

**THE BILLION-DOLLAR SECURITY BLANKET:**

# How Security Spending Overlooks the Biggest Risk of All

**silo**  
By Authentic8

## About the Author



---

### **MATT ASHBURN**

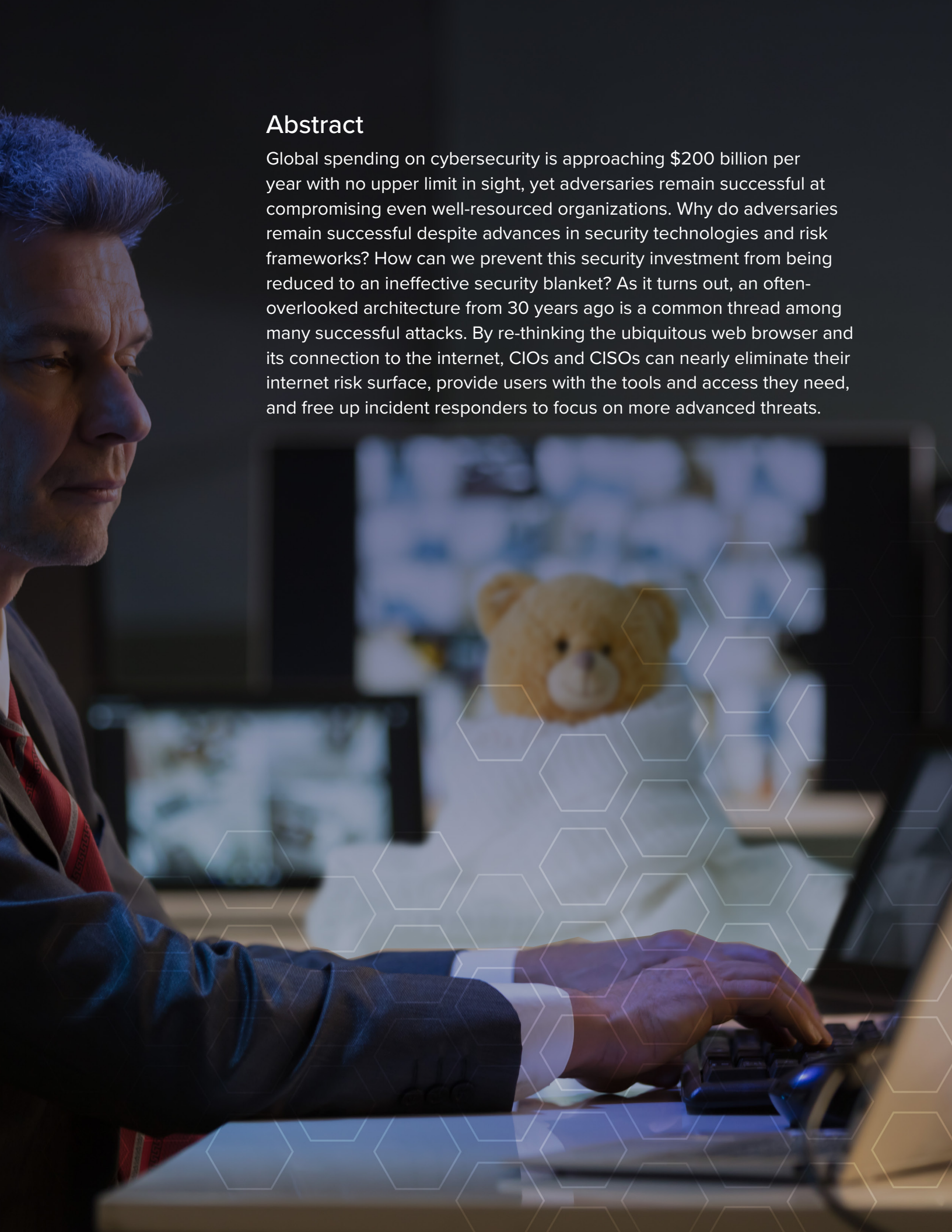
Former CIA Cyber Security Officer and National Security CISO at the White House,  
Head of Strategic Initiatives for Authentic8

---

Matt Ashburn serves as the Head of Strategic Initiatives, focusing on strategy and engagement with national security customers at Authentic8. Previously, Matt served as a CIA officer focusing on cyber issues, including a detail serving on the National Security Council as the Chief Information Security Officer and Special Advisor to the National Security Advisor, leading technical expertise, risk reduction strategies, and policy for national security systems.

At the CIA, Matt led the technical direction and coordination to stand up an innovative, unified cybersecurity operations center to fully harness agency authorities, resources, and talents to prevent and respond to advanced cyber threats. He also led the detection watch floor of CIA's cyber incident response team and has been recognized with a national intelligence award and service ribbon from the Director of National Intelligence and the IC CIO Partnership Award.

Prior to CIA, Matt gained over ten years of government and private sector experience, focusing on intelligence matters and cybersecurity initiatives at federal agencies and a major financial institution. He holds a B.S. in Electrical Engineering from the University of Virginia and is a graduate of the FBI's Intelligence Basic Course at Quantico, VA. Matt splits his time between Washington, DC and Puerto Rico, and volunteers as a sworn reserve police officer with D.C. Metropolitan Police.

A man in a dark suit and red tie is shown in profile, focused on his work at a computer. His hands are on a keyboard. In the background, a teddy bear sits on a desk, and a computer monitor displays a grid of hexagonal patterns. The scene is dimly lit, with a blueish tint, suggesting a late evening or night office environment.

## Abstract

Global spending on cybersecurity is approaching \$200 billion per year with no upper limit in sight, yet adversaries remain successful at compromising even well-resourced organizations. Why do adversaries remain successful despite advances in security technologies and risk frameworks? How can we prevent this security investment from being reduced to an ineffective security blanket? As it turns out, an often-overlooked architecture from 30 years ago is a common thread among many successful attacks. By re-thinking the ubiquitous web browser and its connection to the internet, CIOs and CISOs can nearly eliminate their internet risk surface, provide users with the tools and access they need, and free up incident responders to focus on more advanced threats.

## Persistent Threats Remain Persistent

No matter what cybersecurity defenses organizations put up, it seems that attackers remain capable – and often successful – at penetrating even the most secure barriers. When I first attended the DEFCON hacker convention in 2003, I was amazed to see hundreds of people from around the world, eagerly sharing information about the latest vulnerabilities and attack methods.

At the time, intrusion detection methods were all the rage, so attendees spent their days debating how to identify novel intrusions (or evade discovery, if you were a hacker). The latest security architectures promised fool-proof intrusion detection and prevention in concert with network firewalls – forming a secure perimeter, which would be difficult to breach, compared to open and accessible networks from a few years prior.

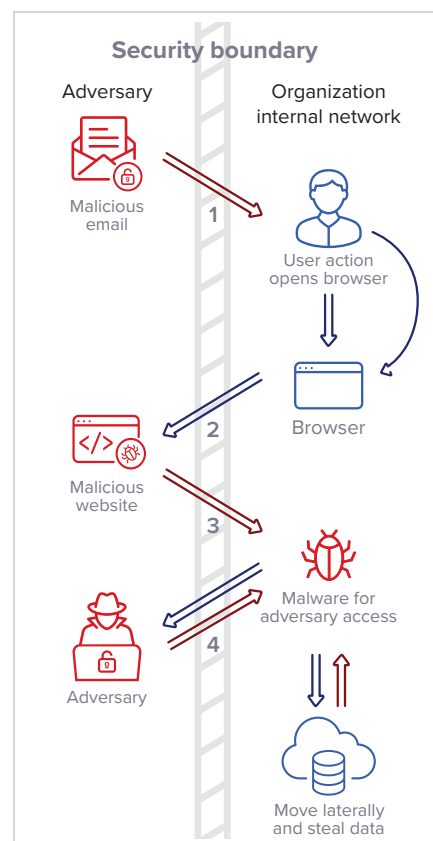
But then a talk by Roelof Temmingh of SensePost<sup>1</sup> presented a novel attack method that worked despite the latest in perimeter defense. His talk focused on using social engineering to trick a targeted user into downloading malicious content from a link embedded in an e-mail. As an attacker, why spend resources attempting to breach a well-guarded perimeter when you could trick the user into opening and downloading malicious code for you? The success of this method surprised and intrigued the audience. “It’s much, much easier than you think,” reassured the presenter, “if you use the correct language.”

Of course, it made sense! After all, critical infrastructure and sensitive data reside on the inside of the network—accessible, by design, from workstations by all authorized users. In Temmingh’s test group of 13 e-mail recipients at a bank, eight clicked a link to download a malicious file, which masqueraded as a screensaver, and one person executed it three times in a row.

The general method of attack really hasn’t changed in 17 years and follows the same ever-successful blueprint now familiar to many security practitioners:

1. Acquire a list of e-mail addresses for a targeted organization, send a convincing message with a sense of urgency, and implore recipients to click on a link or attachment
2. Once a user opens the attachment or clicks on the link, the web browser uses the internet connection to connect to a site hosting malicious code.
3. The malicious code travels across the organization’s security boundary to exploit a vulnerability in the web browser or other local software to install a method of persistence and remote access.
4. Move laterally throughout the network to gain additional access and modify, steal, or destroy information. Exfiltrate information of value via the workstation’s internet connection.

Today, these attacks are far from novel. Every CIO and CISO is aware of the threat posed by highly targeted and coordinated social engineering—a tactic commonly used by nation-state actors to gain initial access for data theft and other attacks. Such actors are typically known as Advanced Persistent Threats (APTs) and have gained much attention from cybersecurity researchers. While their initial attack blueprint has not changed significantly, they usually employ novel exploits, escalation, and lateral movement to evade the latest defenses and remain undetected in targeted organizations.



<sup>1</sup> [https://www.youtube.com/watch?v=VG\\_1G1BiMRU](https://www.youtube.com/watch?v=VG_1G1BiMRU)

In a PricewaterhouseCoopers survey of more than 9,700 persons, including C-suite executives and IT directors, respondents indicated that APTs were the fastest-growing category of malicious incidents as of 2015<sup>2</sup>. In the short time since numerous organizations have fallen victim to internet-enabled nation-state attacks. Prominent examples include the North Korean-attributed WannaCry ransomware attacks<sup>3</sup>, Russian-attributed NetPetya attacks crippling companies worldwide<sup>4</sup>, and the more recent China-attributed compromise of COVID-19 research organizations<sup>5</sup>. CISOs and CIOs are in the unenviable position of providing web browsing access for users who are targeted by adversaries with nearly unlimited resources and patience.

E-mail-based social engineering attacks, unfortunately, remain the number-one initial vector for malware attacks<sup>6</sup>. Why do such attacks continue to plague organizations despite countless training sessions on security awareness and a full stack of advanced security solutions? The answer is surprisingly simple, but let's first start with where we are and how we got here.

## Spending is Rising; Solutions are Plentiful

In a best effort to head off capable adversaries, organizations are increasingly embedding cybersecurity into business processes, rather than being an afterthought. Governments continue to introduce new compliance and regulatory requirements – a seemingly endless list of acronyms like CMMC, PCI, FISMA/NIST, GDPR, CCPA, and SOX – mandating companies and government agencies to implement additional security and privacy safeguards. The mindset of C-suite executives has shifted from “if a breach happens” to “when a breach happens.” They are increasingly aware of the dangers – from common ransomware attacks to highly targeted, well-funded campaigns meticulously executed by state-sponsored adversaries.

CIOs and CISOs need solutions that both protect their assets from compromise and enable rapid response and remediation when a breach occurs.

No longer can a castle's moat consist solely of antivirus software, intrusion detection, and firewalls. Meeting the demand, vendors have introduced a seemingly unlimited number of cybersecurity solutions to the market. Today, hundreds of vendors hawk various panaceas, each promising protection against nearly any threat. Large organizations now have the benefit (and challenge) of orchestrating a dizzying multi-vendor amalgamation of tools: secure web and e-mail gateways, malware detonation/sandbox appliances, identity and access control applications, patch and vulnerability management solutions, endpoint security, network analytics, in-line decryption, data loss prevention, cyber threat intelligence, artificial intelligence, machine learning, data science, security brokers, user behavior analytics, and so much more.

Thanks in part to these security advancements, annual spending for cybersecurity is estimated to be \$173 billion globally for the year 2020, and projected to grow to \$270 billion by the year 2026<sup>7</sup>. And the average cost of data breaches has more than doubled in recent years, from \$3.54 Million in 2006 to \$8.19 Million in 2019<sup>8</sup>. Despite the ever-increasing spending and attention on cyber defense, U.S. government analysis estimates that the impact of malicious cyber activity continues to grow, now costing the global economy over \$100 billion per year<sup>9</sup>.

---

<sup>2</sup> <https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>

<sup>3</sup> <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>

<sup>4</sup> <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>

<sup>5</sup> <https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion>

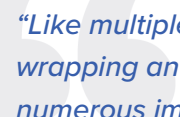
<sup>6</sup> <https://www.ibm.com/security/data-breach/threat-intelligence>

<sup>7</sup> <https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1>

<sup>8</sup> [https://www.ibm.com/downloads/cas/ZBZLY7KL?\\_ga=2.181209767.1686129232.1586105132-321662522.1584074488](https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.181209767.1686129232.1586105132-321662522.1584074488)

<sup>9</sup> <https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>

Organizations have dutifully added layer after layer of security capabilities over the years in response to evolving threats. However, many fail to receive a full return on investment and struggle to integrate, monitor, and maintain multiple technologies to form a cohesive, integrated defense. Like multiple security blankets wrapping an organization, numerous immature solutions can promote a feeling of security without actually preventing advanced persistent threats, ransomware, or other web-based malicious code. As anyone who has worked on a busy SOC floor can attest, network defenders spend considerable time detecting and responding to these incidents despite many layers ostensibly providing defense-in-depth.



*“Like multiple security blankets wrapping an organization, numerous immature solutions can promote a feeling of security without actually preventing advanced persistent threats, ransomware, or other web-based malicious code”*

CISOs and CIOs commonly face competing priorities, unexpected operating and maintenance costs, difficulty integrating solutions from multiple vendors, and budget constraints – while still being held accountable for inevitable security incidents. CIOs and CISOs must prioritize security investment to achieve the best possible risk reduction while considering business needs, cost, and other factors. It’s a stressful position to be in, and these pressures can often lead to fatigue in even the most experienced cybersecurity professionals.

## Evolving Risk Frameworks: from Checklists to Zero Trust

A decade ago, compliance consisted mostly of a checklist of security measures based on some combination of assessed risk and sensitivities of a particular computer system. To achieve a higher return on their security investment, organizations understandably prioritized critical controls that would provide the most risk reduction. Commonly, organizations focused on hardware/software inventories, vulnerability management, security awareness training, configuration management, and comprehensive programs for access control, incident response, audit, monitoring, data loss prevention, plus a few others. To this day, these steps remain the cornerstones of nearly any information security program, regardless of industry or governing security guidance.

Advancement of new frameworks has helped reframe the conversation around risk and mitigations, including zero trust models for security architecture<sup>10</sup> and the MITRE ATT&CK<sup>®</sup> knowledge base<sup>11</sup> of adversary techniques and tradecraft. Both have helped evolve and mature security mindset and deliver excellent value by placing additional emphasis on security gaps that create the highest risk of compromise. These evolving technologies, controls, processes, and concepts are undoubtedly helping advance cybersecurity. But few organizations today have sufficient experience and resources to achieve full maturity and thus remain vulnerable to attacks, which keeps even the most stoic CIOs and CISOs up at night.

Highly mature (and typically well-funded) organizations also may intertwine policies and processes to embed security best practices in everyday IT operations, balancing user needs with risk and cost. For example, a request for new software may kick off a series of events: requirement validation, market survey, security reviews, deliberate software selection, and secure configuration. This process maturity ensures patching, inventory, auditing, and monitoring of the software throughout its lifecycle.

<sup>10</sup> <https://www.beyondcorp.com/>

<sup>11</sup> <https://attack.mitre.org/>

Unfortunately, most frameworks, processes, and tools address the symptoms of the issue rather than the root, especially when it comes to the most common initial attack vector.

## Snipping a 30-year-old Common Thread

If we think of the ever-growing suite of immature cybersecurity products as a potential security blanket, the web browser can be considered a stray thread. When tugged slightly by an attacker, it can unravel and dissolve the security blanket to reveal an organization's sensitive data to outside persons.

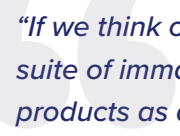
Nearly all successful data breaches, ransomware, and other compromises require two things, both of which abuse the connection from the user's workstation to the internet:

1. The ability to download malicious code to a workstation inside the target's network, and
2. A means of communication from the internal network back to the adversary, who can instruct the malware to perform additional functions, including data theft and further lateral compromise

Organizations invest in securing both the endpoint devices and the network perimeter to allow end-user devices to connect to the internet (so users can do their work) while hoping to detect and prevent abuse that would enable a breach to occur. Securing every endpoint is not cheap: licensing, personnel, monitoring, and maintenance costs can quickly become overwhelming, and, as attacks continue to demonstrate, this approach is hardly 100 percent effective.

Data released by the Cybersecurity and Infrastructure Security Agency (CISA) in May 2020 revealed the top ten vulnerabilities exploited by adversaries from 2016-2019<sup>12</sup>, and the findings are frightening. In addition to common vulnerabilities in browsers and plugins such as Adobe Flash, the vulnerabilities used most frequently across state-sponsored cyber actors from China, Iran, North Korea, and Russia are related to OLE technology in Microsoft software. Adversaries successfully exploit these vulnerabilities using malicious code downloaded from the internet, passing through many layers of security solutions before reaching the vulnerable workstation. Patching can partially mitigate risk, but will always remain a challenge and does not prevent zero-day exploits for which no patch exists. These successful nation-state intrusions are also symptomatic of a different problem.

Despite knowing that threats often abuse the browser connection, security professionals often overlook the actual architecture of web browsing. While content types have evolved, the process used by web browsers has not significantly changed since Tim Berners-Lee first created the concept of a web server and browser 30 years ago.



*“If we think of the ever-growing suite of immature cybersecurity products as a potential security blanket, the web browser can be considered a stray thread... it can unravel and dissolve the security blanket to reveal an organization's sensitive data”*

---

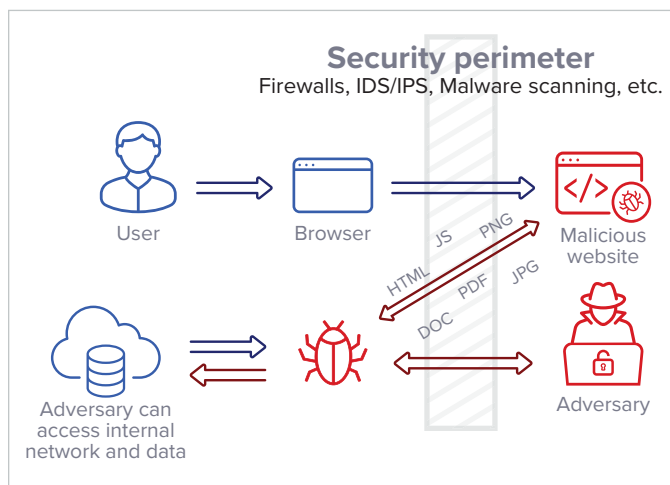
<sup>12</sup> <https://us-cert.cisa.gov/ncas/alerts/aa20-133a#:~:text=U.S.%20Government%20reporting%20has%20identified,and%20CVE%2D2018%2D7600>.

A typical web session looks something like this:

- A user opens a web browser on a workstation with access to both the internet and the organization’s internal network.
- Upon the user’s request, the browser connects to a specified website and requests content, downloading it to the local computer.
- The browser then processes the data downloaded, interprets it, and renders it on the screen.
- If the content downloaded contains malicious code, the browser processes it or passes it along to a vulnerable application. An attacker can gain access to the browser’s workstation, which in turn gives it access to the organization’s network.

### Traditional Browsers

*Untrusted Web Content Transferred Across Security Perimeter*



Essentially, this dated architecture allows traditional web browsers to download, process, and render untrusted data inside the very networks they are so diligently trying to protect. And browsers don’t have the most robust security track record, requiring regular updates for vulnerabilities.

In a stark deviation from the careful selection process other software, the browser often is not deliberately selected at all – despite being both ubiquitous and vulnerable. Unfortunately, many organizations simply accept and use the browser pre-installed with their operating system or select another freely-available browser based on user preferences.

How do we compensate for this risk?

## Adopt a Zero Trust Stance to the Web Browser: Fully Isolate it!

Given that skilled adversaries abuse a locally-installed browser’s dual connection to the internet and internal network, the solution is simple: move the browser from inside your network to the outside of your security boundary. This new architecture allows us to externalize the risk of user access to the internet while maintaining audit capability and control over the information.

The concept is relatively simple: instead of a web browser downloading untrusted internet content to a workstation inside the trusted internal network, a cloud-based browser located safely outside the security perimeter provides a seamless user experience without the risk.

This is what Authentic8 has done with its Silo Web Isolation Platform.

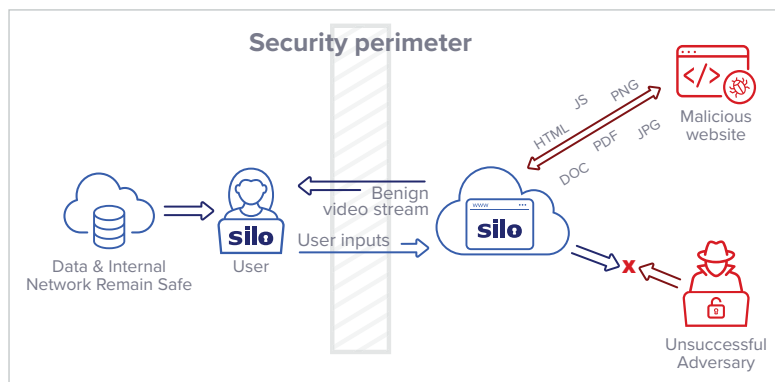
*“In a stark deviation from the careful selection process used for other software, the most prevalent and vulnerable software may not be carefully selected.”*



When organizations use the Silo cloud browser, untrusted web content is rendered safely by a browser within a secure cloud-based container, with the end-user viewing the session remotely. The workstation only receives a harmless video and audio stream of the cloud browser session, preventing malicious code from infecting the user’s local workstation. The user can still view, interact with, and process web content using a familiar interface; however, it is in a completely safe manner that isolates the untrusted web from the trusted internal organization network.

### With Silo Web Isolation Platform

*Untrusted Internet Content Remains Outside*



## The Browser Becomes an Integrated Enterprise Application

Remote browser isolation is excellent for preventing malware, but virtualization and container technology are insufficient by themselves. A modern architecture isolates the trusted from the untrusted, but it should also re-frame the browser as a fully-integrated enterprise application. Fortunately, the Silo platform shifts the browser from a critical vulnerability to a center of administrative governance and control. In addition to secure web browsing, Silo enables enhanced auditing, data loss prevention, and integration with other enterprise security investments:

- **Whitelisting of web content:** Many organizations have a security operations center, but even the most capable cybersecurity professionals can be overwhelmed by the large volume of internet-based malware, suspicious web traffic, and general noise. Using Authentic8 Silo, organizations can enable access to internal web resources via their standard browser of choice, while routing requests for untrusted external content through the remote Silo browser container – seamlessly and without degrading the user experience. Security teams can block all external web connections other than those to the cloud browser, effectively denying all but trusted relationships. Relief from web-based attacks offers tremendous benefit to SOC teams, which recoup time and resources that can instead be used to hunt malicious insiders, supply chain attacks, and other advanced threats.
- **Enhanced auditing:** Even though the remote browser session sits outside of an organization’s security perimeter, SOCs have improved visibility into end-user activity and retain control over web filtering. Many organizations can benefit from the detailed, unified audit trail generated by the Silo browser and standard features such as web category filtering based on user groups, domain name blacklists, and more. Organizations have full control over their log data, which can be encrypted with a customer-supplied key to ensure integrity and privacy.
- **Data loss prevention:** Another benefit of implementing remote browser isolation is greater control over data loss prevention, including: copy/paste, file upload/download, and printings controls. While noticeably absent from standard web browsers, these features can be easily configured on the Silo browser to provide customized controls based on users and access groups.
- **Integration with other security investments:** Built with security in mind, Silo integrates well with other tools in an existing security stack, and offers flexibility in implementation. With its convenient APIs and compatibility with leading technologies, Silo seamlessly works with SAML identity providers, active directory, two-factor authentication, security information and event management systems, and more.

After implementing this architecture, organizations can realize an additional return on investment from the platform's flexibility and applicability across many use cases. Consider the many opportunities to separate the trusted from the untrusted—trusted devices from untrusted data, or untrusted devices from trusted data. For example, users can access sensitive web applications while working remotely from untrusted or unmanaged devices with Silo preserving control over the information, data loss prevention, and identity management. The Silo platform's unique features enable access while protecting sensitive data, even from hostile locations or networks without fear of surveillance, data breaches, or misdirection.

Given this option and its benefits, why would we allow users to access untrusted websites using a locally-installed web browser from a workstation inside an organization's internal network?

Remote browser isolation disrupts the avenue by which malware can infect a computer. It also enables true whitelisting of internet traffic and is a critical component of a real zero trust architecture. This combination of risk mitigation would be otherwise unattainable with other solutions, all of which rely on an expensive multi-layer blanket of security products to detect malicious code after it enters the network.

While I am partial to Authentic8 Silo, I sincerely believe that – dollar for dollar – it is the best service to provide the most substantial risk reduction from web-based threats, including compromises from advanced persistent threats. In hindsight, I wish I had known about this concept many years ago.

## Closing Thoughts

Having spent a lot of my cybersecurity career focusing on incident response and standing up Security Operations Centers, I know the difficulty and frustration of preventing and detecting attacks from well-resourced adversaries. I also understand the tough risk-based decisions CIOs and CISOs must make to secure their networks, systems, and personnel while equipped with finite resources and authority.

I think back to the many audits, cybersecurity incidents, and information assurance programs that I've been a part of over the years, and wish that I would have re-thought the concept of web browsing years ago. It's incredibly simple in hindsight, and I hope that others can benefit from this message.

Through the Silo Web Isolation Platform, organizations can rapidly implement a real zero trust web browsing architecture while preserving a familiar web browser interface to end-users. It also integrates incredibly well with the mission of audit, incident response, and data loss prevention teams, keeping CIOs, CISOs, and users happy.

You can find additional information on Silo and cloud browser isolation at [www.authentic8.com](http://www.authentic8.com), and you can always reach me at [matt@authentic8.com](mailto:matt@authentic8.com).



### CONNECT WITH US

+1 877-659-6535

[www.Authentic8.com](http://www.Authentic8.com)



### PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.