Paladin
Shield

Technical Specs

Inbox Defender

- Works with Office365 or GSuite.
- Machine learning algorithm analyzes each email for social engineering and phishing.
- Realtime intelligence for phishing and malware protection.
- Deep-link analysis traverses proxies and URL shorteners.
- Deployable via browser extension (Edge, Chrome, Firefox) or Outlook Add-in.

Secure Web Traffic

- Secures all HTTP traffic through a TLS tunnel.
- Prevents local network (ethernet and wifi) sniffing of HTTP traffic
- Adds at most 75 ms of delay to requests.
- Does not affect network bandwidth.

Password Manager

- All passwords encrypted with AES-256.
- Team password sharing via PKI.

  Compromised passwords monitoring.
- Generate and save strong passwords automatically.

Harmful Site Blocker

- Full user-identity awareness.
- Decrypted analysis of all SSL/TLS traffic without TLS interception or use of root certificates.
- DNS reputation filtering
- Realtime phishing and malware URL filtering.
- Secures HTTP, HTTPS, WS, and WSS protocols.

Script Protection

- Prevents XSS injections through URLs.
- Prevents non-private IP hosted websites from attempting to connect to private IP spaces.

Content filter

- Full user-identity awareness.
- Blocks embedded frames even in HTTPS secured websites.
- Prebuilt list for NSFW websites.
- Customizable block list.
- Customizable allow list for external and internal web applications.

Security Awareness Training

- Addresses critical topics like ransomware, phishing, email threats, online safety, and data privacy.
- Modules include short videos and quizzes to test knowledge.
- Each employee's curriculum is dynamically updated based on engagement with threat simulations.

Remote Access Monitoring

- Understand the number of remote access services running in your environment.
- Assess security configurations of RDP, SSH, and SMB.
- Remote workforce monitoring.
- Attribute remote access on a per-employee basis.

Host Vulnerability Monitoring

- Continuous monitoring of internet-facing assets.
- Per host CVE reporting.

Email Security Monitoring

- SPF monitoring and assessment.
- DMARC monitoring and assessment.
- Encrypted transport detection.

DNS Monitoring

- Monitor subdomains that are detectable from our DNS sonar.
- Know when private DNS records have leaked to the public internet.

Threat Simulation

- 50+ configuration-free templates modeled after the most commonly spoofed brands/services.
- Link-based phishing with matching credential capture pages simulates entire attack chain, not just a single click.
- Reply based phishing simulates data extraction through social engineering.
- Attachment-based phishing simulates ransomware and other malware payloads via Office and PDF documents.

Website Monitoring

- Content security policy assessment.
  Cookie policy assessment.
- Cross-Origin Resource Sharing (CORS) assessment.
- HPKP detection.
- HSTS detection.
- Secure redirection assessment.
- Subresource Integrity (SRI) assessment.
- X-Content-Type-Options assessment.
- X-Frame-Options assessment.
- X-XSS-Protection assessment.

Breach Monitoring

- See what information of your employees have been lost in prior breaches.
- Dark web crawling.
- Pastebin visibility.

Got questions about Shield?

Set up a free consultation | Call: 1-800-418-8593
Email: contact@meetpaladin.com
Paladins are available Monday to Friday between 6am-6pm PT.

Paladin Shield