MENLO SECURITY

Solution Brief

Secure the way people work on Microsoft 365 and Google Workspace.

Make online work safe for your employees wherever business takes them.

The way we work is changing, making users more reliant than ever on cloud-based productivity suites.

Today, employees are working from home, in remote offices, and in customer sites, and they connect to each other through cloud-based productivity platforms that encourage collaboration with colleagues all over the world through email, file sharing, messaging, and productivity apps. Google Workspace (formerly G Suite) is a pioneer in this space, with millions of users worldwide using Google Drive, Google Docs, Google Chat, and other business apps every day. In addition, Microsoft 365 (formerly Office 365) is now used by one in five corporate employees globally, making it the most widely used cloud service by user count.

However, these platforms' hundreds of millions of business users are also hundreds of millions of potential targets for phishing and ransomware attacks. Malicious actors can easily spin up an authentic-looking email branded with a fake Google or Microsoft logo and send it to carefully vetted targets. These phishing emails often have malicious attachments that include code that infects the user's device when downloaded. The platforms themselves can be used as an attack vector as well, hosting malicious files that can be shared with unknowing targets.

Traditional cybersecurity solutions create gaps in security posture for distributed users.

Traditional cybersecurity solutions rely on a detect-and-respond approach to secure productivity suite access. These solutions use categorization, whitelists and blacklists, and real-time threat intelligence to make an allow-or-block decision at the point of click. Unfortunately, there's no way to identify legitimate from malicious requests originating from these trusted platforms, and network architecture and latency issues prevent the inspection and routing of all Microsoft 365 or Google Workspace traffic through a web proxy.

Complicating the problem is the fact that today's cloud applications are built for ubiquitous connectivity, which puts an enormous stress on traditional security infrastructure made up of the usual firewalls and proxies (such as secure web gateways). The increased traffic requires enterprises to scale by adding additional or bigger boxes—otherwise, performance for users greatly suffers.

This forces enterprises to make a choice. They can either block all Microsoft 365 or Google Workspace traffic, which would severely limit productivity and grind cloud transformation to a halt, or they can allow all traffic to flow unimpeded to users' devices. All too often, enterprises choose to allow Microsoft 365 or Google Workspace traffic to bypass their traditional security layers, such as a proxy, and connect directly to users. However, this approach eliminates a critical security barrier for attackers, allowing them to gain entry into the enterprise.

A modern approach to security: Zero Trust.

At the core of Zero Trust architectures is the idea that no traffic should be trusted. All browser-based Internet traffic should be treated as malicious, and web traffic should be isolated from endpoint devices. This approach is comprehensive and removes many issues associated with detection-based security. But until now, Zero Trust has typically required significant management overhead. Organizations would have to deploy and manage complex and expensive hardware or software clients at every point where a user's device connects to the Internet. This is simply unscalable in today's highly distributed world.

Benefits

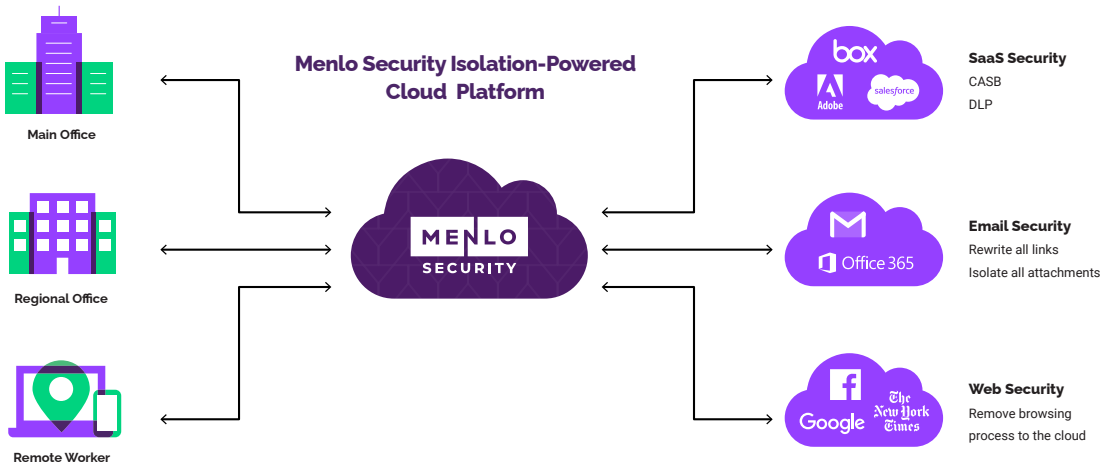
Take malware off the table as a threat to your employees.

Enable direct connections between users and the cloud productivity suite.

Create secure, low-latency connections globally to optimize user experience.

The Menlo Security innovation: An isolation-powered platform.

Menlo Security has taken the Zero Trust approach and made it a scalable, easily implemented solution through the Menlo Security Cloud Platform. Rather than forcing an allow-or-block decision at the point of click, the Menlo Security Platform powered by an Isolation Core™ provides a separate security layer in the cloud where malicious traffic is blocked while all other traffic is isolated far from the end user's device. It doesn't matter if the web content is good or bad, categorized or uncategorized. This isolation-powered platform assumes that everything is malicious and treats it accordingly. And because the platform is in the cloud, it's incredibly agile—scaling to be as large as an organization's cloud and accommodating fluctuating workforces, business cycles, or traffic volume.



The Menlo Security Platform allows users to freely click on any link in webmail or a Google or Microsoft 365 document, with no performance hit or possibility of infection.

The resulting traffic has no avenue for delivering malware to users' devices, and the isolation layer is delivered as a service through the cloud—essentially protecting users around the world no matter where or how they access the productivity platforms.

Solution Brief

Realize the transformational promises of the cloud.

Whether your organization relies on Google Workspace or Microsoft 365, users need reliable, safe, and secure access to business productivity tools wherever business takes them. Unfortunately, traditional detection-based approaches to cybersecurity are ill equipped to stop attackers who use these nearly ubiquitous platforms to breach systems. Instead, enterprises need to take a modern approach to securing work. The Menlo Security Platform powered by an Isolation Core™ enables a Zero Trust approach to securing work by preventing malware and other web-based attacks from using Microsoft 365 or Google Workspace to access the endpoint—and we do this without impacting the application experience.

Learn how Menlo Security is securing work. Visit menlosecurity.com or contact us at ask@menlosecurity.com.

MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.