County Reinsurance, Limited

Issue No. 6 ● July 2024

CRL Cyber Circular

Email Filtering and Web Security

The subject of this issue of the *CRL Cyber Circular* is Email Filtering and Web Security, the fifth of the Top Cybersecurity Controls, and the last of the "Top 5 of the Top 12". (See explanatory note in the inset box.)

Of the many services that operate on the Internet, email and the World Wide Web, taken together, are either the entry point or target of the majority of cyber threats. Email filtering and web security are essential controls for every enterprise.

Top Cybersecurity Controls

1. Multifactor authentication for remote access and admin/privileges
2. Endpoint Detection and Response (EDR)
3. Secured, encrypted, and tested backups
4. Privileged Access Management (PAM)
5. Email filtering and web security
6. Patch management and vulnerability management
7. Cyber incident response planning and testing
8. Cybersecurity awareness training and phishing testing
9. Hardening techniques, including Remote Desktop Protocol (RDP) mitigation
10. Logging and monitoring/network protections
11. End-of-life systems replaced or protected
12. Vendor/digital supply chain risk management

NOTE: Top Cybersecurity Controls numbers 1 through 5 are viewed by cyber insurance carriers as most important in the underwriting process. Cyber insurance applicants that lack strong controls in the top five areas may be denied insurance, pay higher premiums, or have other conditions imposed on their coverage.

Description

Most email filtering and web security technical solutions include capabilities such as: detecting and blocking phishing emails; scanning emails and blocking malware; identifying and filtering out spam email; detecting and blocking Business Email Compromise (BEC) attacks; and Data Loss Prevention. Vendors often combine these functions into a single technology platform, or integrate them across a number of separate products.

Implementation Suggestions

The products listed below are representative of products in this area and can serve as a starting point for counties seeking to research available tools. Many other quality vendors offer similar solutions. Choosing the right products is not by itself sufficient to provide the intended security; the technology must also be deployed and configured properly and supported with sustainable operational procedures.

Vendor	Solution	Description
proofpoint.	Proofpoint Email Security and Protection	Designed to stop a wide range of Business Email Compromise (BEC) attacks, including payment redirect and supplier invoicing fraud. Advanced BEC Defense protects against phishing, BEC, and email fraud. - Analyzes multiple message attributes, such as header data, sender IP addresses, and message body, and then detects attacker tactics, such as reply-to pivots, use of malicious IPs, and use of impersonated supplier domains. - Provides granular visibility into BEC threat details (e.g., BEC type, why the message was suspicious, message samples). Blocks malicious email. - Multilayered detection techniques, including reputation and content analysis, to help defend against email-based threats. - Dynamic classification of a wide variety of emails (e.g., phishing, malware, BEC threats, bulk email, spam). https://www.proofpoint.com/us

FORTINET	FortiMail	▪ Safeguards organizations against the full spectrum of email-based threats such as phishing, ransomware, zero-day, and Business Email Compromise (BEC) attacks. ▪ AI-powered Security Services provide cutting-edge security technology to prevent, detect, and respond to email-based threats in real time. ▪ Monitors for and stops the outflow of sensitive data and encrypts outbound email. ▪ Provides advanced security for Exchange Online including delivery clawback and real-time scanning. ▪ Integrates with FortiSandbox, FortiSIEM, and FortiSOAR to enhance protection and help automate workflows including response. ▪ Mitigates outages of cloud-based or on-premises email services. https://www.fortinet.com/products/email-security
IRONSCALES	IRONSCALES Email Security Platform	▪ Cloud-native, API-based email security detects and remedies advanced threats at the mailbox level, before and after email delivery. ▪ Protects against zero-day malware, credential theft, and phishing with real-time defense against all inbound emails, using multiple anti-virus, visual anomaly detection, and sandbox engines. ▪ Blocks non-signature-based Business Email Compromise (BEC) attacks (e.g., CEO fraud, supply chain attacks, invoice fraud) in real-time. ▪ Anti-phishing simulations and customized training based on real-world scenarios. ▪ Phishing protection for Microsoft Teams ▪ AI-powered Virtual SOC Analyst automates thresholds, analysis, and quarantine of threats. https://ironscales.com/
PERCEPTION POINT	Perception Point Advanced Email Security	Email Security ▪ Next-gen cloud-based email security software that prevents APTs, phishing, malware, ATO, spam, impersonation, and Business Email Compromise (BEC) attacks. ▪ Integrates with Office 365, Microsoft Exchange, Gmail, or any web-based email service. Web Security ▪ Isolates, detects, and remediates attacks on web browsers and SaaS apps from external web threats and data breaches. Scans all web browsing. ▪ Prevents harmful browser extensions from compromising users and data. ▪ Enforces safe access to SaaS apps on managed and unmanaged browsers. Stops data leaks, malicious insiders, and third-party threats. https://perception-point.io/
CHECK POINT	Check Point Harmony Email & Collaboration	API-based inline service that protects SaaS applications from cyber threats, including zero-day threats, phishing, Account Takeover, data leakage, SaaS shadow IT discovery. ▪ Inspects internal and outgoing traffic for data leakage, phishing, and malware. Also inspects every uploaded file for malware and DLP. ▪ Emails can be removed and modified post-delivery if needed. ▪ Supports Microsoft Exchange Online (Office 365 Mail), Gmail, and messaging applications Microsoft Teams and Slack. https://www.checkpoint.com/
DARKTRACE	Darktrace/Email	▪ Analyzes content and context to stop novel social engineering, phishing, Business Email Compromise (BEC) and account takeover, with advanced data loss prevention. ▪ Blocks outbound mail threats with advanced data loss prevention tools (including user behavior analysis) to stop unknown, accidental, and malicious data loss. ▪ Recognizes cases of misdirected emails through behavior analytics. ▪ Analyzes data that is pending labels or cannot be labeled by understanding content and context of every email. Takes action on both classified and unclassified data. ▪ Extends Microsoft Purview policies and sensitivity labels to avoid duplicate workflows, combining the best of both approaches. https://darktrace.com/

Note: This table provides information on a variety of products and services relevant to Email Filtering and Web Security; inclusion here does not represent an endorsement or recommendation of the products and services by CRL. The order in which products are listed is arbitrary.