MENLO SECURITY

State of Browser Security:

Attacks Employ AI to Advance Beyond Phishing and Ransomware Delivery

REPORT

Table of **Contents**

State of Browser Security:

Attacks Employ AI to Advance Beyond Phishing and Ransomware Delivery

This report explores the current landscape of browser security threats, examining the latest attack vectors, vulnerabilities, and trends impacting organizations and users worldwide. Cybercriminals increasingly exploit browsers as the entry point, so enterprises must address these emerging risks. Advanced phishing, zero-day exploits, and data exfiltration through browser-based channels are increasing, and fraudulent Generative AI sites have emerged as a new threat. In this report, we analyze the evolution of browser-based attacks, evaluate protective technologies, such as browser isolation and AI-enhanced threat detection. This research provides actionable insights for strengthening defenses and using browser security to enable zero trust access and to govern the use of GenAI. Our aim is to equip security professionals with an understanding of modern threats against the browser and the tools necessary to build resilient defenses against them.

State of Browser Security:
Attacks Employ AI to Advance Beyond Phishing and Ransomware Delivery

The Macro Environment: A Growing Threat Landscape

The rise of AI-powered attacks, phishing-as-a-service (PhaaS), and zero-day vulnerabilities that focus on enterprise browsers have underscored the need for a new approach to browser security. Traditional network and endpoint security tools alone are no longer enough. Threats get through legacy defenses. Today, secure cloud browsing is crucial for businesses securing the modern workspace. Secure cloud browsing physically isolates and separates a user's browsing activity from the network to protect against browser-based threats without changing the user experience.

Over the last 12 months, Menlo Threat Intelligence has identified more than 752,000 browser-based phishing attacks spanning more than 800 enterprises, a 140 percent year-over-year increase. The rise of GenAI-generated threats has surged, with counterfeit websites masquerading as legitimate GenAI platforms to trick users. In the past year, Menlo Security has stopped hundreds of incidents where fake phishing sites used GenAI names to deceive and exploit unsuspecting victims. This shift in behavior towards the browser has solidified the browser as the focal point for business and personal activities and has caught the attention of cyber-criminals and nation-state actors alike.

Today, browsers are not just tools for web browsing and accessing enterprise applications – they have become the initial access point for sophisticated cyber-attacks, enabling adversaries to exploit vulnerabilities, steal sensitive data, and bypass traditional security controls.

Browser-based Attacks Persist Despite Massive Spending

Today's attackers are no longer relying on simple exploits. Instead, they are leveraging a combination of zero-day attacks, social engineering, and advanced phishing techniques to infiltrate systems and steal valuable data. More than 98% of attacks originate from Internet usage according to Gartner, with 80% of those targeting local, end user browsers. Common attack vectors included:

- Malicious Ads: Malvertising campaigns are exploiting popular websites and advertising networks to distribute malware and steal credentials.
- Browser-based Phishing: Browser-based phishing attacks – especially those leveraging evasive phishing techniques and business collaboration tools such as Slack or Teams – have become more convincing and harder to detect. Brand impersonation has been used at an accelerating rate in phishing attacks to deceive the user about a site's legitimacy.

- Exploitation of Browser Vulnerabilities: Exploiting zero-day flaws in major browsers, such as Chrome, Firefox, and Edge, remains a persistent threat. Heavyweight replacement browsers attempted to address the problem, but wound up offering minimal workspace capabilities and ultimately brought additional challenges around browser manageability and secure application access. They also fell far behind the leading browsers in updates and innovations.

By the second half of 2024, cybercriminals were creating nearly one million phishing sites per month — nearly 700% growth since 2020.

In 2024, browser security was subject to some of the most sophisticated cyber threats we've seen. As enterprises shift to remote work environments – relying on SaaS platforms, cloud-based applications, hybrid work environments, and BYOD policies – attackers trained their focus on the browser, relentlessly exploiting vulnerabilities and leveraging evasion techniques. Numerous high-profile browser-based attacks made headlines in 2024, accentuating the evolving threat landscape and the need for organizations to adopt a proactive approach to browser security. Some of these threats include:

***"0.0.0.0 Day" Vulnerability – The team at Oligo Security explains the 2024 "0.0.0.0 Day: Exploiting Localhost APIs From the Browser**. Researchers disclosed the latest vulnerability to all major browsers that enables external websites to communicate with, and potentially exploit, software that runs locally on MacOS and Linux. This "0.0.0.0 Day" vulnerability exposes a fundamental flaw in the way browsers handle network requests, granting malicious actors access to sensitive services and highlights the risk to local endpoint browsers.*

***In 2024, there was a notable rise in zero-day vulnerabilities affecting the Chrome and Edge browsers,** underscoring the growing sophistication of attackers targeting unpatched systems. Chrome experienced multiple high-severity exploits, including CVE-2024-7971, that allowed remote code execution. This vulnerability enabled attackers to access corporate networks and sensitive data before security patches were applied. Affected organizations experiencing downtime, data breaches, and costly recovery efforts.*

***Google Drawings and WhatsApp URL Shortener Phishing Attack:** Another noteworthy attack in 2024 involved a Google Drawings and WhatsApp URL redirect phishing scheme that tricked users into sharing their login credentials using an impersonated Amazon account verification link hosted on Google Drawings. What makes this attack particularly insidious is its reliance on the browser's inherent trust in established services to harvest login credentials. Masked as part of Google's own suite of tools, this phishing attack made it difficult for users to distinguish between a legitimate page and a fraudulent one.*

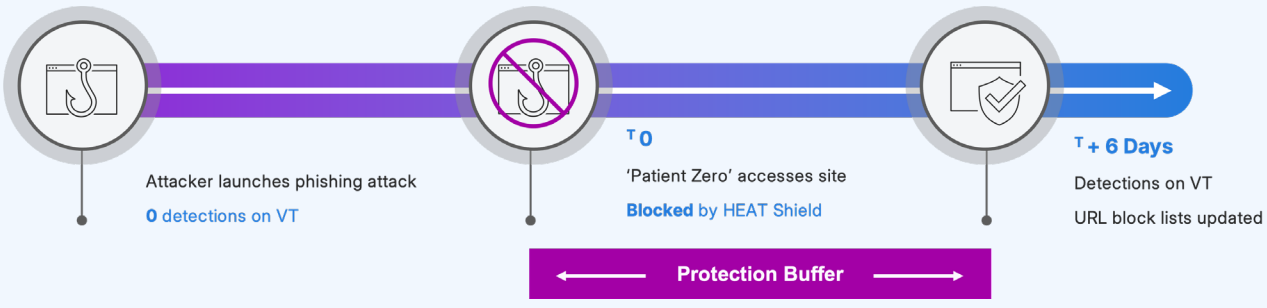
***Abuse of Cloudflare domains for phishing up 104 percent in 2024:** Just under 5,000 incidents of the Cloudflare Workers platform being misused for phishing were detected by the Fortra SEA team, up 104 percent, resulting in more than 500 attacks per month. Fortra warns about the increasing abuse of Cloudflare's pages.dev and workers.dev domains for phishing attacks. These platforms are attractive to cybercriminals because they offer free hosting, legitimate appearances, and the ability to bypass security filters. Attackers host phishing pages and malware on these domains, often redirecting users to fake login pages.*

Why Credential Phishing Continues to Threaten Enterprises

Credential phishing continued to run rampant targeting enterprises in 2024, largely because traditional security measures like firewalls, secure web gateways, and antivirus tools remain ineffective against these and other sophisticated techniques used by cybercriminals. While many enterprises have endeavored to improve browser security, they tend to focus on security at the network or endpoint level, which are not equipped to combat evasive threats.

Cloud-network services have attempted to address the problem, but they often add to complexity and come with high management costs without providing effective protection against advanced phishing attacks. Additionally, check-box solutions like traditional Remote Browser Isolation (RBI) have proven largely ineffective against evasive browser-based phishing attacks such as LURE attacks. These Legacy URL Reputation Evasion (LURE) attacks evade web filters that attempt to categorize domains based on implied trust. By compromising poorly secured websites, LURE attacks are used to gain entry to endpoints, delivering malware to further the attacker's goal to move laterally and deeper within organizations. Cybercriminals are also leveraging AI-powered techniques to increase their chances of bypassing traditional security layers, enabling them to enhance the scale at which they compromise poorly secured websites, create counterfeit sites, and embed malware in files that existing tools fail to detect. As a result, enterprises remain vulnerable to credential phishing, which continues to evade detection and prevention mechanisms.

6 days is the average window of exposure before legacy security tools can detect threats from zero-hour phishing attacks.



The Rise of Evasion Techniques to Gain Initial Access

In 2024, the state of browser security was characterized by an alarming 130 percent increase in zero-hour phishing attacks mounted against enterprises according to Menlo Threat Intelligence, with new tactics emerging regularly. These evasion techniques used for gaining initial access through the browser have become a significant cybersecurity concern. Cyber attackers are increasingly exploiting browser vulnerabilities, obfuscating malicious code, and employing evasion tactics, such as fileless malware and memory-only payloads, to bypass traditional defenses. These techniques often involve hiding malicious activity within seemingly legitimate web traffic, making detection more challenging. As enterprises adopt stronger endpoint security measures, threat actors are shifting focus to browser-based exploits, where subtle, evasive approaches can circumvent conventional security tools and enable a foothold for further compromise.

As of Q4 2024, the US, Taiwan, Japan, Singapore and South Korea were the top 5 most targeted countries by zero-hour phshing attacks.

The Rise of Brand Impersonation Logos in Phishing Attacks

The use of impersonated logos in phishing attacks targeting browsers has become a prevalent tactic for gaining initial access into enterprise networks. Cybercriminals are leveraging brand logos to craft convincing counterfeit websites that mimic legitimate business portals or services, tricking employees into divulging sensitive credentials or downloading malicious payloads.

According to Menlo Threat Intelligence, nearly 51 percent of browser-based phishing attacks employed some form of brand impersonation, with Microsoft as the number-one choice, to convince users that they are interacting with trusted organizations. This tactic significantly heightens the likelihood of successful exploitation, as users are more likely to trust a site that visually resembles a legitimate business.

Phishing attacks involving brand impersonation surged in 2024, according to Menlo Threat Intelligence, with Microsoft, Facebook and Netflix as the most impersonated brands across browser-based phishing attempts.

Insights from Menlo Security Threat Intelligence

In light of the incidents we've described, it is clear that the browser has become a prime target for cyber-criminals. Menlo Threat Intelligence has detected numerous cybercrime phishing campaigns that attempt to bypass traditional security controls, particularly those focused on browser-based threats.

Unlike the widespread use of "spray and pray" tactics of the past, these attacks are more refined, using evasive techniques to specifically target users through their browsers. The primary goals of these campaigns are to deliver ransomware and steal credentials. Notably, ransomware attacks, which often begin with phishing, can go undetected for five days or longer, allowing attackers to carry out malicious activities before traditional security systems respond. Menlo Threat Intelligence has observed a troubling trend over the past 12 months, with these threats evolving and showing no signs of slowing down, presenting a growing risk to organizations.

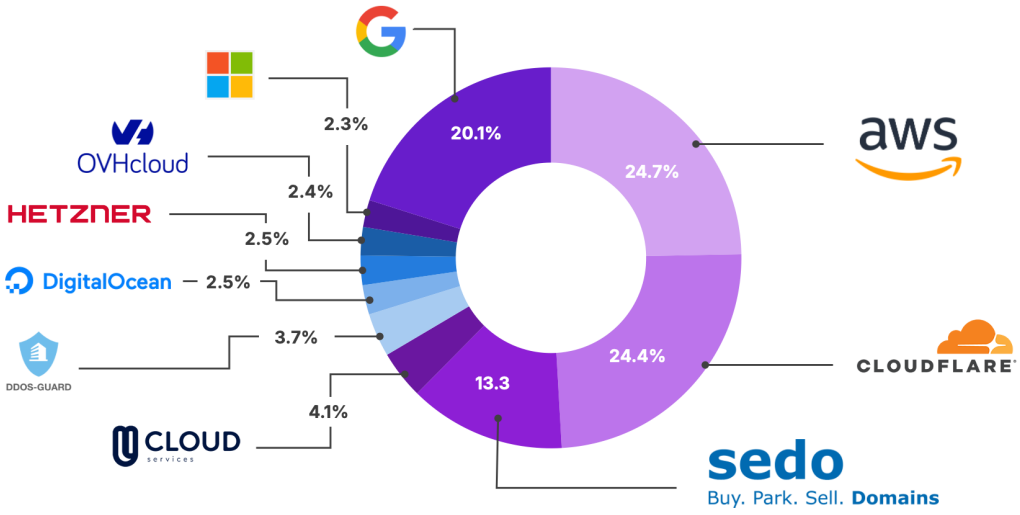
- Over the last 12 months, Menlo detected more than 752,500 browser-based phishing attacks
- This volume represents a nearly 140 percent year-over-year increase
- In 2024, one in five attacks displayed some form of evasive technique designed to evade traditional network and endpoint-based security controls
- Menlo Threat Intelligence identified more than 170,000 zero-hour phishing attacks mounted against Menlo customers over the last 12 months, a 130% increase from 2023
- Menlo identified Facebook, Microsoft, and Netflix as the top three impersonated brands in 2024
- GenAI threats have began to surge over the last year with nearly 600 incidents identified using GenAI names as imposter sites to manipulate and exploit unsuspecting victims

The Rise of Abusive Cloud Hosting Services

Notably, the rise of abusive cloud hosting services has become a major concern for enterprises, as cybercriminals are increasingly exploiting cloud services to host malicious content, such as phishing sites, ransomware, and command-and-control (C2) infrastructure.

Unlike traditional hosting services, cloud providers are less likely to monitor for illegal or harmful activities, making it easier for attackers to hide in plain sight. This is especially dangerous for enterprises, because these platforms can quickly scale, making it harder for traditional security measures to detect and mitigate threats. Abusive cloud services also offer anonymity and resilience, enabling attackers to rapidly deploy and move their operations, further complicating incident response and posing a significant risk to corporate data and network integrity.

Distribution of Abused Cloud Hosting



Vextrio: Evolving Malware Techniques

The Vextrio campaign highlights the growing sophistication of browser-based threats. It leverages the very infrastructure of the web – the advertising networks that we often trust – to infect users and gain a foothold into enterprise environments. The use of javascript code obfuscation techniques, combined with the integration of legitimate-looking ads, makes it difficult for traditional endpoint security solutions to detect and block these attacks.

Quick Facts

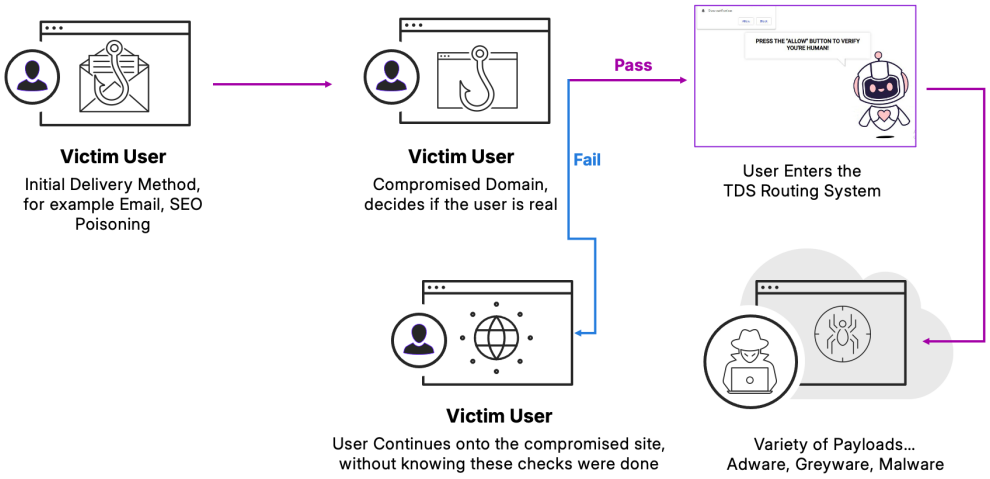
- Malicious TDS as-a-service
- Can lead to malware, backdoor, ads, greyware
- Infrastructure can rapidly change

Top Verticals Targeted

- All Industries

Techniques Employed

- TDS
- Compromising wordpress sites
- Social engineering



Open Water Phishing Campaign

In 2024, Menlo Threat Intelligence identified another campaign that utilizes CloudFlare services. This campaign uses a pre-built phishing kit with the tagline, "Powered by Jehova," and seems to have been in circulation for the last three years according to our analysis. Notably the C2 used with these campaigns seems to be open directories, exposing the stolen credentials and sometimes exposing the entire kit, which are often stored on the C2 infrastructure. Hosting services being abused is particularly dangerous as it allows operations to scale up quickly and cheaply, making the landscape more saturated with malicious domains and easier for attackers to increase their success rates. Secure cloud browsing solutions protect against evasive phish kits by leveraging AI-driven runtime analysis and real-time logo detection capabilities to isolate malicious content in a secure cloud environment, preventing brand impersonation tactics and providing dynamic security controls to protect users from credential theft and social engineering attacks.

Quick Facts

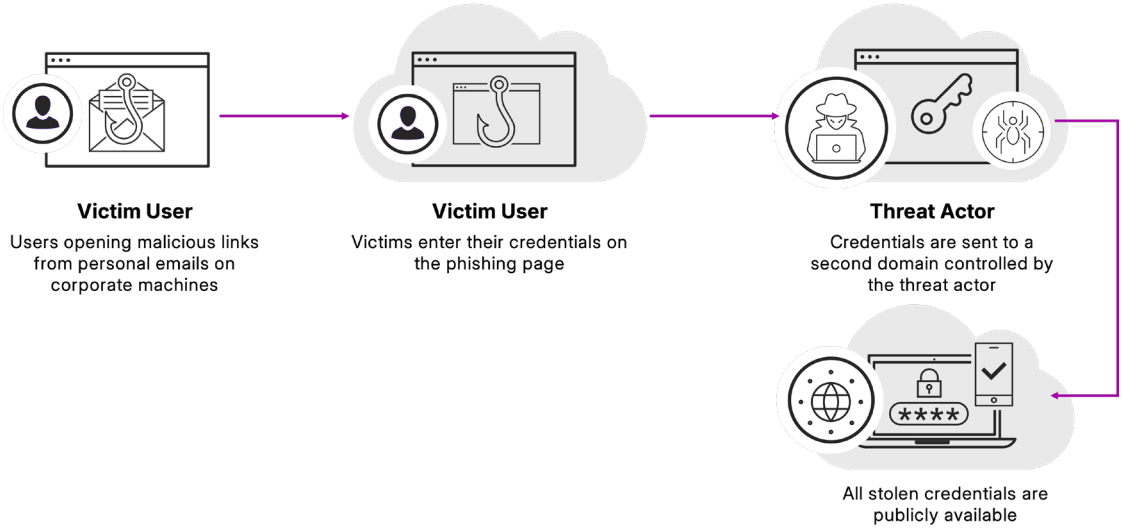
- Threat actor likely based in Vietnam
- Open directories often found on the same infrastructure contain stolen credentials

Top Verticals Targeted

- All Industries

Techniques Employed

- Hosting Services
- C2 communications
- Email C2 communications



Greatness 2FA Phish Kit

Menlo Threat Intelligence found and analyzed a phishing campaign that utilized a phishing kit called "Greatness." This kit is part of a Phishing-as-a-Service (PhaaS) infrastructure that is available for purchase via Telegram. The Greatness PhaaS includes email templates, C2 panel access, the kit, Telegram support, and other Telegram options.

PhaaS offers almost anyone the ability to conduct phishing campaigns and provides a layer of anonymity for the threat actor, as they don't need to set up infrastructure and can easily terminate a campaign. With secure cloud browsing, enterprises can isolate potentially malicious websites and email links away from the endpoint in a hardened digital twin of the local browser that resides in the cloud, preventing users from interacting with phishing pages designed to steal 2FA credentials and executing them in a safe, remote environment.

Quick Facts

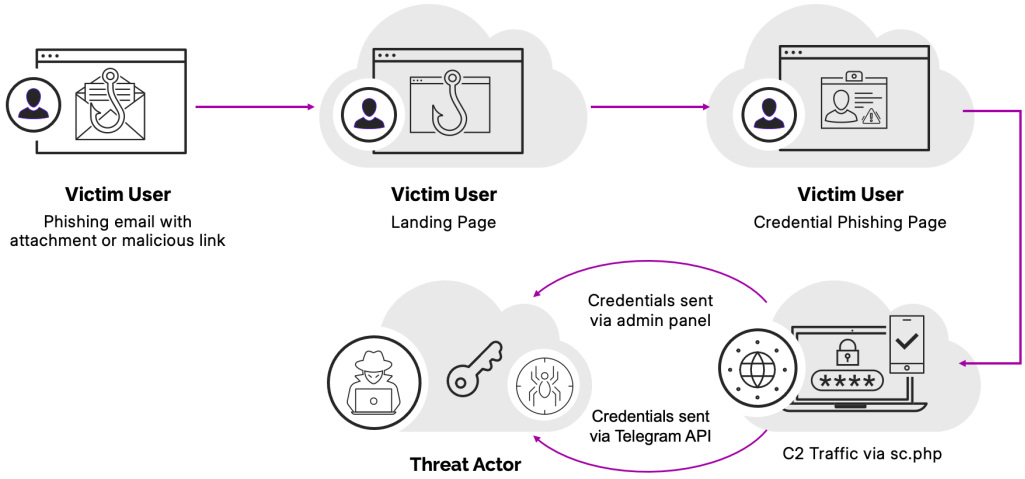
- Asks for a 2FA code
- Robust PhaaS offers

Top Verticals Targeted

- All Industries

Techniques Employed

- Anti-bot detection
- Telegram C2
- Admin panel
- Uses server side scripts



Looking Ahead: The Shifts That Will Define 2025

As we enter 2025, cybercriminals are expected to adopt more sophisticated and specialized tactics, with a focus on more targeted and impactful attacks. Anticipated trends include the rise of cybercrime groups and more elaborate PhaaS kits specializing in specific attack-chain segments, allowing for more precise and efficient exploitation. Cloud environments will become an even greater focal point for adversaries, as attackers target cloud-specific vulnerabilities amid the growing reliance on multiple cloud providers. Additionally, the proliferation of automated hacking tools on dark web marketplaces will expand, with browser-based phishing kits, and and Ransomware-as-a-Service(RaaS) becoming more prevelent.

The eruption of GenAI-created threats has also began to surge, with fraudulent websites posing as legitimate GenAI platforms to deceive users. In the past year alone, Menlo Security uncovered nearly 600 incidents where these imposter sites used GenAI names to manipulate and exploit unsuspecting victims. The integration of AI and large language models (LLMs) into these cybercrime services will further enhance the scale and automation of attacks, enabling cybercriminals to leverage sophisticated browser-based phishing techniques and automated social media reconnaissance for more effective phishing campaigns.

Top Five Predictions from Menlo Threat Intelligence as We Head into 2025:

1. Ransomware will Remain Prolific Targeting Critical Infrastructure to Extract Substantial Financial Gains

In the new year, cybercriminals will increasingly use browser-based attacks to deploy ransomware, targeting critical sectors like healthcare, energy, and transportation, bypassing traditional defenses. Phishing attacks, which have been the most common threat since 2019, will continue to grow in frequency and sophistication and continue to be used to gain entry to systems and user devices. Businesses will be confronted with multi-pronged attack strategies used to steal sensitive information, compromise internal systems, and exploit system or browser vulnerabilities for financial motives. The profound impact of ransomware attacks, like the major phishing campaign against Change Healthcare in 2024 highlights the need for organizations to prioritize browser security, adopt strong measures, and stay updated with the latest threat intelligence and business continuity protocols.

2. AI-driven Deepfakes and Exploitation of User Trust Will Continue to bypass Traditional Security tools

In 2025, AI-driven cyber fraud will rise, making it harder to distinguish between legitimate and malicious sites. AI-driven deepfakes impersonating trusted brands and individuals will fuel targeted phishing and credential theft, bypassing traditional security measures and exploiting unpatched vulnerabilities, risking widespread breaches unless enterprises adopt AI-driven defenses. Scam activities such as Fake AI tools used to offer premium AI services will be used to steal login credentials and personal data, or redirect users to phishing forms. Exploitation of user trust through sophisticated social engineering techniques will be key to targeting social media platforms and search engines. The integration of AI to enhance the success of these fraudulent and Fake AI sites is already proliferating across corporate devices.

3. Widening of the cyber gap across enterprises: Small businesses will remain vulnerable to attack, while larger businesses will continue to invest heavily in cybersecurity and AI

Over the next 12 months we will see a larger proportion of small businesses continue to be affected by ransomware and other browser-based threats due to their inability to effectively monitor user behavior and provide dynamic security controls in the browser. Larger enterprises will begin to incorporate browser security strategies and security tooling will start to incorporate more AI, helping with defenses that are cumbersome and leave too much room for human mistakes. Organizations will also start to leverage AI to level out their Security Operations Centers (SOCs), so that they don't need as many resources to run it. Regardless of size, browser security is no longer optional but a fundamental survival strategy requiring proactive protection and preventative security. CISOs will start to align security initiatives with business goals by adopting security products that balance ease of use with robust protection.

4. Growing Threats to Edge and IoT Devices

Another theme that we'll continue to see grow in 2025 will be Edge and Internet of Things (IoT) devices becoming prime targets for cybercriminals, particularly due to their often limited security measures and widespread use. The increasing deployment of these devices from smart cameras and wearables to home assistants, will likely result in more zero-day vulnerabilities being exploited in the wild. Threat actors will exploit these weaknesses to commandeer devices, using them for DDoS attacks and potentially other malicious activities. Additionally, devices in critical sectors such as healthcare (e.g., pacemakers, glucose monitors), industrial SCADA systems, and utilities will become increasingly attractive targets, as cybercriminals seek to exploit their vulnerabilities for profit, disruption, or espionage. This growing threat underscores the urgent need for improved security measures across all connected devices.

5. Remote and Hybrid Environments Will Exacerbate Insider Threat Risks

Lastly in 2025, we expect insider threats to increasingly originate from well-intentioned users who fall victim to sophisticated targeted attacks. The persistence of widespread remote and hybrid work environments will exacerbate this risk. To combat this emerging threat, new tools and technologies will emerge to assist users, removing the burden of identifying and mitigating potential risks on their own. These tools will detect malicious activity and operate far beyond the capacity of manual human analysis.

As we move further into 2025, it is clear that browser security will remain a critical area of focus for both security teams and end users. The landscape of cyber threats is shifting dramatically, driven by advancements in technology and changes in work environments. With cybercriminals and nation-state actors constantly refining their tactics, organizations must look to implementing robust security measures, prioritizing browser safety, and leveraging innovative tools to detect threats will be essential in mitigating these risks.

Secure cloud browsers, the next generation of remote browser isolation, work with leading local browsers to safeguard enterprise browsing, providing cloud-delivered security and addressing the core shortcomings of endpoint-centric approaches. Notably, secure cloud browsing mitigates the risk of evasive phishing attacks, browser vulnerabilities, and compromised devices, while improving user productivity through the continued use of familiar browsers and GenAI tools. By staying informed and adapting to emerging challenges using AI-driven threat prevention and secure cloud browsing solutions, businesses can better protect their data and maintain trust in an era where the line between reality and deception continues to blur.

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.

MENLO SECURITY

Learn more: https://www.menlosecurity.com
Contact us: ask@menlosecurity.com