Menlo Security

WHITE PAPER

Parting the Clouds

COVID-19 has handed CSOs a unique opportunity to embrace web isolation, and secure employee productivity

Change is in the air. Even before the pandemic it felt like history was happening faster. Now business, tech, and society all seem to be evolving at warp speed.

The acceleration of digital transformation under COVID-19 has handed CSOs significant challenges, but it's also opened the door to replacing outdated approaches to cybersecurity.

Today's vulnerabilities are driven by the spike in remote working, changing customer behaviour, and the complexity of cloud environments. Rather than return to default approaches or devise more workarounds, what's needed now is a re-think about traditional reliance on detect and prevent technologies.

When 81% of businesses say they've experienced a breach of some kind, cybersecurity has reached an inflexion point. Those ready to embrace change could emerge from the pandemic more secure than ever—but only if they're willing to change their mindset and adopt a fresh attitude to isolation.

80%

Businesses say they've experienced a breach of some kind.

Haven't I Heard This Before?

As a concept, isolation isn't new. But the technology behind today's solutions is. It promises to finally liberate corporate IT from outdated bromides like 'when it comes to breaches, it's not a matter of if but when.'

Traditional isolation technologies like virtual desktop infrastructure (VDI), application virtualization, and client virtualization attempt to protect users by stopping active content from being delivered to endpoints. They work in principle but the user experience (UX) they deliver is slow and sub-optimal.

With VDI and application virtualization, content is executed on separate computing infrastructure and then rendered pixel-by-pixel on an end-user's screen. Web pages load slowly, and there is a notable delay between taking an action (typing a character, clicking a link) and seeing the execution happen on-screen. Users often lose standard functions like printing pages or copying and pasting content.

[1] The Future of IT Network Security Report 2020, Menlo Security

Client virtualization requires dedicated endpoint software, OS changes, and a PC re-build which often creates instability. When it does operate as expected, significant resources are required from the user's machine.

At Menlo Security, our cloud-based platform isolates web content using our proprietary Isolation Core™ technology and offers businesses a 100%-safe way to view web and email content that doesn't diminish productivity or user experience.

It tackles major threats like phishing, ransomware, and malvertising head-on. It also secures corporate and personal email and makes it easier for companies to achieve compliance — all without reducing functionality or UX.

Let's consider what that means for a typical organization.

Stronger Protection for Remote Workers

A distributed workforce that conducts most of its daily work online has helped stabilize operations in a time of extreme disruption, but remote workers make cybersecurity harder to deliver. At least 70% of employees now use SaaS solutions and remote network access to connect devices to company networks.

70%

of employees now use SaaS solutions and remote network access to connect devices to company networks

Browser exploits can be a source of vulnerability, and they need to be regularly updated, patched and maintained. That can be difficult if users, devices, and IT teams are geographically separated.

To some extent, CSOs depend on users' willingness to follow the rules and treat their devices as if they could be breached at any time. Attempting to scale that expectation across the tens of thousands of endpoints that can exist in a large enterprise, makes the scope of the challenge clear. Any of those disparate devices can bring down the network.

Menlo Security Isolation Core™ enables safe remote working by ensuring that those cybersecurity policies stay with users wherever they log in—whether it's from home, the office, a customer site, or public Wi-Fi.

Menlo Security has extended its isolation core to a Cloud Security Platform that provides a separate and ubiquitous security layer in the cloud. All web and email traffic flows through it. Any malicious traffic is blocked while all other traffic is isolated far from the user's endpoint. Security teams can apply data protection and control traffic flows from a single platform.

That means even if there's a known or unknown vulnerability on the user's device, malware can't sneak in. Good or bad, it doesn't matter. No content is executed within the user's browsers.

The platform's Secure Web Gateway (SWG) capabilities include Cloud Access

Security Broker (CASB), Data Loss Prevention (DLP), Firewall as a Service, and Private Access. Together they support Menlo Security's ambition to make the internet safe and seamless for companies and users. Today it protects eight of the world's ten largest banks, four of the five largest credit-card issuers, and large US government agencies.

A Safe Space for Cloud and Digital Transformation

Shifting IT infrastructure and services to the cloud is an essential component of digital transformation. Still, it breaks the traditional hub-and-spoke network model that directs all internet traffic through a central security choke point. Under that architecture, end-users can log on to SaaS platforms and web apps from anywhere in the world, but the control point can become a bottleneck and cause latency issues.

The SaaS applications workers use can change over time, and that alters traffic patterns. Office 365 alone can create more than 20 persistent connections per user, overloading network hardware. The dips and spikes in traffic volume create unpredictable patterns that can overload cornerstone elements of the network security stack. On their own or in combination, these issues create application performance issues that degrade user experience.

Isolation eliminates these concerns by fundamentally changing how end-users are protected. Instead of creating traffic choke points, isolation executes web sessions away from employee endpoints and only delivers a rendered version of live content to devices.

> Isolation eliminates these concerns by fundamentally changing how end-users are protected. Instead of creating traffic choke points, isolation executes web sessions away from employee endpoints

This approach stops malware and other risks like lateral breaches by separating cybercriminals from users' devices—no matter what documents have been downloaded or which links have been clicked. Employees can use the internet without worry and have all the benefits of the cloud without posing an inside threat to the business.

That makes isolation a cloud and digital transformation enabler. It unblocks the real value of SaaS applications by enhancing traffic visibility and the application of security controls. Users can use cloud applications without worry because all web traffic is sent to Menlo Security's isolation platform, which guarantees protection.

Success Stories

More than 350 of the world's biggest corporations use Menlo Security's isolation platform every day to protect end-users and stop malware in its tracks.

A global financial services brand deployed Menlo Security's isolation core technology for its 100,000 plus users. Over a period of 180 days, close to 2,000 phishing links were clicked, 8,500 malicious websites were accessed, and only 30% of the clicks on those sites were categorized as safe.

Number of Malware Infections or Other Network Breaches: Zero.

A regional bank in the US with 2,000 employees and a billion dollars in annual revenue used network isolation to achieve 100% protection against web and email threats. Over a three-year period, it eliminated appliances and moved its security to the cloud. Network performance was improved by reducing VPN bandwidth.

Return on investment: 261%

A federal government agency in the US with 80,000 users saw significant improvement after just 30 days using Menlo Security's Cloud Security platform. File downloads to end-user devices reduced by 70%. VPN bandwidth was reduced by 50%

More than 8,000 malicious websites were visited—without causing malware infection or a breach.

Isolate and Liberate

Sector by sector, the changes brought on by COVID-19—new customer behaviour, a move to all-digital touchpoints, and a massive spike in home working — have propelled a rapid migration to digital.

The pandemic continues to change how we work and live, but cybersecurity isn't keeping up. Relying on traditional detect-and-respond strategies is loaded with risk, and simply unsuited to companies moving more of their critical systems and applications to the cloud.

We've reached a turning point in security, and it presents a unique opportunity to reconsider how networks, IP assets, and end-users are protected from an expanding array of cyber threats. Those who choose the right path could emerge more secure than ever before.

CSOs have a once-in-a-lifetime opportunity to challenge the things that have held them back in the past.

As digital transformation continues, isolation from Menlo Security can help them protect users' web browsing and email habits. As a result, employees can access web applications and SaaS services on any endpoint, from any location, without worrying about infecting the company network.

To learn more about the Menlo Security Cloud Platform powered by an Isolation Core™, visit menlosecurity.com or email ask@menlosecurity.com.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The company's Cloud Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Contact us

menlosecurity.com
(650) 695-0695
ask@menlosecurity.com