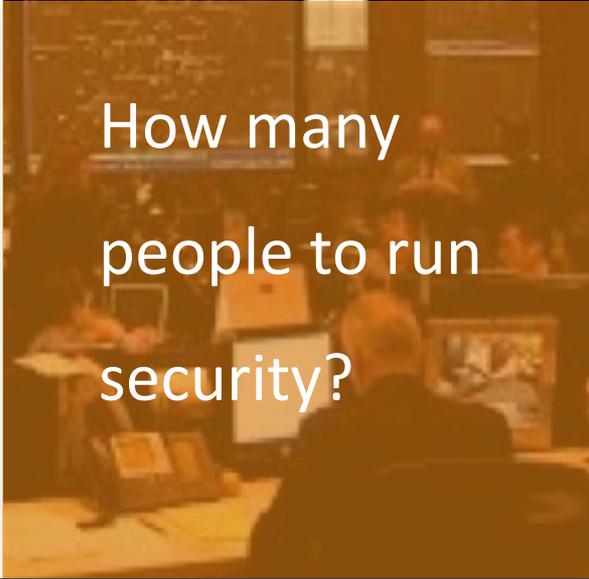# Web & Phishing Isolation

Security Teams Are Facing Difficult Questions
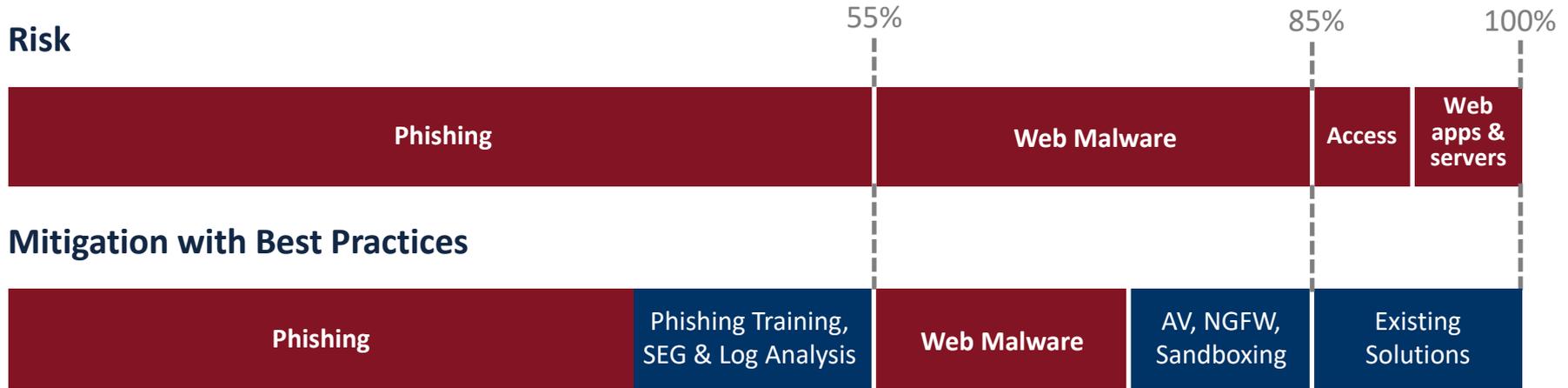
Will we be the next headline breach?

How many people to run security?

Are we protected against incoming cyber attacks?

To answer these questions, we have to look at where the risk is coming from

Typical Enterprise Risk Mitigation Today

Menlo Security
IT'S SAFE TO CLICK

Risk

	55%		85%	100%

Phishing	Web Malware	Access	Web apps & servers

Mitigation with Best Practices

Phishing	Phishing Training, SEG & Log Analysis	Web Malware	AV, NGFW, Sandboxing	Existing Solutions

- Attackers shifted to easiest paths into the Enterprise: Web and Email

  - Combination of Web and Phishing is **~ 85% of Enterprise Risk**

- Traditional "good vs. bad" prevention has become ineffective

Security alert volume and incident response is killing SOC staff productivity

Join Our Mission
Eliminate 100% of Malware from Web and Email Via Menlo's Patented Isolation Platform

"It's Time to Isolate Your Users From the Internet Cesspool With Remote Browsing"
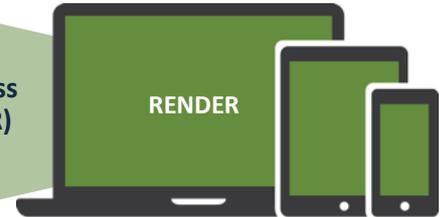Neil MacDonald - Gartner

Menlo Security's Isolation Platform

Menlo Security
IT'S SAFE TO CLICK

Menlo Security | ISOLATION PLATFORM

Web

Documents

Email

PHISHING

FETCH
EXECUTE

FETCH
EXECUTE

FETCH
EXECUTE

Dispose with every click

Adaptive Clientless Rendering™ (ACR)

USERS

RENDER

- **SECURE, Zero Malware**
- **Native UX**
- **Any Device, OS, Browser**
- **No Endpoint Software**
- **No Appliances**
- **Infinite Cloud Scale**
- **Available On-Prem**

Use Cases

Web and Document Isolation:

- **Web Isolation**

  - Allow safe access to Risky Web
    - Uncategorized Sites
    - Sites running Vulnerable Services
    - Flash
    - Known security incidents

  - Isolate All
    - Isolate all web requests and Flash

- **Document Isolation**
  - Protect against weaponized documents
  - Sandbox/AV to inspect/analyze original downloads

Email Isolation:

This website has been identified as suspicious. You can enable data submission by clicking the button to the right. Proceed with caution.

URL shortener

Disable Input Protection

- ## Email Link Isolation

  - Eliminate drive-by exploits by isolating all email links
  - Isolate, Read-Write, or Read-Only Policy is enforced based on Risk Score
  - Prevent Credential Theft and Spear Phishing
    - Users cannot inadvertently give away credentials to Risky Sites
  - Coach and Educate Modes reinforce Anti-Phishing Training
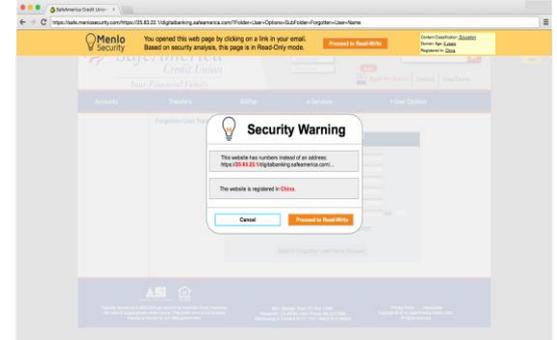
JPMorgan Chase & Co.

Step 1: Isolate Risky Websites

- 80% of malware emanating from uncategorized sites

Step 2: Isolate Email Links **Enterprise Wide**

- Spear-phishing an on-going concern

Step 3: Isolate All Web for High-Value Users

- Eliminate **All** Risk from Web and Email

Dr. Rohan Amin
Global CISO

"We were impressed by Menlo Security's innovative approach to protecting the firm from web-based threats. Its Isolation Platform has been integrated with zero impact to users, providing a seamless user experience for our employees."

Leader in Isolation & Enterprise Protection

JPMorgan Chase & Co.

Winner: 2016 Innovation Award

RSA Conference Innovation Sandbox

2016 Finalist for Most Innovative Startup

SINET

Named to 2016 List for Cybersecurity Innovators

InformationWeek DARK Reading

2016 Security 20
20 Coolest Web & Security Vendors

Interop Tokyo 8 – 10 JUNE 2016 MAKUHARI MESSE

2016 Interop Japan Grand Prize Winner

MITSloan CIO Symposium

2016 Innovation Showcase Top 10 Finalist

Forbes

Hottest Cybersecurity Startups 2015

Case Study: Isolate All

Pain Point:

- User admin rights on machines + unfettered browsing
- Ransomware hit once per month
- Lateral spread via shared folders
- Restore from back up – 3 day delay/projects
- Expensive overhead sat idle during restore
- Up coming GDPR legislation 4% scary prospect

Menlo Success:

- Isolate all except trusted websites
- Locked service down and mandated
- Internal sponsor traded risk for UX

Manufacturing: £1.3bn Revenue

Competition

Increasing Competition Validating the Market:

- **Visual Streaming and poor user experience**

  - Scrolling Issues
  - Pixelated Video
  - Browser extensions fail
  - Scaling issue
  - No Sandbox
  - Practicality Issues

- **Hardware Isolated End Point Security**

  - Endpoint based
  - Min requirements for OS, RAM and CPU
  - Difficult to deploy & manage enterprise wide
  - Only subset of browsers
  - Windows Only
  - Heavy lifting on the endpoint

Competition:

Key taking points on this worthy of highlight where Menlo win:-

1. Solution must allow the browser to support the capability of printing documents
2. Solution must allow the browser to support the capability for video playback
3. Solution must allow the browser to support the capability for saving pages
4. Solution must allow the browser to support the capability of allowing the user to interact with the browser and web site natively
5. Solution must protect the endpoint from malicious PDF documents
6. Solution must provide the capability of being able to selectively control what is isolated
7. Solution must provide the capability of being able to selectively control what is SSL inspected
8. Solution must provide inspection SSL capability without any additional software being installed
9. Solution must provide capability to scale at size (support 40,000+) connections
10. Solution must provide capability to provide reports on sites / connections with risk associated with them
11. Solution must provide the capability of using SSO via SAML to allow users to authenticate to the service

Anti Phishing Alternatives

- Cannot Eliminate 100% Malware
- Sandbox can fail, isolation cannot
- Patient Zero
- Cannot Eliminate Credential Phish
- No Reinforcement of Anti-Phishing Training
- No protection from Mis-categorized phishing Link