# Isolation solves the cybersecurity dilemma

## Keeping malicious traffic off user devices takes Zero Trust to the next level.

Protecting agencies from cyberattacks is imperative. At stake is the safety of classified and personal information as well as avoiding ransomware, unplanned downtime, and regulatory penalties. Yet sophisticated cyberattacks continue nonstop, despite the time, money, and effort spent to prevent them.

It's time to ask: Why are most cybersecurity strategies and tactics so ineffective, and how can we do better?

### ‘Detect and mitigate’ falls short

The longstanding approach to cyber defense is first to detect attacks and then mitigate their effects, but this has proven to be ineffective. Yet, according to the 2021 Cost of a Data Breach Report from IBM,[1] the average time to detect and contain a breach is 287 days (212 to detect, 75 to contain), an increase of one week over 2020.

### Remote work's impact

A remote or hybrid workforce requires absolutely secure connectivity. Current solutions include virtual private networks (VPNs) as well as Trusted Internet Connection (TIC) 3.0. Both VPNs and TICs add latency that slows remote connectivity and it's been proven that some VPNs can be hacked.

Meanwhile, remote devices, including the Internet of Things (IoT), make the network perimeter fluid, creating the need for more effective access controls. Enter Zero Trust security.

### Zero Trust: security inside the fence

Many perimeter-based security solutions give logged-in users and devices virtually unlimited access to network resources. A Zero Trust approach, on the other hand, grants “least-privilege” access to applications and data

### Security technologies for a connected world

To stem the tide of attacks, agencies rely on a number of on-premise and cloud technologies, including:

**Secure Web Gateway (SWG)** – Protects users from phishing attacks and malware while assuring regulatory compliance,. analyzes web traffic and implements policies to block unsecured traffic from entering a network..

**Cloud Access Security Broker (CASB)** – Enables cloud usage while protecting sensitive data; consolidates and enforces multiple types of security, including authentication, policies, single sign-on, and encryption.

**Data Loss Prevention (DLP)** – Identifies and blocks sensitive data on endpoints, in motion across networks, and at rest in storage; inspects email and IM content and performs contextual analysis of data. an be integrated into SWG, CASB, or other tools.

DLT
A TECH DATA COMPANY

Menlo Security

[1] https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

and continues to ask for authorization from users and devices even after that initial login.

Simple in concept, Zero Trust architectures (ZTA) could be time-consuming and costly to implement. Still ZTA became mandatory for federal agencies by President Biden's executive order of May 2021, which recommended the adoption of CISA's Zero Trust Maturity Model.

### Is Zero Trust enough?

While Zero Trust can limit the damage of cyberattacksit isn't 100 percent effective. The Cost of a Data Breach Study found organizations with a mature Zero Trust strategy had an average data breach cost of $3.28 million, $1.76 million less than those that had not deployed Zero Trust — but still significant. Still, Zero Trust might frustrate bad actors enough to outweigh the cost and effort of an attack.

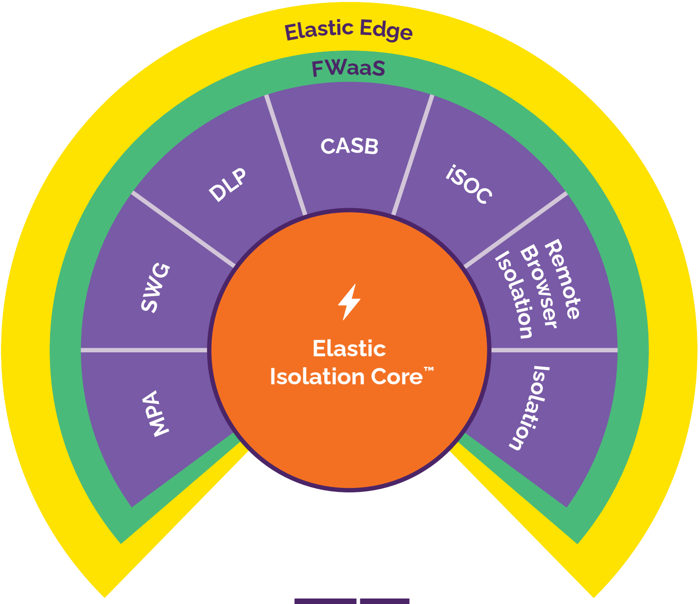
### Isolation changes the game

Is a better implementation of Zero Trust possible – one that can completely eliminate successful attacks? The answer is isolation.

Remote Browser Isolation (RBI) delivers true Zero Trust by creating a virtual air gap that prevents malicious payloads from ever reaching user devices; in effect, no device and no online resource is trusted. RBI enables users to view web content and email messages in a cloud-based virtual browser, isolating any malware or hidden code from your systems. Instead of detect and mitigate, isolation keeps malware and intruders from ever touching network resources.

### Menlo Security — powered by an Isolation Core™

The Menlo Cloud Security Platform overcomes the failures of detect and mitigate and improves on Zero Trust, reducing security alerts by 90% while reducing VPN traffic by more than 70% — without increasing risk.



The key is Menlo's Isolation Core™ that supports every function of the solution.

Highly scalable and quick to implement, Menlo's platform consolidates the functions of several appliances, including SWG, DLP, and CASB, into a single cloud-based platform — helping you identify suspicious activity and resource hogs while minimizing shadow IT.

While classified traffic still routes through VPN, email, web browsing, and SaaS applications can be routed via a "split VPN" through Menlo's cloud platform, where content is cleaned and accessible through the browser.

### Safe, remote... and productive

Unlike detect-and-mitigate security, Menlo Security protects remote users' systems and networks even if the online resources have been compromised. The result is a highly-responsive online experience that maximizes productivity and security across your enterprise.

Learn how Menlo Security can deliver true Zero Trust solutions for your remote and hybrid workforce:
**ask@menlosecurity.com**