GUIDEPOINT® SECURITY

1900 Reston Metro Plaza
Suite 701
Reston, VA 20190

FACSIMILE FORM

VENDOR NAME: GuidePoint Security, LLC – Authorized Reseller/Representative for Proofpoint
BUYER: Toby L Welch
SOLICITATION NO: CRFQ OOT2700000005
BID OPENING DATE: TUESDAY, AUGUST 25, 2026
BID OPENING TIME: 1:30 P.M.
FAX NUMBER: 304-558-3970

Bid Delivery Address and Fax Number:
Department of Administration, Purchasing Division 2019 Washington Street East
Charleston, WV 25305-0130
Fax: 304-558-3970

Submitted by:

8/25/26

GUIDEPOINT SECURITY

Corry Tice
Account Executive
W (877) 889-0132 x1483
M (443) 962-7972
A 1900 Reston Metro Plaza, Suite 701
Reston, VA 20190
corry.tice@guidepointsecurity.com
guidepointsecurity.com

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Info Technology

Proc Folder:	2028979		Reason for Modification:
Doc Description:	Addendum No 1 Advanced Email Security		Addendum No 1 is issued to publish vendor questions with agency responses and to modify the bid opening date.
Proc Type:	Central Master Agreement		
Date Issued	Solicitation Closes	Solicitation No	Version
2026-08-18	2026-08-25 13:30	CRFQ 0231 OOT2700000005	2

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

Vendor Customer Code: VS0000009240 5
Vendor Name: Guidepoint Security
Address: 1900 Reston Metro Plaza
Street: Suite 701
City: Reston
State: VA, 20190 Country: United States Zip: 20190
Principal Contact: Cory Tice
Vendor Contact Phone: (877)889-0132 Extension: 1483 | Cell # 443.962.7972

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X: [signature] FEIN# 46-3694402 DATE 8/25/26

All offers subject to all terms and conditions contained in this solicitation

Date Printed: Aug 18, 2026 Page: 1 FORM ID: WV-PRC-CRFQ-002 2020/05

ADDITIONAL INFORMATION
Addendum No 1 is issued for the following reasons: 1) To publish vendor questions with the agency's responses. 2) To modify the bid opening date from 8/19/26 to 8/25/26 ---no other changes---

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON US	WV	WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Core Detection	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON US	WV	WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Core Detection - Year 2 (Optional Renewal)	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON US	WV	WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Core Detection - Year 3 (Optional Renewal)	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON US	WV	WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON US	WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Core Detection - Year 4 (Optional Renewal)	22000.00000	EA		

Comm Code	Manufacturer	Specification	Model #
43230000			

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions are due by 3:00 p.m.	2026-08-11

	Document Phase	Document Description	Page 4
OOT2700000005	Final	Addendum No 1-Advanced Email Security	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

GUIDEPOINT® SECURITY

Sales Proposal: 301529-1

Today's Date: 8/19/2026	Expires On: 10/1/2026	Payment Terms: Net 30	Billing Schedule: Upfront
Sales Rep: Corry Tice	Email: corry.tice@guidepointsecurity.com	Phone:	Fax: (877) 888-0132
Prepared by: Kacl Ward	Email: kacl.ward@guidepointsecurity.com	Phone:	

Sales Proposal Prepared for:

Toby L. Welch State of West Virginia Office of Technology	Wv Office Of Technology 1900 Kanawha Blvd E Rm 510 Charleston, WV 25305-0009 United States	Email: toby.l.welch@wv.gov Phone: 304.352.4944

Please send all Purchase Orders to masos@guidepointsecurity.com and kacl.ward@guidepointsecurity.com

Group 1

Line #	Vendor	Quantity	Product Type	Part Number	List Price	Client Unit Price	Client Total
1	ProofPoint, Inc.	22000	Software	PFPT-S-P0M-S-A	$27.14	USD 0.00	USD 0.00
Description: PFPT Enterprise P0-McAfee-S-NPRS, Email Protection, TAP URL & Attachment Defense, TAP URL Iso. (VAP only), Threat Response Auto-PullMcAfee-SaaS-Term: 12 month22000 Users 6 Month Term							
2	ProofPoint, Inc.	1	Software	PPA0-M-LAPI-S-A	$16,000	USD 0.00	USD 0.00
Description: Log API Forwarding is a feature available for PoD customers to receive mail logs (filterd & sendmail) from their PoD cluster in real-time. The logs are sent in syslog format. Customers can receive these logs on common SIEM tools-Term:12 month22000 Users6 Month Term							
3	ProofPoint, Inc.	22000	Software	PFPT-M-TAPAU-S-A	$5.43	USD 4.78	USD 105,160.00
Description: PFPT TAP Account Takeover (US-Only Deployment)-PFPT TAP Account Takeover (up to 1,000 monthly activities) (US-Only Deployment)Term: 12 months22000 Users 6 Month Term							
4	ProofPoint, Inc.	1	Vendor Services	PP-PST-IS-IMP	$146,308	USD 0.00	USD 0.00
Description: InfoSec PS Implementation Services Tier 1 - 1000000 - Term: 12 Months							
					Group 1 Total:	USD 105,160.00	

Group 2

Line #	Vendor	Quantity	Product Type	Part Number	List Price	Client Unit Price	Client Total
5	ProofPoint, Inc.	22000	Software	PFPT-S-P0M-S-A	$27.14	USD 6.48	USD 120,560.00
Description: PFPT Enterprise P0-McAfee-S-NPRS, Email Protection, TAP URL & Attachment Defense, TAP URL Iso. (VAP only), Threat Response Auto-PullMcAfee-SaaS-Term: 12 month22000 Users 6 Month Term							
6	ProofPoint, Inc.	1	Software	PPA0-M-LAPI-S-A	$0.00	USD 0.00	USD 0.00
Description: Log API Forwarding is a feature available for PoD customers to receive mail logs (filterd & sendmail) from their PoD cluster in real-time. The logs are sent in syslog format. Customers can receive these logs on common SIEM tools-Term: 12 month22000 Users6 Month Term							
7	ProofPoint, Inc.	22000	Software	PFPT-M-TAPAU-S-A	$5.43	USD 4.78	USD 105,160.00
Description: PFPT TAP Account Takeover (US-Only Deployment)-PFPT TAP Account Takeover (up to 1,000 monthly activities) (US-Only Deployment)Term: 12 month 22000 Users 6 Month Term							
					Group 2 Total:	USD 225,720.00	
					Client Grand Total:	USD 330,880.00	

Sales Proposal Notes:

All Pricing Information is Confidential

GUIDEPOINT® SECURITY

Payment 1 in the amount of $331,760.00 due upon Net Terms on Invoice.
Upon exercise of option year 1, $461,840.84 is due no later than twelve (12) months from the subscription term start date.
Upon exercise of option year 2, $548,694.76 is due no later than twenty-four (24) months from the subscription term start date.
Upon exercise of option year 3, $645,346.69 is due no later than thirty-six (36) months from the subscription term start date.
Upon exercise of option year 4, $742,102.62 is due no later than forty-eight (48) months from the subscription term start date.

Free months are a one time incentive that will not be available upon renewal.
The incentive pricing stated herein is specifically contingent on receiving a corresponding purchase order by close of deal no later than 9/30/2026.
This proposal is valid only: (1) for the Proofpoint SKU items identified above (taken as a whole), and (2) until the quote expiration date. The fees listed herein do not include sales, use, withholding, value added, excise or other similar taxes and duties, or shipping fees. Updates for Spam Detection (regular updates based on external threats), Virus Scanning (periodic releases supplemented by external virus discoveries), and Regulatory Compliance (periodic updates of regulatory dictionaries) products are provided at N/C to Proofpoint customers throughout the subscription term. Customer accepts and agrees to the following italicized terms: "Unless the end user customer ("Customer") has a written license agreement in place with Proofpoint for the products listed above, Customer's issuance of a purchase order (constitutes Customer's agreement that its use of the Proofpoint products is governed solely by the terms of the Proofpoint Customer Agreement found at https://www.proofpoint.com/us/legal/license/customer-agreement, which contains terms regarding license and usage, data privacy obligations, disclaimers and limitations of liability, Proofpoint's right to suspend or terminate Customer's subscription for non-payment, and automatic renewal of the subscription."
In the event Customer does have a written agreement in place with Proofpoint, Customer's issuance of a purchase order constitutes Customer's agreement that its use of the Proofpoint products is governed by such written agreement and the applicable product terms found at https://www.proofpoint.com/us/legal/license/product-terms.

ADDITIONAL TERMS
Acceptance of this proposal constitutes acceptance of, and agreement to be bound by, any and all applicable terms and conditions, copies of which are available for download here: https://www.proofpoint.com/us/legal/contact

GuidePoint Security Terms and Conditions:

This Sales Proposal is governed by the GuidePoint Sales Proposal Terms and Conditions located here unless Client has a mutually executed master agreement then in effect for the purchase of Products from GuidePoint, in which case such agreement will govern.

Product Type shown is not meant for tax purposes. Any taxes quoted are estimates only. Actual taxes will be assessed upon invoice.

4. GENERAL REQUIREMENTS:

4.1 Contract Items and Mandatory Requirements: Vendor shall provide Agency with the Contract Items listed below on an open-end and continuing basis. Contract Items must meet or exceed the mandatory requirements as shown below.

4.1.1 *Core Architectural Requirements (Non-Gateway).*

To preserve native email delivery speeds, prevent MX record modifications, and eliminate single-point-of-failure routing risks, the State requires a **native, API-integrated deployment model.**

4.1.1.1.1 No Gateway Routing: The solution **must not** require changing the State's MX (Mail Exchanger) records or routing inbound, outbound, or internal email traffic through an external secure email gateway (SEG) appliance, mail relay, or cloud proxy.

Proofpoint **Core Email Protection API (CEP API)** meets this requirement through a **native API-based deployment architecture** that integrates directly with the State's Google Workspace environment without requiring changes to the State's MX records or rerouting email traffic through a Proofpoint Secure Email Gateway.
CEP API operates independently of the SMTP mail flow. As a result:

- **No MX record changes are required.**
- **No external SEG appliance is required.**
- **No Proofpoint mail relay or cloud proxy is placed in the State's email delivery path.**
- **Inbound, outbound, and internal email do not need to be routed through Proofpoint for CEP API protection.**
- The State can maintain its **existing Google Workspace mail architecture and routing configuration.**
- Deployment can be accomplished without introducing an additional inline dependency into normal email delivery.

Proofpoint uses API integration with the cloud email environment to provide advanced email threat detection and response capabilities while preserving the State's existing email infrastructure.
This architecture enables Proofpoint to provide advanced detection for threats such as **phishing, Business Email Compromise (BEC), executive and vendor impersonation, financial fraud, account compromise, and lateral phishing** without requiring Proofpoint to function as the State's email gateway.

4.1.1.1.2 API-Based Deployment: The proposed platform must connect directly to the State's Google Workspace environment using Google Workspace APIs.

Proofpoint **Core Email Protection API (CEP API)** meets this requirement through a **native API-based deployment architecture** that integrates directly with the State's Google Workspace environment without requiring changes to the State's MX records

or rerouting email traffic through a Proofpoint Secure Email Gateway.

4.1.1.1.3 **Zero Infrastructure Footprint:** The solution must be 100% cloud-native (Saas) and require no on-premises hardware, virtual appliances, must not require customer-managed virtual machines or cloud compute resources in any form. or local software installations.

Proofpoint **Core Email Protection API (CEP API)** meets this requirement as a **cloud-delivered SaaS solution** that integrates directly with the State's Google Workspace environment through APIs and does not require the State to deploy, operate, or maintain dedicated email security infrastructure.
CEP API requires:

- **No on-premises hardware or appliances**
- **No customer-managed virtual appliances**
- **No customer-managed virtual machines**
- **No customer-managed cloud compute resources**
- **No locally installed email security software**
- **No Proofpoint Secure Email Gateway deployed within the State's infrastructure**
- **No MX record changes or rerouting of the State's mail flow through Proofpoint**

Proofpoint operates and maintains the underlying cloud infrastructure, detection services, AI/ML capabilities, threat intelligence, and platform components required to deliver the service. This eliminates the need for the State to provision and maintain infrastructure supporting the email security solution.

4.1.1.1.4 **Latency-Free Evaluation:** Security analysis must occur asynchronously or inline via API hooks post-delivery, ensuring there is zero artificial latency introduced to standard communication flows.

Proofpoint **Core Email Protection API (CEP API)** meets this requirement through an **API-based architecture that operates outside the SMTP mail-delivery path,** allowing Google Workspace to process and deliver email without requiring messages to traverse a Proofpoint gateway, relay, or proxy.
Because CEP API does not sit inline with standard mail routing, Proofpoint's security analysis does **not introduce artificial gateway processing latency into normal email delivery.**
Key architectural benefits include:

- **Out-of-band/API-based analysis** without inserting an additional SMTP hop into the State's mail flow.
- **No MX record changes** required for CEP API deployment.
- **No Secure Email Gateway, mail relay, or cloud proxy** required in the delivery path.
- **No artificial mail-flow latency** attributable to routing messages through Proofpoint.
- **API-based detection and response** for threats that evade Google Workspace's native security controls.
- **Automated remediation capabilities** to take action on malicious messages identified after delivery.

Proofpoint CEP API therefore allows the State to preserve the performance and availability characteristics of its existing Google Workspace email environment while adding an independent layer of advanced AI/ML and behavioral threat detection.

4.1.1.1.5 **Dual-Platform Flexibility:** While optimized immediately for Google Workspace/Gemini The solution must provide full, native API-level functional parity across Google Workspace and Microsoft 365. Microsoft 365 support must include historical mailbox scanning, automated remediation, mailbox rule monitoring, time-of-click URL inspection, account-takeover detection, and access to all required Microsoft Graph API scopes. The solution must not require MX changes, journaling, SMTP relays, or gateway-based routing for either platform

For Microsoft 365, Proofpoint Core Email Protection API (CEP API) integrates directly using the Microsoft Graph API. During onboarding, Proofpoint performs a one-time 12-month historical synchronization of protected users' email, including attachments, to establish behavioral models based on historical sending patterns, behaviors, and communication relationships

4.1.2 Gemini & Workspace Functional Integration

The solution must operate exclusively through Google Workspace APIs (inside the perimeter') without altering mail routing or MX records. Internal-to-internal email traffic includes all messages exchanged between State-managed mailboxes across all domains and OUs. The solution must not disable, degrade, or interfere with Gemini features including smart replies, AI-generated summaries, context lookups, or native message rendering. Historical scanning must include all existing mailbox content messages, attachments, and mailbox rules-for the full retention period available within Google Workspace and must begin immediately upon activation.

4.1.2.1 **Internal Threat Detection (East-West Traffic):** Because it sits inside the API tier, the solution must analyze internal-to-internal state emails (employee to employee) for lateral phishing, data exfiltration, or account compromise. Internal-to-internal email traffic includes all messages exchanged between State-managed mailboxes, regardless of domain, OU, or routing path.

Proofpoint **Core Email Protection API (CEP API)** meets this requirement by providing API-based visibility and behavioral analysis of **internal email communications between protected State-managed mailboxes**, enabling detection of threats that may never traverse an external secure email gateway.
Proofpoint applies **AI/ML, behavioral analytics, identity and relationship**

Intelligence, and message context to identify anomalous internal communications indicative of compromised accounts and lateral attacks.
Capabilities include:

- **Lateral phishing detection** – Identifies suspicious phishing and social-engineering messages originating from compromised internal accounts and targeting other State users.
- **Account-compromise detection** – evaluates deviations from established user behavior and communication relationships that may indicate a trusted account is being abused.
- **Internal sender and relationship analysis** – analyzes communication context and behavioral relationships even when the sender would otherwise be considered trusted because the message originates internally.
- **Payload-less attack detection** – identifies suspicious social-engineering activity that may not contain known malware, malicious URLs, or traditional indicators of compromise.
- **Data-risk analysis** – Proofpoint's broader API-based capabilities can provide visibility into sensitive information and risky user behavior to help address potential data loss and exfiltration scenarios.
- **API-based visibility** – because CEP API does not depend solely on an external SMTP gateway, internal messages can be evaluated without requiring those messages to be routed externally through Proofpoint.

4.1.2.2 **Coexistence with Gemini:** The tool must not interfere with Gemini's native capabilities, such as AI-driven draft summaries, smart replies, or workspace context lookups or disable, degrade, or interfere with Gemini features including smart replies, AI-generated summaries, context lookups, and native message rendering.

Proofpoint **Core Email Protection API (CEP API)** meets this requirement through its **API-based, non-gateway architecture**, which is designed to complement Google Workspace rather than replace or proxy Google's native email experience.
CEP API operates outside the State's normal SMTP mail-delivery path and does not require Proofpoint to replace the Gmail user interface or route email through a Proofpoint Secure Email Gateway. As a result, users continue to access email and native Google Workspace functionality through Gmail while Proofpoint provides an additional layer of advanced threat detection and response.

Proofpoint's API architecture allows the State to separate **productivity AI from security AI**. Gemini can continue providing Google's native productivity capabilities, while Proofpoint applies specialized email threat detection to identify phishing, BEC, impersonation, lateral phishing, and other malicious activity.

4.1.2.3 Historical Scanning: The API integration must allow the tool to scan existing historical mailboxes retrospectively to establish a baseline threat profile immediately upon activation. Historical scanning must include all existing mailbox contents, including messages, attachments, and mailbox rules, for the full retention period available within Google Workspace. Scanning must begin immediately upon activation and complete without requiring mail routing changes.

Proofpoint **Core Email Protection API (CEP API)** uses historical and ongoing email telemetry to establish behavioral context and communication relationships that support AI/ML-driven detection of phishing, BEC, impersonation, lateral phishing, and account-compromise activity.
CEP API is deployed through cloud APIs and does **not require MX-record changes, SMTP relays, or gateway-based mail routing** to perform API-based analysis.
Proofpoint's behavioral detection approach establishes organization-, user-, and relationship-specific context and combines that information with **Proofpoint global threat intelligence, identity intelligence, behavioral analytics, and AI/ML models.**
This enables the solution to identify deviations from expected communication behavior without relying exclusively on static signatures or previously observed attack patterns.
Proofpoint supports historical synchronization as part of its API-based architecture.
However, Proofpoint proposes clarification of the requirement that the solution scan **every historical message, attachment, and mailbox rule for the entire Google Workspace retention period.**
The security objective of establishing an accurate behavioral baseline can be achieved without requiring unrestricted retrospective processing of every item retained within the State's environment. Proofpoint's approach is designed to obtain the historical and ongoing information necessary to establish effective behavioral models while minimizing unnecessary data access and processing.

4.1.3 Technical & Threat Protection Capabilities

The solution must utilize machine learning that includes behavioral baselining, anomaly detection, and language-pattern analysis beyond static rule-based filtering. BEC detection must include internal and external impersonation, vendor compromise, invoice fraud, and look-alike domain analysis. Time-of-click URL inspection must analyze redirect chains, embedded URLs, QR-encoded links, and dynamically generated phishing pages. Malware and zero-day protection must include deep file inspection and cloud-based sandboxing for executables, archives, scripts, Office documents, PDFs, and containerized payloads. ATO monitoring must include mailbox rule changes, anomalous login behavior, impossible travel detection, OAuth token misuse, MFA bypass attempts, and unauthorized API-scope grants.

4.1.3.1 Business Email Compromise (BEC) & Spoofing: Must analyze language sentiment, communication baselines, and look-alike

domains to stop executive impersonation, vendor invoice fraud, and employee payroll diversion tactics.

Proofpoint **Core Email Protection API (CEP API)** meets this requirement through a multi-layered, AI-driven approach to detecting **Business Email Compromise (BEC), impersonation, and socially engineered fraud**, including attacks that contain no malware, malicious attachment, or known malicious URL.
Proofpoint combines **AI/ML-based content and language analysis, behavioral and communication relationship intelligence, identity analysis, domain intelligence, and global threat intelligence** to identify suspicious communications and attacker intent.
Proofpoint capabilities include:

- **Language and content analysis** – AI/ML analyzes message content, context, and linguistic characteristics to identify socially engineered communications associated with financial fraud, credential theft, and impersonation.
- **Communication baselining** – behavioral models evaluate normal communication patterns and relationships between users and external correspondents to identify anomalous or unexpected activity.
- **Executive impersonation detection** – identity and behavioral signals help identify messages attempting to impersonate executives and other high-value State personnel.
- **Vendor and supplier fraud detection** – relationship and identity analysis helps identify fraudulent communications impersonating trusted vendors, including suspicious invoice and payment-change requests.
- **Payroll diversion detection** – content, identity, and behavioral signals can identify socially engineered requests involving payroll or direct-deposit changes.
- **Look-alike domain detection** – domain and identity intelligence helps identify domains designed to resemble trusted State, executive, vendor, or business-partner domains.
- **Payload-less BEC detection** – Proofpoint does not require the presence of malware or a malicious URL to identify a potentially malicious message.

Proofpoint correlates these signals rather than relying on any single indicator. This is particularly important for BEC, where an attacker may use a newly registered look-alike domain, convincing language, or a compromised legitimate account and therefore lack conventional indicators of compromise.

4.1.3.2 Advanced Phishing & Credential Harvesting: Must perform real-time URL sandboxing and dynamic link inspection at the time-of-click to block morphing malicious links.

Yes—Proofpoint supports time-of-click dynamic link inspection and real-time URL sandboxing to block URLs that become malicious after delivery.
URLs can be rewritten so clicks are routed through Proofpoint's cloud service for real-time analysis and blocking, including when a link morphs post-delivery.
Predictive and click-time URL sandboxing are supported; when a URL is deemed malicious, users can be shown a "block page" instead of being sent to the destination site.
If a URL turns malicious post-delivery, affected emails can be quarantined or removed from inboxes, and the message can be pulled from mailboxes based on the URL indicator.
When sandboxing is not possible prior to click, Proofpoint Isolation can be used to open the site in an isolated environment to prevent exposure to malware, with keyboard

interaction disabled to reduce credential-harvesting risk.

4.1.3.3 Malware & Zero-Day Attachments: Must include deep file inspection and sandboxing capabilities for modern vector payloads.

Yes—Proofpoint includes deep file inspection and integrated sandboxing to detect and block malicious attachments, including modern payload vectors and zero-day threats. Attachments are analyzed using static scanning and dynamic sandbox detonation, with sandboxing providing real-time behavioral analysis and dynamic analysis of code behavior, network activity, credential phishing attempts, and memory forensics (with bare metal support).
Suspicious attachments can be held until verdicts are received, with clean files delivered to inboxes and malicious ones quarantined.
Detection is supplemented by native AV engines (McAfee or F-Secure) for known malware and additional proprietary threat detection using reputation analysis, content inspection, sender profiling, behavioral AI, machine learning, behavioral analytics, and threat intelligence, including identification of PuP files, ransomware indicators, and zero-day threats.
Embedded URLs, QR codes, and images are analyzed via the URL-2-URL Classifier, and threat forensics are available via a web portal or API for SIEM integration.

4.1.3.4 Account Takeover (ATO) Monitoring: Must monitor mailbox rule modifications (e.g., sneaky auto-forwarding rules created by attackers) and anomalous login behaviors across the state infrastructure.

Proofpoint meets this requirement by providing account takeover detection and response capabilities that monitor cloud account activity for suspicious login behavior and post-access attacker actions. Proofpoint Account Takeover Protection analyzes the full ATO lifecycle, detects compromised accounts across Microsoft 365, Google Workspace, and Okta, and provides visibility into mailbox rule changes, MFA changes, file activity, and third-party application changes. Proofpoint can automatically remediate malicious mailbox-rule changes and other post-compromise activity, helping security teams quickly contain and reverse attacker actions

4.1.4 Compliance, Certifications, & Data Security

4.1.4.1 To maximize vendor competition while ensuring rigorous data security for State infrastructure, the vendor solution must meet one of the following compliance pathways. **All customer data must be stored and processed exclusively within the United States**

Proofpoint **Core Email Protection API (CEP API)** can be provisioned to support U.S.-based data residency requirements and provides enterprise-grade controls designed to protect customer data throughout the service lifecycle

4.1.4.2 **Pathway A - Federal Cloud Alignment (FedRAMP)** The vendor must hold a current FedRAMP Authorized (Moderate or High baseline), FedRAMP In-Process, or FedRAMP Ready designation listed on the official FedRAMP Marketplace. FedRAMP Legacy status is not acceptable.

Proofpoint CEP API does not hold any FedRAMP status.

4.1.4.2.1 Vendor should provide the FedRAMP Package ID (PID) for verification.

Proofpoint CEP API does not hold any FedRAMP status.

4.1.4.3 **Pathway B (State Cloud Alignment):** Hold a current **StateRAMP** Category 2 or 3 Authorization, or maintain a reciprocal, active state-level cloud authorization (e.g., TX-RAMP).

Proofpoint CEP API does not hold any StateRamp status.

4.1.4.4 **Pathway C (Commercial Enterprise Security Framework):** Hold a validated **SOC 2 Type II** certification *plus* a signed addendum outlining **Strict Data-Isolation Protocols.** This protocol must explicitly verify:

Proofpoint undergoes annual SOC 2 Type II audits covering the Availability, Confidentiality, and Security trust services principles, performed by Schellman & Co.These certifications and audits apply to both its solutions and the hosting environments.

4.1.4.4.1 State of West Virginia data is logically or physically isolated from other commercial tenants.

Yes—tenant data is logically isolated from other tenants in a shared, multi-tenant environment (i.e., not physically separated).
Logical separation is enforced at the application and database layers using unique tenant identifiers (e.g., Customer GUIDs) and customer-specific unique keys that scope queries and responses to the applicable tenant.
Dedicated single-tenant capabilities are not provided; segregation is maintained through the use of unique Customer GUIDs and encryption keys.
Access to tenant data is restricted by role-based controls, transactions use unique IDs for authorization, access is logged/auditable, and data is encrypted with AES-256 at rest and over HTTPS/TLS in transit.

4.1.4.4.2 The solution uses end-to-end data encryption both at rest (AES-256) and in transit (TLS 1.3).

Yes, the solution uses end-to-end data encryption, including AES-256 encryption for data at rest and TLS 1.3 encryption for data in transit.

4.1.4.4.3 Vendor employees have no zero-trust or un-audited access to mailbox contents.

No Proofpoint personnel can access client data or email unless specifically asked by the customer (for example, to help analyze email in quarantine).
Access to customer data hosted in Proofpoint services is granted based on role (primarily support and operations), and when Proofpoint support personnel access customer data as part of customer-requested troubleshooting, all access is logged.

4.1.4.4.4 Alignment with **NIST SP 800-53** or **ISO/IEC 27001** cybersecurity frameworks.

Yes. Proofpoint's Information Security program is based on the requirements of NIST 800-53 and ISO 27001.
Proofpoint maintains an information security governance program aligned with NIST SP 800-53 and is certified to ISO/IEC 27001.
Security controls are audited annually as part of a SOC 2 Type II audit covering the Availability, Confidentiality, and Security trust services principles, and are also assessed as part of the ISO 27001 certification process.
Information Security Policies are reviewed annually by all employees and approved by the Security Governance Committee.

4.1.5 Administrative & Incident response Automation

4.1.5.1 Automated Remediation (Search & Destroy): When a threat is detected in one mailbox, the tool must have API permissions to automatically find and claw back (quarantine) identical malicious emails across all 22,000 state mailboxes globally in seconds of detection. This must include messages in all domains, agencies, OUs, shared mailboxes, delegated mailboxes, and any mailbox where the malicious message exists. Automated remediation must execute without manual administrator approval and must support SOAR-triggered workflows

Yes—Proofpoint's Core Email Protection with Targeted Attack Protection (TAP) and Threat Response can automatically remediate (remove or quarantine) malicious emails post-delivery, including retroactive remediation of emails delivered to user inboxes in the last 14 days when new Indicators of Compromise (IoCs) are ingested, with no limitation on the number of mailboxes or emails remediated at a time.
Threat Response Auto-Pull (TRAP) automatically captures TAP alerts and can automatically move a malicious email and any forwarded copies from Exchange 2010, 2013, 2016, Office 365, GSuite, and Domino inboxes into an administrator-only quarantine; there is no limit on the number of mailboxes TRAP will attempt to access and it will access as many mailboxes as allowed by Exchange simultaneously.
Built-in SOAR capabilities and API integrations are available to orchestrate and automate incident response workflows, including automated removal/quarantine of malicious emails.

4.1.5.2 Role-Based Access Control (RBAC): Must support granular administrative controls allowing specific state department IT staff access to view logs only for their own respective agencies. RBAC must support multi-agency separation, delegated administration, and audit logging of all administrative access.

Yes. Proofpoint's Information Protection Platform and Proofpoint's Data Security Platform support granular Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) to restrict access for individuals and groups, including limiting SOC analyst access to only incidents within their remit and only to incident content appropriate to their role. Administrators can be assigned roles for server administration, user administration, and policy creation, and permissions can be defined down to specific views, reports, incidents, and incident event data; access can also be narrowed further by configuring views so only certain data is visible to specific users or groups.
Access can be managed through predefined roles (e.g., Admin, Viewer; Admin, View-only Admin, Config Admin) and can be customized, with roles and view scoping assignable to users individually or via groups.