MENLO SECURITY

# Everywhere Access:

## The Zero Trust Revolution for Hybrid Work

WHITE PAPER

As digital transformation progresses, employees are increasingly working remotely, accessing critical business applications and data from a variety of managed or unmanaged devices and locations. Third parties—partners, contractors, and others—need access to select applications, and the enterprise seldom has any control over their endpoints. Enterprises need to solve two overarching issues at once: they need to provide secure, seamless access to applications with fine-grained controls over these resources, all while mitigating the risks associated with such work.

Another aspect of digital transformation that's important to consider is that, as applications have moved to the cloud, they have become browser based. Browsers add an element of familiarity and ease of use, but they can also introduce risks. While browser-based applications offer the promise of reduced costs and increased agility, they can also result in a lack of visibility. Despite applying patches, deploying specific client software agents, and investing heavily in web security and app access governance, organizations may still struggle to achieve adequate visibility. That's because policies alone are insufficient without the ability to monitor and verify their effectiveness. Though you might see that someone accessed an application, you may not be able to discern their actions within it. Neither approach addresses the risks of stolen credentials or compromised devices.

The solution is a "secure by design" approach that enables everywhere access. Users need to securely access internal resources and SaaS applications from anywhere, anytime, and on any device. A secure-by-design solution must include zero trust access, the ability to continuously validate each access request, and minimize the risk of unauthorized access and data breaches, even if devices or networks themselves are compromised. Visibility into application access is vital to ensure, and demonstrate, that policies are working as intended.

### Access Without Visibility is not Secure

Menlo Secure Application Access enables discrete controls over user access to applications, rather than granting encrypted VPN tunnels, and avoids the visibility problems that VPNs and legacy ZTNA create. Menlo Browsing Forensics records user activity within the Menlo Secure Cloud Browser, including visited sites and actions. Forensics can be configured for specific users, BYOD users, or third parties, and it can be triggered by events, such as DLP alerts or phishing attempts.

### Combine Secure Application Access with Browsing Forensics to:

- Ensure zero trust architecture effectiveness, and monitor user behavior to verify that zero trust policies are being enforced.
- Track risky activities to identify potential threats like copy/paste or upload/download actions.
- Derive user intent with insights into user behavior that enable you to make informed decisions.

Browsing Forensics complements Secure Application Access by providing detailed visibility into user behavior. This visibility enables organizations to monitor user actions, verify policy compliance, and identify potential threats.

**Key benefits of everywhere access with zero trust security:**

- **Enhanced security –** Protects against unauthorized access and data breaches
- **Improved productivity –** Enables employees to work efficiently from anywhere using any device
- **Reduced costs –** Eliminates the need for costly VPN infrastructure and management
- **Enhanced user experience –** Provides a seamless and secure access experience

Menlo Secure Application Access provides comprehensive protection for applications and users by leveraging the Menlo Secure Cloud Browser. Menlo supports secure-by-design and zero trust access, shielding applications from compromised endpoints, vulnerable browsers, and malicious requests, while enabling everywhere access. Menlo Browsing Forensics completes the continuous improvement loop, with complete visibility into browsing sessions.

## The Big Challenges

A ten-thousand-foot view of application access challenges reveals issues that organizations of all sizes have been attempting to overcome for decades. The primary issues in enabling and securing access to needed applications include:

- The need for zero trust security that protects from misuse of privileges, while accounting for the browser as the primary access method
- The requirement to provide secure access from unmanaged devices that the enterprise does not control
- The desire to modernize access systems, including minimizing VDI and replacing VPNs

Each of these challenges poses unique problems, and most organizations have more than one of these scenarios in play.

CHALLENGE

## Zero Trust Must Go Beyond the Network

The concept of zero trust has been a goal for enterprises since it was introduced in 2010. Its basic tenets of continuous authentication and authorization along with the elimination of implicit trust were first adopted in the network, with good reason. After all, most applications lived in the network at that point, and the expectation that most users would be located on the network or, in limited situations, accessing apps by VPN, was reasonable at the time. Zero Trust Network Access (ZTNA) became a popular buzzword.

But then came digital transformation—applications moved to the cloud and remote work became the norm. Today, the concept of limiting zero trust to the network is irrelevant; enterprise apps aren’t there anymore, and neither are the users that must access them. Instead of relying on a perimeter-based model that trusts everything inside the network, today’s zero trust access assumes that nothing is inherently trustworthy, regardless of location. Users must be authenticated and authorized, and their access to applications must be limited to only the apps that are required to do their job, regardless of where they are.

The final missing element in a zero trust model is visibility. Without the ability to see—and, sometimes, prove—how controls are working, modifications can easily become reactionary and are only applied after something goes wrong.

CHALLENGE

## Providing Secure Access to Applications from Unmanaged Devices

The desire to provide application access to users working on unmanaged devices has been a goal of organizations ever since there were applications. Allowing employees to use their own laptop, tablet, or mobile device to access applications and data enables the business agility that organizations need. The ability to extend that same type of access to business partners, contractors, and other third parties adds still more benefit. Unfortunately, while the promise of enabling app access via unmanaged devices is clear, the limitations are equally obvious. They include threats to the application server and the data within it, as well as the very real risk of data loss and privacy breaches.

The fact that most applications are now accessible by browsers seems like it would simplify access, but in fact it does just the opposite, because browser traffic has historically been invisible to the majority of security tools. A lack of visibility into and control over unmanaged devices makes it virtually impossible to detect suspicious browser behavior or take measures to prevent a problem before it happens.

While the overarching issue of providing access to any type of unmanaged device is central to this challenge, there are also concerns for each user type that must be addressed.

## BYOD

Most conversations about user access via an unmanaged device begins with BYOD. Many enterprises have enabled some sort of BYOD policy, but there is always risk. While it is possible that an employee would limit the use of an enterprise-managed device to work only, there is no way to guarantee such restrictions would extend to devices t hat the user owns. A device like a home computer or laptop may well be shared with others whose activities are unknown. When devices are shared, or simply used for non-work activities, you have no way to know what the user (or users) are doing. They might visit risky websites, share information on social networks, download suspicious content, or access sketchy web-based applications. It can even be difficult to ascertain what browser is being used on the unmanaged endpoint and whether or not the browser has been updated regularly, particularly if the device is shared by others.

In order to realize the promise of BYOD, access solutions under consideration must make it easy to access applications and resources, while protecting enterprise apps and resources.

## Third Parties

This user category includes individual contractors and business partners, as well as more specialized groups, such as those on either side of a merger or acquisition scenario. Access for these users should be limited to only the applications required to perform their tasks. Specific controls when the user/group is using the app or accessing resources must also be specific and fine-grained. In order to safely enable third-party access, it is essential that any solution consider precisely what that group will require and allow nothing more. To make the solution practical, controls must be easy to apply and change with minimal disruption to other users.

### CHALLENGE

## Modernizing Legacy Access Systems

One of the key goals of an everywhere access strategy is to find a way to upgrade legacy access methods to better reflect user needs and the applications they use at work. Some examples of legacy systems include Virtual Desktop Infrastructure (VDI) and virtual private networks (VPNs), both of which reflect times when the majority of applications were located on the enterprise network. Such access does not reflect today's reality, where applications often live in the cloud and users could be anywhere. The most common access methods, VDI and VPNs, got a boost when the pandemic struck and organizations needed to act immediately, but as time has passed and digital transformation has marched on, these technologies have become increasingly removed from business realities.

## VDI

The concept of VDI was relatively simple; the enterprise managed and secured virtual desktops, while data was secured and stored on centralized servers. Unfortunately, the reality of VDI has proved to be far more complex. Servers are no longer centralized, and the task of maintaining and upgrading the hardware and software stack is burdensome for IT teams more focused on cloud management. Although there are still situations where VDI is the right choice, it no longer matches most organizations' current reality, due to factors including where applications are housed, the skills IT teams possess, or the experience that users expect.

Visibility poses another problem for VDI. The common security tools that are well understood by most SOC and IT teams just don't work in a VDI scenario. Centralized monitoring and log analysis tools are required, and frequently must be provided from VDI vendors themselves, raising costs and furthering vendor lock-in. Another component, originally designed to get around the slow response times for which VDI is notorious, is end-user monitoring tools. This adds yet another specialized tool that must be purchased, deployed, and maintained.

## VPNs

VPNs are another access method originating from the days when applications were housed in the enterprise network. VPNs give users the experience of being "on the network," and, in fact, they are. Unfortunately, most applications no longer live there.

Not only is the VPN user experience sub-par, as traffic goes into the network, up to the cloud, and back, the security risks are enormous as shown in the host of data breaches that have been traced back to VPNs. In some cases, breaches were the result of a user whose credentials had been stolen, or a device that had been compromised. A threat actor who was able to breach the VPN by stealing a user's credentials through a well-executed phishing campaign would suddenly have what was needed to access any business system without having to go through another authorization process. In other cases, incidents were traced back to vulnerabilities in the VPN technology, which attackers have been quick to exploit. And, because VPNs have to be network-facing to perform their function, they are also a target. Regardless of the specific issues, the central problem is built into how VPNs work; they were designed to connect users to the entire network, rather than a specific application.

The visibility problems posed by VPNs, while not as specialized as those found in VDI deployments, are still daunting. Investigations require time-consuming techniques like deep packet inspection, network flow analysis, or network log reviews to gain visibility into sessions.

## For True Zero Trust, Leave the Network Out of It

Forward-thinking organizations are evolving their cybersecurity strategies to focus more on browser security. Moving from broad-based network-level access control to browser-based access controls can reduce exposure and limit access to specific applications only. The reality of today's enterprise includes the fact that it is impossible to ensure the security of partner or contractor endpoints, and that it is likewise impossible to control all of a partner or contractor's actions. Controls based on device or network location simply don't figure into the issues any longer.

# The Solution

## Secure Application Access from Menlo Security

### The Antidote to Legacy Access Methods and Unmanaged Devices

When you deploy Menlo Secure Application Access, you provide vital protection to your applications from compromised endpoints, while protecting your users from infected traffic coming from application servers. Unlike traditional technologies that utilize complex infrastructure or give access to the entire network, Menlo Security provides access to only what's necessary, with policies for users, groups, source IPs, and geolocations.

Menlo Secure Application Access safeguards applications by using the Menlo Secure Cloud Browser to communicate with applications. Rather than accessing the origin server, users interact with the Menlo Secure Cloud Browser. This hardened remote browser creates a rendered representation of the application and delivers content to the endpoint device within the user's local browser. In addition to providing access, the combination of the local browser and the Secure Cloud Browser shields the user from content-based attacks. Unlike legacy access that was based around the network, the Menlo architecture also shields the application from malicious requests that might involve parameter tampering, web scraping, API abuse, and a host of other problems. This shielding is accomplished because the Menlo Cloud provides separation between the application and the endpoint, and all requests are inspected by

AI-driven protections within the Menlo Cloud. Even if the endpoint somehow gets compromised, a threat actor cannot get direct access to issue requests to the server. All application requests are executed from the Menlo Secure Cloud Browser rather than the endpoint browser.

To provide further protection for the valuable data enterprise apps hold, Menlo Secure Application Access offers additional fine-grained application controls. These controls, which can be used to protect intellectual property, help with data loss prevention, and more, include:

- Download/Upload
- Read-only/Read-write
- Watermarking of applications and documents
- Data redaction
- Copy/Paste

Secure access to applications can be delivered without an agent by using the browser or a browser extension. In the case of legacy applications that require a RDP or SSH connection, secure access is achieved using the Menlo Security Client for non-browser–based applications.

## Browsing Forensics from Menlo Security

### Essential Visibility to Enable Everywhere Access

A cybersecurity strategy focused on browser security enables your ecosystem of users to have secure access to the applications they need and nothing more. Menlo Browsing Forensics then completes the picture, with a detailed view of users' browser sessions and third-party actions, making it possible to ensure that access policies are working as intended. The combination delivers needed separation between endpoint and application and provides essential visibility into the user actions that have been almost impossible for security teams to gather in the past.

# The Takeaway

Operating in the modern world requires you to provide application and data access to users everywhere, on a range of unmanaged devices, at all times. The security controls of the past can no longer protect your organization from compromised devices or poor security practices. But a modern security solution can. Together, Menlo Secure Application Access coupled with Menlo Browser Forensics provide the security, control, and visibility you need to protect your organization from vulnerable legacy hardware, compromised endpoints and servers, insider threats, and third-party or supply-chain attacks.

The future of work is everywhere access, secure by design, and it's built on zero trust that starts in the browser. Follow your users and your apps beyond the networks that you own and control, with Menlo Security.

# 10 Questions to Ask About Zero Trust

### 1. Is zero trust tied to the network?

In today's landscape of remote work, cloud-based applications, and BYOD policies, the effectiveness of a zero trust solution is severely limited when it is tied to the network perimeter. To provide stronger security in today's dynamic environment, zero trust access must instead be based upon the user or group, the specific app users need to get to, and the precise level of access required in order to do their job. By prioritizing zero trust access, regardless of user location, organizations can ensure that access to specific resources is granted only to those with proper authorization. This significantly reduces the potential impact of security breaches.

### 2. Can the approach provide differentiated access to different users or groups? If yes, how difficult is it to make a change to those policies?

The ability to implement highly customizable controls is key to establishing a least-privileged access model. But because organizations are constantly changing, it's vital to have a centralized, straightforward management interface to ensure that the enterprise remains nimble. Security and IT teams need to be able to swiftly adapt access for new users, role changes, application additions, or emerging threats. The combination of strong security measures and streamlined management capabilities ensures that organizations can effectively safeguard sensitive data, while fostering productivity.

### 3. How are applications protected from malware on an endpoint?

Malware can infiltrate applications by exploiting vulnerabilities within the application itself or through its underlying operating system. Sophisticated threats can deceive users into installing malware through disguised files, malicious links, or even from compromised websites. Traditional security technologies often face challenges in preventing such infections, because the majority of these products were designed to monitor network traffic and identify known malware signatures. These defenses literally cannot "see" threats that are brought in via browser traffic. To combat this shortcoming, organizations should look for a technology that provides network separation, so that even if an endpoint is infected, it will never have direct access to the application.

### 4. Are data loss prevention controls available? If yes, what controls are available?

Data loss prevention features are crucial for secure access to enterprise applications to prevent sensitive data from leaving the organization's control. Data loss prevention controls you might want to consider include:

- Watermarking
- Data redaction
- Copy/Paste controls
- Read-only/Read-write web site controls
- Upload and download controls

## 5. If an intruder could gain an authorized user's device/credentials, what could this allow the intruder to do? Is lateral movement possible?

It's important to restrict access only to the specific applications that a user needs. These barriers within a system help prevent lateral movement because it limits the damage an intruder can cause after gaining initial access. Such controls must ensure that even if one application is compromised, the intruder would not gain access to the organization's entire network.

## 6. Are VPNs still being utilized? If yes, why?

Enterprises no longer need to connect users to their network to provide access to applications. The pandemic, which drove organizations to enable remote users to get to mission-critical apps, exposed many of the flaws in such legacy approaches. Because VPNs connect users to the entire network, rather than a specific application, a threat actor who was able to breach the VPN by copying a user's credentials or stealing their device would suddenly have what they need to access the entire enterprise network.

## 7. How long does it take you to review a user's actions?

Some access approaches lack the ability to track user activity within applications and often offer no centralized logging for comprehensive auditing. This makes it extremely difficult to view the necessary user activity for resolution.

## 8. How do security teams resolve potential insider threats? How many devices are involved? How much time does it take?

Resolving potential insider threats regarding application access typically involves extensive review of information across a multitude of platforms that were not designed to provide visibility into browser traffic. Unfortunately, such investigations often end with guesswork. Organizations need a solution that can easily provide the detailed visibility needed to ascertain user actions and intent, particularly in cases where a user is considered "risky."

## 9. How are audits of user access to applications handled?

Auditing users' application access has typically posed real problems for security, IT, and compliance teams because of the lack of visibility intrinsic in legacy network-based access technologies. A better solution incorporates visibility into browser traffic to enable workable security policies, ensure that these controls are working as they should, and provide the details required for investigations to be conducted without ambiguity.

### 10. How difficult is it to reconstruct a user's application access activities, including credentials used and assets viewed?

The answers to these questions lay bare the limitations of traditional access methods. In cases where a user is being investigated, time is of the essence, and guesswork cannot be tolerated.

## About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling zero trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.

MENLO SECURITY

Learn more: https://www.menlosecurity.com

Contact us: ask@menlosecurity.com