BAE SYSTEMS

Targeted Attack Protection

BAE Systems Email Protection Services

Targeted and zero-day threat prevention. Protects any cloud and premise email platform.

Sandbox-aware malware defense

Don't let malware sleep in your email sandbox

Sandboxes were introduced to defeat malware sent in emails by checking email payloads for malware **before** getting to users.

But this process is an incomplete way to detect malware since advanced cyber criminals can use new evasion techniques to beat detection. It is also **slow,** delaying email delivery.

BAE Systems' instrumented browser **defeats and outwits** sandbox-aware malware that has 'learned' it is in a sandbox.

We isolate and defeat sandbox–aware malware before it can deploy and evade detection - **delivering clean emails within seconds, not minutes.**

Targeted and phishing attack prevention

Protection from harmful email links

Over 77% of malware installations come from email, and just 10 malicious targeted emails guarantees a breach because of the effort cyber thieves take to make messages look so real - like they have come from a reliable source.

BAE Systems detects and prevents advanced threats before they happen.

Website links are safe and clean with Targeted Attack Protection

Targeted Attack Protection combines both static- and dynamic-analysis engines with immediate detect and block capabilities for complete protection against malicious links.

BAE Systems provides a complete portfolio of email security solutions.

We are better able to identify, understand, and effectively defend against the professional hackers currently assaulting the IT infrastructure of corporations.

Benefits of Targeted Attack Protection

Protects vulnerable business email from advanced threats

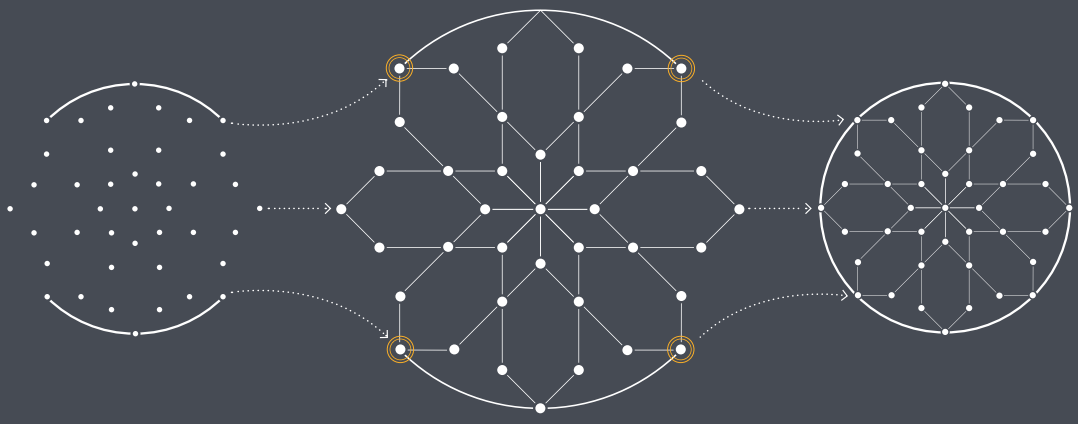
- Provides the most effective protection against unknown malware in spear phishing attacks and zero-day exploits.
- Helps protect companies from reputational damage and intellectual property theft from cyber criminals.
- Protects all third-party cloud and on-premise email, including Google and Office 365.

Succeeds where typical sandbox detection fails

- Deployed directly in-line with mail flow. Advanced static analysis detection capabilities are more accurate and execute faster than out-of-band sandboxing.
- Performs granular analysis within the browser process itself using instrumented browser technology to detect and defeat environmentally-aware malware.
- Identifies zero-day malware before it can deploy and evade detection – with rapid detection, containment, and response.

Pure cloud solution for security, affordability and ease of use

- Nearly impossible to reverse engineer the way appliance-based detection can be compromised by hackers.
- Offers predicable monthly costs. No hardware or software to purchase or manage.
- Fast and effortless activation. No migration or integration is required.



BAE Systems, 1676 International Drive, Suite 1000, McLean, VA 22102, USA

T: +1 (703) 848 7000

E: learn@baesystems.com | W: baesystems.com/businessdefense

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai