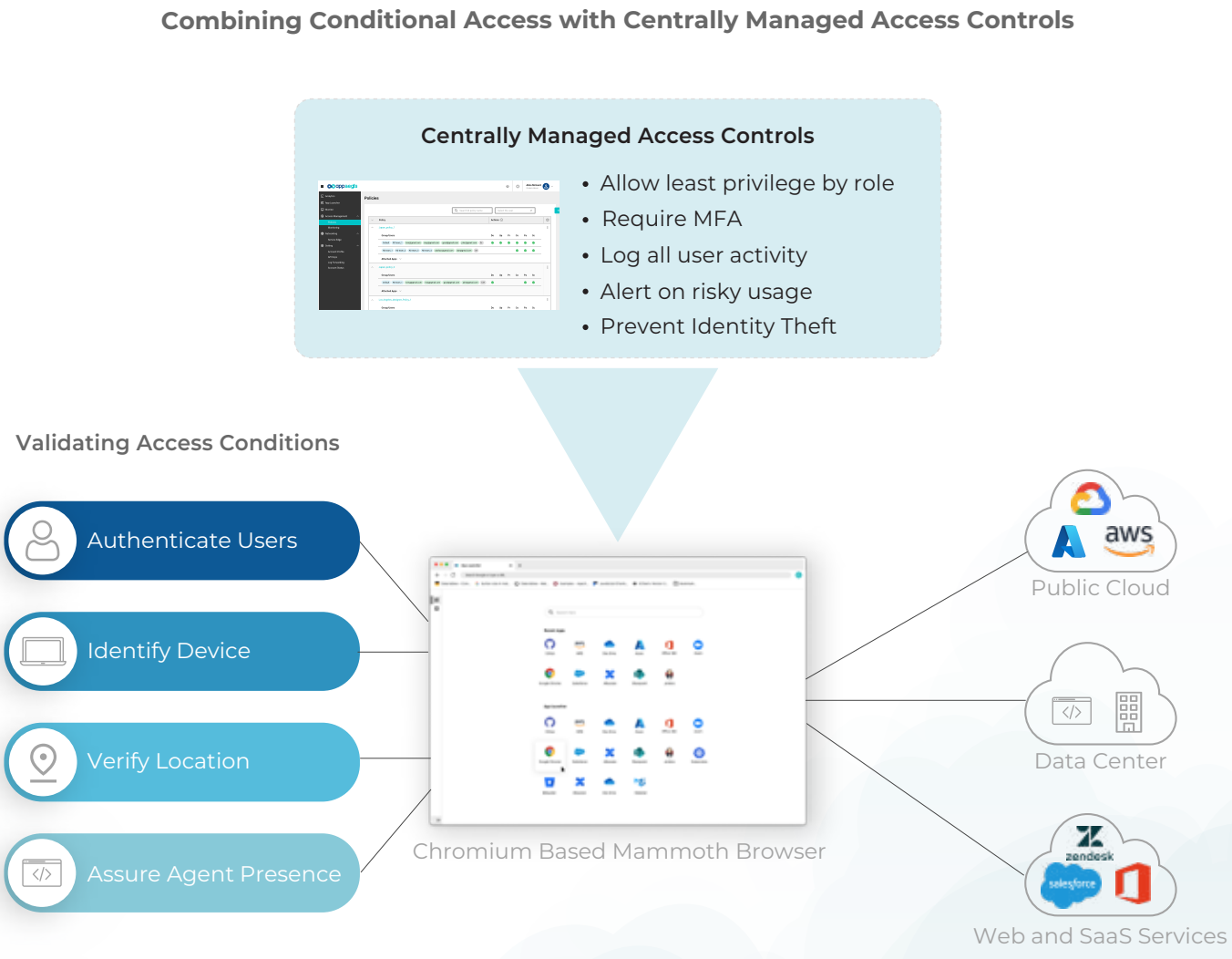

Figure 1. The centrally managed Enterprise Access Browser enforces zero-trust least privileged access to protect against unauthorized access and risky behavior

Deployment Simplicity

In order to accelerate and simplify Enterprise deployments, the EAB can be deployed in two different ways to fit a variety of 3rd party and remote access use cases. In deployments where the IT and Security teams have control over the devices that will be accessing corporate resources, the EAB can be downloaded to each endpoint, and functions not only as the browser, but also as the Mammoth agent. The single package simplifies deployment and maintenance. There is also an Appaegis mobile app for iOS and Android devices, covering access options for all kinds of remote workers.

In the case where the IT team does not have control of the endpoint, the Secure Portal Access (SPA) proves connectivity by running the EAB as software as a service in the cloud. Remote users just point the browser of their choice towards the SPA, and a secure connection is established providing all of the benefits of having the browser installed locally, without the need to dictate browser choice to a contractor or partner organization.

Whether connecting with the EAB loaded on the endpoint or via Secure Portal Access, the EAB solution is easily deployed in a few short steps. The first step is to connect the EAB to your Identity Provider (IdP) with a standardized SAML integration for user authorization. The next step is to configure application entitlements and policies in the EAB. While the implementation of this step is quite straight forward, determining the policies can require internal discussion to ensure consistent policies are deployed across the various 3rd party groups connecting to corporate resources. The third step in the deployment process is to add the EAB Service Edge into the data centers where any internal applications are running. This is a simple container with just a few configuration lines that can be deployed in minutes, creates a private link to the browser and doesn't require exposing any public IP addresses. The fourth and final step is to download the EAB onto the endpoint and connect to any required resources from web access to cloud infrastructure to internal applications. In the case where the Enterprise does not want to deploy the EAB to the endpoint, step 4 can be further simplified to just pointing any browser to the Secure Portal Access

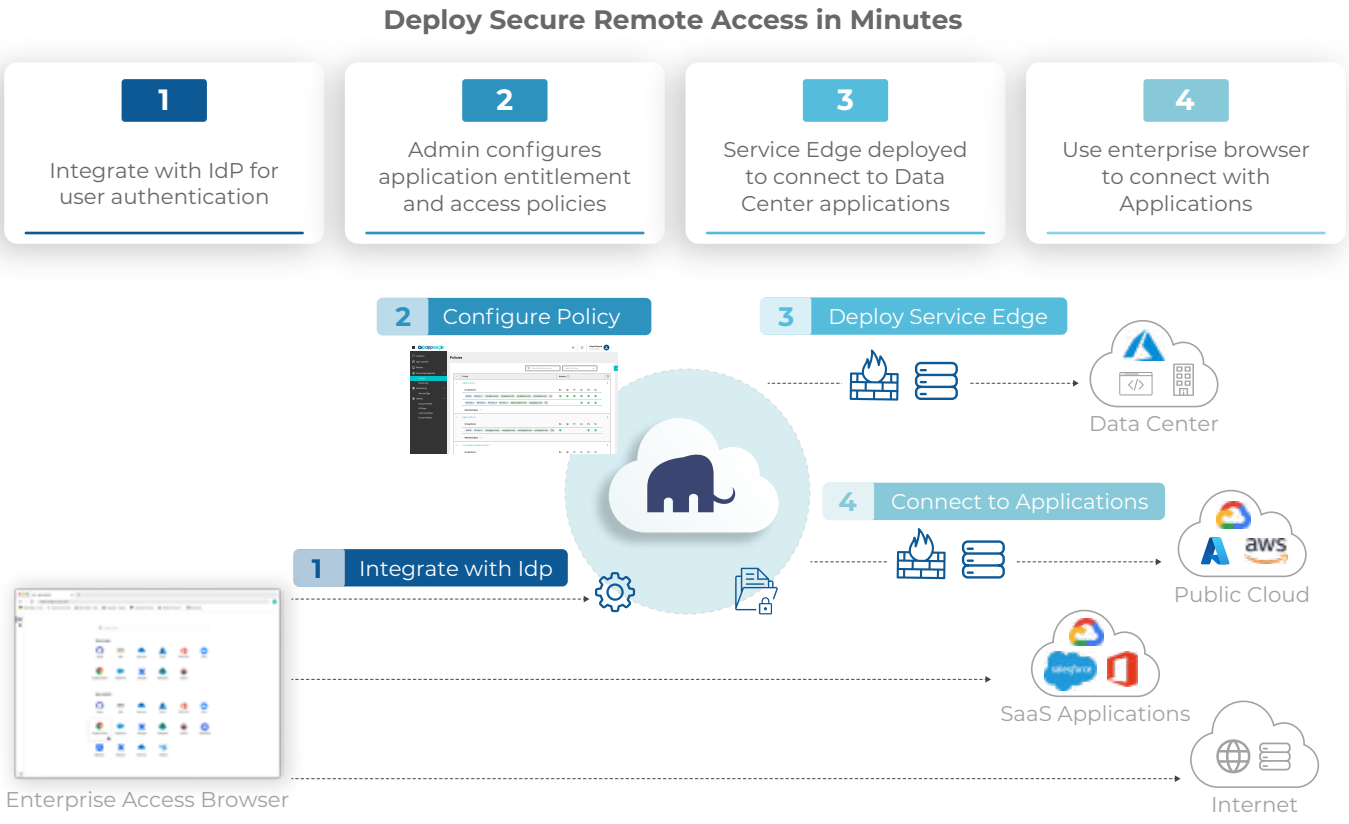

Figure 2. Deploying Secure Remote Access in 4 Simple Steps

Meeting Compliance Mandates

Data security and data privacy regulations are born from a need for data protection. As pointed out in the most recent Verizon DBIR, gaining access to a corporation's data remains a top target for attackers and will remain a top target for years to come. As a result, many business sectors are subject to meeting sector specific data security and data privacy regulations aimed at safeguarding the security of their customers' data.

To help companies meet these security and privacy regulations, the EAB provides both controls and visibility to audit and report on 'who accessed what data'. The EAB also provides strict controls with the role-based access policies needed to enforce least privileged access.

The combination of visibility and privileged access control in a single platform helps IT security teams enforce consistent and secure access to applications and data that fall under a regulatory requirements for audit access and role-based access controls.

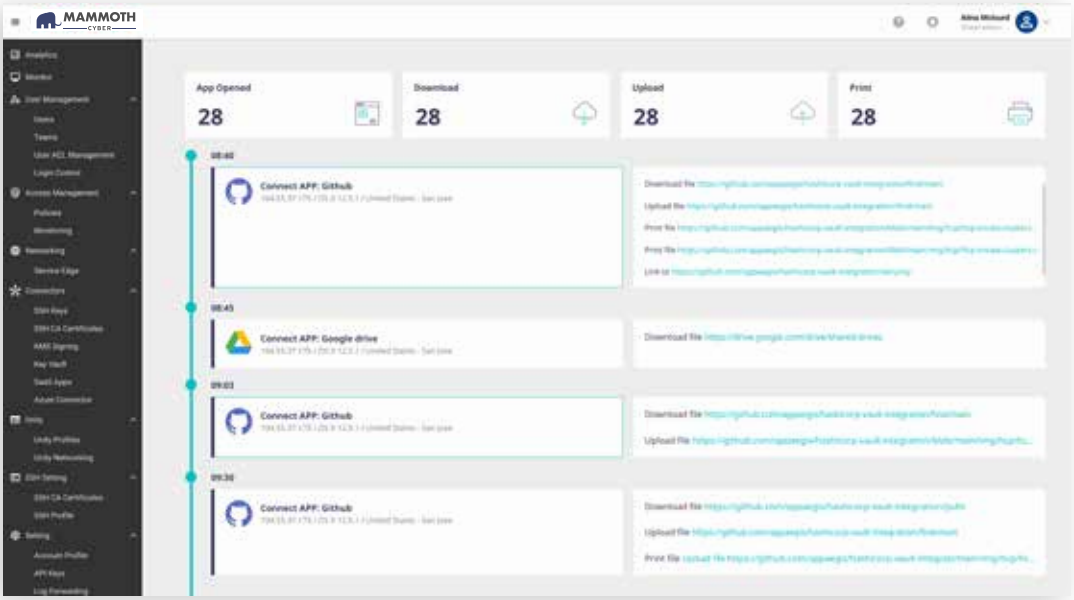

Figure 3. Logging user actions with the Enterprise Access Browser

User Experience

Employee productivity and efficiency are important for any business. When relying on a contracted workforce to manage critical aspects of the business, balancing digital security without impacting productivity becomes especially important.

Centralizing access and policy management onto an enterprise browser is designed to help IT security teams balance strict secure access while minimizing the impact to the end user. The EAB presents a familiar interface for users to access the applications and data they need to do their jobs. Access to both SaaS and internally hosted applications is seamless to the user, and they no longer need to toggle between multiple VPN and ZTNA clients to access different applications.

Managing access policy controls locally from the browser improves SaaS security without having to hairpin and redirect traffic to a central proxy. Additionally, the EAB can improve the user experience a step further by allowing users focused on dev and engineering roles to utilize their local environments for SSH, RDP, Git, Kubernetes and Database access.

Figure 4. Providing the ability for users to utilize their local environments for access with the EAB

Conclusion

There is every indication that Enterprises worldwide will continue to rely on contract workers and partner organizations to meet their staffing needs. These workers need access to corporate resources in order to do their jobs, and the challenge of connecting them with corporate resources in a simple, secure and manageable fashion will only increase in importance. The Enterprise Access Browser provides a new approach that overcomes the issues of traditional VPN and VDI implementations and should be considered as companies look to improve their security posture against increasingly common threats from compromised 3rd party contractors and partners.

Key Benefits of the Mammoth Enterprise Access Browser

- Improve security posture with complete control over 3rd party contractors and partners access and actions
- Drive compliance to industry mandates with visibility and audit logs for user behavior
- Enhance productivity and increase adoption with 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 Demo
+1 669 699 1122 · info@mammothcyber.com

MAMMOTH CYBER