The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 3

List View

General Information | Contact | Default Values | Discount | Document Information | Clarification Request

Procurement Folder: 2028979

Procurement Type: Central Master Agreement

Vendor ID: VS0000053520

Legal Name: Cyber Defense Advisors

Alias/DBA: CDA

Total Bid: $1,606,000.00

Response Date: 08/25/2026

Response Time: 12:37

Responded By User ID: siegelba

First Name: Bryan

Last Name: Siegel

Email: bsiegel@cyberdefenseadvis

Phone: 5408411410

SO Doc Code: CRFQ

SO Dept: 0231

SO Doc ID: OOT2700000005

Published Date: 8/18/26

Close Date: 8/25/26

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum No 1-Advanced Email Security

Total of Header Attachments: 3

Total of All Attachments: 3

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

State of West Virginia
Solicitation Response

Proc Folder:	2028979
Solicitation Description:	Addendum No 1-Advanced Email Security
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2026-08-25 13:30	SR 0231 ESR08252600000001336	1

VENDOR

VS0000053520
Cyber Defense Advisors

Solicitation Number: CRFQ 0231 OOT2700000005

Total Bid: 1606000 **Response Date:** 2026-08-25 **Response Time:** 12:37:49

Comments:

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

Vendor
Signature X **FEIN#** **DATE**

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Core Detection	22000.000	EA	18.000000	396000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

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.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Core Detection - Year 2 (Optional Renewal)	22000.000	EA	18.000000	396000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

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.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Core Detection - Year 3 (Optional Renewal)	22000.000	EA	18.500000	407000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

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.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Core Detection - Year 4 (Optional Renewal)	22000.000	EA	18.500000	407000.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

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.

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

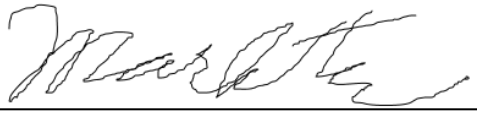
BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code: VS0000053520
Vendor Name : Cyber Defense Advisors (CDA, LLC)
Address :
Street : 100 S. Ashley Rd
City : Tampa
State : Florida **Country :** USA **Zip :** 33602
Principal Contact : Mark Hale
Vendor Contact Phone: 937-620-3378 **Extension:**

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

Vendor Signature X  **FEIN#** 87-4233337 **DATE** 8/24/2026

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

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		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Core Detection	22000.00000	EA	$18	$396,000

Comm Code	Manufacturer	Specification	Model #
43230000	PhishFirewall	PhishEQ	

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		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Core Detection - Year 2 (Optional Renewal)	22000.00000	EA	$18	$396,000

Comm Code	Manufacturer	Specification	Model #
43230000	PhishFirewall	PhishEQ	

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	WV OFFICE OF TECHNOLOGY
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Core Detection - Year 3 (Optional Renewal)	22000.00000	EA	$18.50	$407,000

Comm Code	Manufacturer	Specification	Model #
43230000	PhishFirewall	PhishEQ	

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	WV OFFICE OF TECHNOLOGY
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Core Detection - Year 4 (Optional Renewal)	22000.00000	EA	$18.50	$407,000

Comm Code	Manufacturer	Specification	Model #
43230000	PhishFirewall	PhishEQ	

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

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Mark Hale

(Address) 100 S. Ashley Rd, Tampa, FL 33602

(Phone Number) / (Fax Number) 9376203378

(email address) mhale@cyberdefenseadvisors.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

CDA, LLC
(Company)

(Signature of Authorized Representative)

Mark Hale - VP of Partnershps and Business Development 8/24/2026
(Printed Name and Title of Authorized Representative) (Date)

9376203378
(Phone Number) (Fax Number)

mhale@cyberdefenseadvisors.com
(Email Address)

WEST VIRGINIA OFFICE OF TECHNOLOGY

Advanced Email Security

Technical Submission

CRFQ 0231 | OOT2700000005 | Proc Folder 2028979

Offeror	CDA LLC
Proposed platform	PhishEQ + PhishFirewall
Environment	West Virginia Office of Technology Google Workspace environment
Submission status	Technical submission with signed WV CRFQ form and Addendum No. 1 acknowledgement
WV registration	VS0000053520

August 24, 2026

1. Executive Summary

Cyber Defense Advisors (CDA) submits this technical response to the West Virginia Purchasing Division and the West Virginia Office of Technology (WVOT) for Advanced Email Security. CDA proposes PhishEQ by PhishFirewall as the primary email-security platform, delivered and supported by CDA as the prime contractor. PhishEQ is designed for Google Workspace API deployment without MX-record changes and provides continuous protection against phishing, spear-phishing, business email compromise, vendor fraud, impersonation, account takeover, malicious links, malicious attachments, and social-engineering attacks that bypass conventional filtering.

CDA recommends PhishEQ because its large-language-model reasoning engine evaluates the meaning, intent, context, sender-recipient relationship, and behavioral indicators of every inbound and outbound email, while deterministic controls and threat intelligence add authentication, header, URL, attachment, reputation, and sender-behavior evidence. PhishEQ provides human-readable explanations, inbox-native quarantine, time-of-click and post-delivery protection, automated retraction and clawback, account-takeover detection, security-hygiene scanning, and operational reporting. PhishFirewall is included with PhishEQ at no additional charge and extends the program into adaptive awareness, phishing simulation, just-in-time coaching, and human-risk management.

CDA LLC will serve as WVOT's prime-contractor contact and state champion during the build and transition to the new platform. CDA will own the commercial relationship, contracting and invoicing coordination, implementation communications, transition governance, and state-side decisions. PhishFirewall will perform the technical onboarding, API connection, configuration, operation, monitoring, support, reporting, and software administration. After transition, WVOT will work directly with PhishFirewall for day-to-day platform operations. CDA will not act as the MSP or require platform access.

2. Understanding of WVOT's Requirement

The CRFQ describes an open-end contract for Advanced Email Security layered on WVOT's Google Workspace environment. CDA understands the requirement as a need for more than a pre-delivery filter: WVOT needs protection for internal and external email, advanced analysis of intent and relationships, account-takeover detection, suspicious-link and attachment analysis, post-delivery remediation, explainable user and administrator workflows, and measurable operational reporting. The official pricing form provides four annual line items based on an estimated 22,000 mailboxes: base year and three optional renewal years.

Requirement signal	CDA response
Google Workspace API overlay	PhishEQ connects through Google Workspace APIs without MX-record changes and supplements native controls with message analysis, identity-aware detection, inbox-native response, and continuous hygiene improvement.
LLM-based email reasoning	PhishEQ evaluates meaning, intent, urgency, relationship dynamics, authentication, URLs, attachments, sender behavior, and identity risk, then explains its decision in human-readable language.
Phishing, BEC, and vendor fraud	Layered detection covers targeted social engineering, BEC, vendor compromise, executive and brand impersonation, payment-change fraud, spoofing, lookalike domains, and credential harvesting.
Account takeover and identity risk	PhishEQ evaluates suspicious login, MFA fatigue, forwarding, delegation, OAuth, device, location, mailbox-rule, and anomalous outbound-email indicators, with guided containment and evidence preservation.
Post-delivery threats	Continuous monitoring, time-of-click analysis, message retraction, tenant-wide clawback, quarantine, blocking, notification, and remediation address threats that become malicious after delivery.
Security hygiene	PhishEQ assesses SPF, DKIM, DMARC, domain spoofing exposure, risky configurations, policy gaps, exceptions, allow lists, and identity controls, then tracks prioritized improvements.
PhishFirewall human-risk extension	The normally standalone PhishFirewall platform is included with PhishEQ and automates adaptive education, simulation, remediation, compliance training, and reporting across the 22,000-user environment.
22,000 mailbox estimate	Price as a per-mailbox annual subscription; actual usage remains subject to the State's estimate-only treatment and monthly true-ups.
Open-end / renewals	Years 2, 3, and 4 are separately priced optional renewal periods on the State pricing form.

3. Recommended Solution: PhishEQ by PhishFirewall

3.1 Proposed architecture

- Google Workspace remains the system of record for mail and identity. PhishEQ is layered through API access as an Integrated Cloud Email Security control for message analysis, identity-aware detection, policy enforcement, investigation, inbox-native quarantine, security-hygiene assessment, sandboxing, and remediation. The approach strengthens WVOT's existing Google Workspace investment without requiring an MX-record change or a wholesale mail-platform change.

3.1.1 Google Workspace API integration and authorization

PhishEQ uses a Google Cloud service account with Google Workspace domain-wide delegation. A WVOT Google Workspace Super Admin authorizes the service account's OAuth client ID and scope list in Admin console API Controls. PhishEQ then impersonates authorized Workspace users for the selected APIs; individual end-user consent is not required. The deployment is API-based and does not require an MX-record or mail-routing change.

Required Google services include the Gmail API for mailbox read/modify actions, watch registration, message handling, and simulation-message insertion; the Admin SDK Directory API for user, domain, group, and security-status operations; the Admin SDK Reports API for audit activity; the Google Workspace Alert Center API when Alert Center collection is enabled; and Google Cloud Pub/Sub for Gmail push notifications. Gmail watches publish to a pre-existing project topic.

The current base OAuth scopes are:

- https://www.googleapis.com/auth/gmail.modify
- https://www.googleapis.com/auth/gmail.insert
- https://www.googleapis.com/auth/admin.directory.user
- https://www.googleapis.com/auth/admin.directory.user.readonly
- https://www.googleapis.com/auth/admin.directory.user.security
- https://www.googleapis.com/auth/admin.directory.domain.readonly
- https://www.googleapis.com/auth/admin.directory.group.readonly
- https://www.googleapis.com/auth/admin.reports.audit.readonly

Capability-specific scopes are https://www.googleapis.com/auth/apps.alerts for Alert Center collection, https://www.googleapis.com/auth/gmail.settings.basic for mailbox-filter and basic-settings remediation, and https://www.googleapis.com/auth/gmail.settings.sharing for automatic forwarding, forwarding-address, and delegate remediation. The two Gmail settings scopes are requested by a separate remediation client; if they are not granted, core mail processing remains available but mailbox-settings remediation is unavailable.

Google Workspace prerequisites are a tenant and Super Admin, a Google Cloud project and service account with domain-wide delegation enabled, the required APIs enabled, the service-account client ID and exact scopes entered under Admin console > Security > Access and data control > API Controls > Manage Domain Wide Delegation, an approved mailbox identity for impersonation, a Pub/Sub topic and reachable push endpoint for real-time monitoring, and customer-approved credential storage and rotation.

3.1.2 Microsoft 365 and Microsoft Entra API integration

PhishEQ uses a multitenant Microsoft Entra application with the OAuth 2.0 client-credentials flow. Tokens are requested from the customer tenant using https://graph.microsoft.com/.default, with effective access controlled by Microsoft Graph application permissions granted through tenant-wide administrator consent.

The current Microsoft Graph application permissions are:

- Mail.ReadWrite.All (legacy token alias accepted: Mail.ReadWrite)
- MailboxSettings.ReadWrite
- eDiscovery.Read.All
- eDiscovery.ReadWrite.All
- SecurityEvents.Read.All
- SecurityAnalyzedMessage.Read.All
- ThreatSubmission.Read.All
- Organization.Read.All
- Policy.Read.All
- Application.Read.All

- DelegatedPermissionGrant.ReadWrite.All
- User.Read.All
- User.EnableDisableAccount.All
- User-PasswordProfile.ReadWrite.All
- User.RevokeSessions.All

Microsoft 365 prerequisites are a Microsoft 365 / Microsoft Entra tenant, an Entra administrator authorized to grant tenant-wide application consent, a multitenant app registration and tenant-specific consent flow, an approved redirect URI, the configured permission set, an approved client secret, certificate, or federated credential, permission to create and renew Microsoft Graph message subscriptions, and the customer tenant ID and primary domain. GCC High, DoD, and other national-cloud endpoints require endpoint and permission validation before commitment.

During onboarding, PhishFirewall validates tenant consent and confirms that the approved Google Workspace or Microsoft Graph permissions support the selected PhishEQ capabilities. CDA coordinates the state-side approvals and transition; PhishFirewall performs the technical connection, validation, and platform operation.

3.1.3 Administration, support, and data controls

PhishEQ provides tenant-scoped role-based administration, custom roles, parent/child tenant hierarchies, and server-side scope enforcement for delegated administration and agency separation. Built-in roles include System Owner, Super Administrator, Administrator, Security Analyst, Viewer, Tenant Administrator, and Quarantine User. Custom roles can limit access to mail actions, incidents, users, roles, integrations, settings, API keys, audit logs, reporting/export, security lists, quarantine, and tenant administration.

Tenant Administrator supports delegated-tenant and subtenant administration. Viewer is read-only. Account-takeover remediation is separately permissioned as remediate_accounts, while audit visibility and export are separately controlled. Administrative and account-takeover actions are journaled with tenant ID, incident ID, timestamp, action type, trigger, outcome, error, duration, metadata, and actor information such as user ID, email, source IP, user agent, and request ID. Refused actions are recorded as blocked.

PhishFirewall's support workflow uses the support portal and designated escalation channels for support, bug, and feature-request tickets. Tickets support low, normal, high, and critical priority, assignment, status tracking, attachments, and customer notifications. Critical events include material protection failure, production outage, active security incident, or suspected data-security event and activate the incident-response and engineering escalation path. Support coverage, service availability, maintenance communications, and security-incident procedures are governed by the applicable customer agreement and security terms.

PhishFirewall protects customer data with encryption in transit and at rest, dedicated secret-management controls, and logical tenant isolation. Customer data, users, roles, integrations, policies, security records, and administrative access remain tenant-scoped. Operational email snapshots are retained for 90 days by default; quarantine, incident, and audit records follow the configured retention policy and applicable service terms. Customer data is securely deleted from active systems under the applicable deletion procedures, with backup aging managed through the backup lifecycle. Customer data is used to provide, operate, secure, support, and improve the customer's services and is not used to train shared or general-purpose AI models.

PhishFirewall maintains a current security and compliance documentation package for qualified customer review. Available materials include:

- Privacy and data-handling documentation.
- Google Workspace and Microsoft 365 integration, consent, and permissions documentation.
- Role-based access-control and delegated-administration documentation.
- Data storage, tenant-isolation, retention, backup, and deletion documentation.
- Security telemetry, incident-response, remediation, and audit-journaling documentation.
- Security-awareness, phishing-simulation, phishing-reporting, and platform-operational documentation.

PhishFirewall aligns its security-awareness and training content to common compliance frameworks, including SOC

2, ISO 27001, HIPAA, PCI DSS, NIST CSF, and CMMC. Current approved security documents, attestations, and certifications are available to authorized reviewers under the applicable confidentiality process.

3.1.4 CRFQ-specific compliance statements

U.S. data residency: PhishFirewall confirms that all WVOT customer data, including email metadata, threat logs, security evidence, and analysis artifacts, will be stored and processed exclusively within data centers physically located in the United States.

SIEM/SOAR compatibility: PhishEQ supports real-time or near-real-time export of threat and security-event data through JSON, syslog, STIX/TAXII, and API-based delivery. SOAR-triggered actions support global message clawback across State mailboxes, mailbox-rule removal, quarantine and blocking, user notification, evidence preservation, and account-level response actions such as session revocation or account containment.

Google Workspace and Gemini coexistence: PhishEQ operates through Google Workspace APIs without altering mail routing or MX records and does not disable, degrade, or interfere with Google Workspace or Gemini capabilities, including smart replies, AI-generated summaries, context lookups, or native message rendering.

- CDA coordinates the commercial onboarding schedule, WVOT contacts, access approvals, meetings, and state-side decisions. PhishFirewall performs tenant discovery, API connection, mailbox verification, configuration, pilot design, production rollout, policy tuning, reporting, and operational acceptance. CDA remains the reseller and communication bridge and does not administer the PhishEQ environment.
- PhishFirewall will tune the configuration to WVOT's governance requirements, administrative boundaries, incident workflow, user experience, data-retention decisions, and agency structure. CDA will communicate WVOT priorities and obtain state-side decisions, while PhishFirewall maintains the technical configuration and approval controls.

3.2 Capabilities proposed for the response

Capability	Proposed outcome
LLM and behavioral analysis	Evaluate message meaning, intent, urgency, relationship dynamics, authentication, sender behavior, URLs, attachments, and identity signals, with explainable findings.
Phishing, BEC, and impersonation	Detect targeted social engineering, vendor and executive impersonation, lookalike domains, homograph attacks, reply-to changes, payment fraud, and credential harvesting.
Account takeover defense	Surface suspicious login, credential theft, MFA fatigue, anomalous outbound activity, forwarding, delegation, OAuth, device, IP, location, and communication-pattern changes.
Inbox-native quarantine	Keep users in Gmail, explain the risk, and support approved review, release, recovery, and audit workflows without a separate portal.
Email hygiene and posture	Assess SPF, DKIM, DMARC, spoofing exposure, forwarding, delegation, OAuth, MFA, exceptions, allow lists, and policy gaps with prioritized recommendations.
URL and attachment analysis	Apply time-of-click analysis, reputation and redirect inspection, QR/image phishing analysis, file inspection, and true sandboxing for suspicious files.
Automated response	Quarantine, retract, claw back, block, notify, preserve evidence, guide account containment, and support safe release and recovery workflows.
PhishFirewall awareness	Deliver nano-learning, risk- and role-based education, randomized adaptive simulations, just-in-time remediation, RePhish contextual exercises, compliance training, and reporting.
Reporting and oversight	Provide daily and weekly threat summaries, remediation and incident activity, high-risk users and domains, posture findings, trends, audit records, executive summaries, and human-risk metrics.

3.2.1 Explainable AI analysis

PhishEQ uses a large-language-model security reasoning engine as its core analytical layer. Each email receives senior-analyst-style scrutiny, augmented by deterministic controls and threat intelligence. The result is a consistent, explainable verdict that helps users make better decisions and gives administrators a common evidence layer for support, incident response, and audit records.

3.2.2 Identity, account, and relationship intelligence

PhishEQ evaluates impossible travel, suspicious logins, credential theft, MFA fatigue, anomalous outbound activity, mailbox rules, forwarding, delegation, OAuth access, device and location changes, thread identity drift, vendor changes, payment-change requests, unusual urgency, and altered communication patterns. These signals help surface account takeover, vendor compromise, and fraud before the compromised account can spread the attack.

3.2.3 Inbox-native user experience and security hygiene

PhishEQ keeps quarantine review inside the user's normal inbox, explains why a message was isolated, and supports approved review, release, recovery, and audit workflows. It also continually assesses SPF, DKIM, DMARC, forwarding, delegation, OAuth, MFA, exceptions, allow lists, policy gaps, and other hygiene conditions, producing prioritized recommendations that reduce the attack surface over time.

3.2.4 PhishFirewall human-risk automation

PhishFirewall operates as a continuous behavioral-risk program rather than a periodic campaign. It automates scheduling, randomized simulations, risk-based frequency, role-based content, just-in-time remediation, completion monitoring, exception reporting, executive summaries, and future adaptation based on measured behavior. Its dynamic API connectivity, full integration with PhishEQ, multitenancy, and group management support WVOT's agency structure.

3.3 Product and security evidence

- PhishEQ uses API-based Google Workspace integration without MX-record changes. Its LLM-based analysis is augmented by authentication results, headers, URLs, attachments, reputation, sender behavior, communication patterns, identity signals, and threat intelligence. Exact OAuth scopes, administrative permissions, and tenant prerequisites will be established during mobilization.
- PhishEQ includes true sandbox analysis for suspicious attachments and files, alongside inspection for dangerous attachments, macro-enabled documents, encrypted archives, file-type mismatches, malicious URLs, redirects, OAuth-consent attacks, QR-code phishing, and image-based phishing.
- PhishFirewall will provide the technical support and platform operations model directly to WVOT, including monitoring, investigation, remediation, reporting, and product escalation. CDA will champion the build and transition, remain available for commercial matters, and participate in transition governance; CDA will not be part of day-to-day operations.
- PhishEQ processes WVOT data to provide message analysis, account-protection, detection, remediation, reporting, threat intelligence, security-hygiene assessment, and security-awareness services. The platform applies tenant isolation, access controls, audit logging, administrative safeguards, and industry-standard encryption. Data-use, retention, deletion, backup, subprocessor, and incident-notification requirements will be governed by the applicable PhishEQ security and privacy terms and any State SaaS Addendum incorporated into the resulting contract.

4. CDA Delivery and Support Model

4.1 Mobilization and deployment

Schedule convention: API connection, authorization, and full-mailbox verification will be completed within 24 hours after award/NTP, subject to WVOT providing required administrative access. The remaining schedule covers change-managed pilot, staged rollout, tuning, training, and handoff.

Phase	PhishFirewall delivery / CDA reseller and champion role	Acceptance evidence
1. API onboarding - Within 24 hours	PhishFirewall connects and authorizes the Google Workspace API, verifies mailbox population, and records required permissions. CDA schedules the meeting, coordinates WVOT access approvals, and communicates status.	Connection record, verification report, access-control record.
2. Mobilize and design - Days 2-10	PhishFirewall documents policies, alert routing, exception handling, pilot criteria, and security objectives. CDA gathers WVOT decisions, maintains the commercial action log, and coordinates review meetings.	Kickoff notes, approved solution design, test plan, risk register.
3. Pilot - Days 11-20	PhishFirewall enables the controlled cohort, validates detection, false-positive handling, user reporting, and administrative workflows. CDA coordinates WVOT participants and records state acceptance decisions.	Pilot results, issue log, go/no-go decision.
4. Production rollout - Days 21-30	PhishFirewall executes staged deployment, monitors service health, tunes policies, and communicates technical changes. CDA coordinates the WVOT change window and stakeholder communications.	Deployment record, configuration baseline, open-items list.
5. Transition - Days 31-35	PhishFirewall provides technical administrator orientation, operating procedures, reporting cadence, escalation path, and handoff. WVOT identifies the resources who receive training; CDA coordinates the handoff meeting.	Handoff package and acceptance sign-off.
6. First service review - Day 45	PhishFirewall conducts the first operational service review directly with WVOT. CDA participates only for transition or commercial matters when requested.	Initial service-review report and action log.

4.2 Ongoing service management

- CDA will provide a named commercial point of contact during the build and transition, maintain the reseller relationship, coordinate state-side decisions, and champion the move to the new platform. After transition, WVOT will work directly with PhishFirewall for day-to-day administration, operations, support, reporting, and technical matters.
- PhishFirewall will produce and deliver platform-level reporting directly to WVOT. PhishFirewall will conduct operational service reviews with WVOT; CDA may participate in the initial build/transition review or commercial discussions when requested, but will not manage the day-to-day review cadence.
- PhishFirewall will report deployment status, alert trends, significant incidents, remediation activity, policy changes, and coverage recommendations directly to WVOT. CDA will remain informed on material build, transition, and commercial matters without performing operational reporting or analysis.

- After transition, WVOT will communicate directly with PhishFirewall for technical requests, support, platform administration, reporting, and day-to-day operations. CDA will champion the build and transition and remain available for commercial or relationship matters; CDA will not route operational requests or administer the platform.
- Critical technical events will be handled directly between WVOT and PhishFirewall. PhishFirewall will maintain the technical incident record, investigation, remediation, notifications, and closure evidence. CDA will be notified of material build, transition, contractual, or relationship matters but will not perform day-to-day incident handling.

4.3 Technical integration and operations

- Google Workspace: PhishEQ connects through Google Workspace APIs without MX-record changes and applies the same analytical approach to internal and external email. It evaluates message meaning, intent, urgency, financial requests, impersonation, credential-harvesting language, sender-recipient relationships, authentication evidence, URLs, attachments, and communication-pattern changes.
- Time-of-click and post-delivery protection: PhishEQ evaluates URLs at click time, continuously monitors delivered messages, detects links that become malicious after delivery, and supports post-delivery retraction and remediation. When a threat is validated, PhishEQ can identify affected recipients and retract the message across the tenant.
- Dynamic sandboxing: PhishEQ provides true sandbox analysis for suspicious attachments and files and combines those results with file-type, macro, archive, URL, reputation, and behavioral evidence.
- Historical scanning: PhishFirewall will configure and execute the required 90-day historical mailbox scan upon activation, preserving findings for investigation, remediation, and baseline reporting. CDA will champion the build schedule and transition communications; PhishFirewall will operate the scan and communicate technical results directly to WVOT.
- SIEM/SOAR and operational response: PhishEQ supports security-event export, incident creation, evidence preservation, policy-driven response, user and administrator notification, and automated remediation workflows for WVOT security operations and automation tooling.
- RBAC and multi-agency separation: PhishFirewall will configure and administer the platform's role-based access, delegated administration, logical separation, and audit workflows for WVOT administrators, agencies, departments, supervisors, and security operations personnel. CDA will communicate state-side requirements during the build and transition and will not administer the platform.

5. WVOT Requirement and Responsiveness Matrix

This matrix provides CDA's direct response to the WVOT CRFQ requirements and identifies the supporting evidence for each response.

WVOT requirement	CDA / PhishEQ response	Supporting Evidence / Verification Source
CRFQ 4.1.1.1.1 - No gateway / no MX change	Comply - PhishEQ connects through Google Workspace APIs, does not require MX changes, and does not route WVOT mail through an external gateway, relay, or proxy.	Architecture narrative in Part I; PhishEQ integration figure in Appendix A.
CRFQ 4.1.1.1.2 - API-based deployment	Comply - PhishEQ operates through Google Workspace API access and is delivered as a cloud-native SaaS control.	Part I Sections 3.1.1 and 3.1.2; exact OAuth scopes and prerequisites stated above.

WVOT requirement	CDA / PhishEQ response	Supporting Evidence / Verification Source
CRFQ 4.1.1.1.3 - Zero infrastructure / no added latency	Comply - The proposed deployment requires no on-premises appliance, virtual appliance, customer-managed VM, or local agent; analysis is performed through API workflows without changing ordinary mail routing.	Implementation plan in Part I.
CRFQ 4.1.1.1.5 - Native Microsoft 365 parity	Comply - PhishEQ's capability narrative identifies Microsoft 365 and Exchange Online API integration, historical analysis, remediation, mailbox-rule monitoring, time-of-click inspection, and identity-aware protection without MX changes.	Part I Section 3.1.2; exact Microsoft Graph permissions and prerequisites stated above.
CRFQ 4.1.2 - Google Workspace / Gemini coexistence	Comply - PhishEQ operates through Google Workspace APIs and preserves native Workspace and Gemini functionality, including smart replies, AI-generated summaries, context lookups, and native message rendering.	Part I Sections 3.1.1 and 3.1.4; API architecture and Gemini coexistence statement.
CRFQ 4.1.2.1 - Internal-to-internal traffic	Comply - PhishEQ analyzes internal and external email, including lateral phishing, compromised-account activity, vendor fraud, and anomalous internal communications.	PhishEQ technical documentation and Appendix A and Part I response.
CRFQ 4.1.2.3 - Historical scanning	Comply - PhishFirewall will configure and execute the required 90-day historical mailbox scan upon activation, including messages, attachments, and mailbox rules, with findings preserved for investigation, remediation, and baseline reporting.	Part I implementation plan and PhishFirewall 90-day historical scan statement.
CRFQ 4.1.3 - Behavioral and language analysis	Comply - PhishEQ uses LLM reasoning, behavioral baselining, anomaly detection, communication patterns, authentication evidence, and threat intelligence beyond static rules.	PhishEQ technical documentation and Appendix A; Appendix A figures.
CRFQ 4.1.3.1 - BEC and spoofing	Comply - Coverage includes internal and external impersonation, vendor compromise, invoice/payment fraud, executive impersonation, look-alike domains, urgency, and altered communication patterns.	PhishEQ technical documentation and Appendix A.
CRFQ 4.1.3.2 - Time-of-click URLs	Comply - PhishEQ provides real-time URL inspection, redirect-chain and reputation analysis, morphing-link detection, QR/image phishing analysis, and post-delivery remediation, with security events available for operational and automation workflows.	Part I Sections 3.2.5 and 3.1.4; PhishEQ time-of-click and SIEM/SOAR statements.
CRFQ 4.1.3.3 - Malware and zero-day attachments	Comply - PhishEQ provides deep attachment inspection and true cloud sandboxing for suspicious files and modern payloads.	Part I Section 3.2.6 and Appendix A platform evidence.

WVOT requirement	CDA / PhishEQ response	Supporting Evidence / Verification Source
CRFQ 4.1.3.4 - Account-takeover monitoring	Comply - PhishEQ evaluates mailbox rules, forwarding, delegation, OAuth access, suspicious login, impossible travel, MFA fatigue, anomalous outbound activity, and identity-risk indicators.	PhishEQ technical documentation and Appendix A.
CRFQ 4.1.4 - Compliance pathway and US data residency	Comply - PhishFirewall confirms U.S.-only storage and processing for WVOT customer data, including email metadata, threat logs, security evidence, and analysis artifacts. PhishFirewall maintains the current security and compliance documentation package described in Part I Section 3.1.3, including privacy, integration, RBAC, tenant isolation, retention, deletion, incident response, and audit documentation.	Part I Sections 3.1.3 and 3.1.4; current approved security documents, attestations, and certifications available to authorized reviewers under applicable confidentiality terms.
CRFQ 4.1.5.1 - Automated remediation / global clawback	Comply - PhishEQ supports quarantine, post-delivery retraction, global clawback across State mailboxes, blocking, mailbox-rule removal, notification, evidence preservation, and account-level response actions triggered by SOAR workflows.	Part I Sections 3.2.7 and 3.1.4; PhishEQ automated-remediation and SIEM/SOAR statements.
CRFQ 4.1.5.2 - RBAC and multi-agency separation	Comply - The proposed operating model provides agency, department, supervisor, and security-operations separation with delegated administrative workflows and audit records.	Part I Sections 3.4 and 3.5; PhishEQ RBAC, delegated administration, tenant hierarchy, scope enforcement, and audit journaling are confirmed.
CRFQ 4.1.6.1 - Architecture verification	Comply - The Part I architecture narrative and Appendix A evidence show API-based operation inside Google Workspace without intermediary MX routing or gateway proxy.	Part I Sections 3.1.1, 3.1.2, and 3.1.4; API architecture, no-MX deployment, and U.S. data-residency statements.
CRFQ 4.1.6.2 - Compliance verification	Comply - PhishFirewall maintains a current security and compliance documentation package for qualified customer review. Available materials include privacy and data handling, Google Workspace and Microsoft 365 integration and permissions, RBAC and delegated administration, data storage and tenant isolation, retention and deletion, security telemetry, incident response, remediation, audit journaling, and platform operations. PhishFirewall aligns its security-awareness and training content to SOC 2, ISO 27001, HIPAA, PCI DSS, NIST CSF, and CMMC, with current approved documents, attestations, and certifications available to authorized reviewers under applicable confidentiality terms.	PhishFirewall current security and compliance documentation package; authorized-reviewer materials.

WVOT requirement	CDA / PhishEQ response	Supporting Evidence / Verification Source
CRFQ 4.1.6.3 - Under-24-hour onboarding	Comply - PhishFirewall confirms that onboarding and full-mailbox API verification can be completed within 24 hours without disrupting active State communications, subject to WVOT providing the required administrative approvals and access.	PhishFirewall onboarding confirmation; connection record and mailbox verification report.
CRFQ 4.1.6.4 - Flat annual SaaS pricing	Comply - The official pricing pages provide per-mailbox annual pricing for the estimated 22,000 mailboxes, with PhishEQ and PhishFirewall included as stated in Section 6.	Signed WV pricing form and Section 6 commercial response.
CRFQ 6.0 - Optional renewal years	Comply - Years 2, 3, and 4 are separately priced optional renewal periods initiated by WVOT and executed through the required change-order process.	Signed WV pricing form and Section 6.
CRFQ delivery and operations	Comply - CDA provides deployment, training, handoff, support coordination, service reviews, incident tracking, and reporting; cloud delivery avoids physical shipment dependencies.	CDA delivery plan in Part I.
SaaS Addendum and data protection	Comply - CDA accepts the State SaaS Addendum and will perform the applicable data-protection, incident-notification, encryption, U.S. data-location, and contract-stage obligations when incorporated into the resulting contract.	State SaaS Addendum and signed Addendum No. 1 acknowledgement.

6. Compliance and Commercial Response

CRFQ item	Commercial response	Pricing/form treatment
Core Detection - base year - 22,000 EA	$18.00 per mailbox; $396,000 subscription total	Manufacturer: PhishFirewall; product/specification: PhishEQ; model/SKU: none. PhishFirewall is included at no additional cost.
Core Detection - Year 2 optional renewal - 22,000 EA	$18.00 per mailbox; $396,000 subscription total	Monthly true-ups apply to actual mailbox usage.
Core Detection - Year 3 optional renewal - 22,000 EA	$18.50 per mailbox; $407,000 subscription total	Monthly true-ups apply to actual mailbox usage.
Core Detection - Year 4 optional renewal - 22,000 EA	$18.50 per mailbox; $407,000 subscription total	Monthly true-ups apply to actual mailbox usage.

6.1 Commercial structure

The CRFQ's 22,000-mailbox quantity is an estimate, not a guaranteed minimum. The proposed pricing is per mailbox, with monthly true-ups based on actual mailbox usage. Year 2, Year 3, and Year 4 are optional renewal periods and apply only if exercised by WVOT under the resulting contract.

6.2 Included scope and pricing assumptions

The proposed per-mailbox prices include the PhishEQ email-security platform and the PhishFirewall security-awareness and human-risk-management platform at no additional charge. Pricing includes the proposed reseller margin, discounts, applicable taxes, platform fees, licensing, support, reporting, remediation, API use, storage, and implementation, training, and handoff activities described in this response. No separate PhishEQ or PhishFirewall SKU is required; the product name for the State form is PhishEQ.

6.3 CDA commercial responsibility

CDA will remain responsible for the prime-contract relationship, reseller functions, WVOT communications during build and transition, invoicing coordination, commercial schedule, and relationship governance. PhishFirewall will perform technical setup, platform administration, monitoring, operation, technical documentation, support, reporting, and manufacturer escalation directly with WVOT. CDA will not act as an MSP or participate in day-to-day operations.

6.4 Services outside the defined scope

CDA can provide ad hoc consulting requested by WVOT after setup, training, and handoff at $190 per hour. These services are outside the defined implementation and handoff scope, are not included in the official annual subscription line-item totals, and would be performed only when specifically requested and authorized by WVOT.

7. PhishFirewall Partner and CDA Role Alignment

CDA will submit as prime contractor and reseller and will be WVOT's relationship owner and state champion. PhishFirewall will be the proposed technology manufacturer and will perform the technical setup and ongoing operation of the platform. The response presents one integrated platform recommendation with clear separation between CDA's commercial/state-facing role and PhishFirewall's technical service role.

Work area	CDA responsibility	PhishFirewall responsibility
Commercial and relationship management	Prime contract, reseller functions, pricing, invoicing coordination, build/transition communications, and state champion role.	Provide PhishEQ product, licensing, technical documentation, platform operations, reporting, support, and manufacturer escalation directly to WVOT.
Implementation	Champion the build, coordinate WVOT schedules and decisions, and support transition governance; CDA does not perform technical setup.	Perform discovery, API connection, configuration, pilot, rollout, tuning, technical training, and handoff.
Technical operations	Participate in build and transition decisions only; CDA does not administer the platform, require platform access, or act as the MSP.	Administer, monitor, operate, support, report on, and maintain the PhishEQ/PhishFirewall platform directly for WVOT.
Reporting and reviews	Participate in initial build/transition reviews and commercial governance when requested; no day-to-day operational reporting.	Generate and deliver platform telemetry, threat trends, remediation reports, human-risk analytics, service reviews, and support-case updates directly to WVOT.

Work area	CDA responsibility	PhishFirewall responsibility
Incident escalation	Remain informed of material contractual or relationship matters; no day-to-day incident triage or technical routing.	Work directly with WVOT to investigate incidents, perform technical remediation, preserve evidence, and provide closure evidence.

APPENDIX A - INTEGRATED PHISHFIREWALL PLATFORM VALUE-ADD

PhishEQ supplies the technical email-security, identity, remediation, and security-hygiene layer. PhishFirewall extends that protection into human-risk management, adaptive awareness, phishing simulation, just-in-time remediation, compliance training, and behavioral reporting. Together, they provide a continuous defense model for WVOT rather than two separate products operating independently.

A.1 PhishEQ Email Security Capability

PhishEQ applies large-language-model reasoning to every inbound and outbound email, evaluating meaning, intent, urgency, sender-recipient relationships, authentication, URLs, attachments, reputation, sender behavior, communication history, and identity risk. The AI reasoning layer is supplemented by deterministic controls and threat intelligence so that decisions are based on combined evidence rather than a single signature or indicator.

The platform detects phishing, spear-phishing, targeted social engineering, business email compromise, vendor email compromise, payment-change fraud, executive and brand impersonation, look-alike and homograph domains, credential harvesting, OAuth-consent attacks, QR-code and image-based phishing, malicious URLs, dangerous attachments, macro-enabled documents, encrypted archives, and file-type mismatches.

PhishEQ also addresses account takeover and identity risk through suspicious-login and impossible-travel indicators, credential theft, MFA fatigue, anomalous outbound activity, mailbox rules, forwarding, delegation, OAuth access, device and location changes, thread identity drift, and abnormal sender or recipient behavior. These capabilities help identify compromised accounts before they are used to spread phishing, redirect payments, or impersonate employees and vendors.

The user experience keeps quarantine review inside Gmail. Users receive a clear explanation of why a message was isolated and can follow the approved review, release, recovery, and request-for-review workflow without leaving the inbox. Administrators retain approval, release, recovery, and audit capabilities while PhishEQ supports quarantine, post-delivery retraction, global clawback, blocking, notification, evidence preservation, and guided account containment.

PhishEQ continually assesses email-security hygiene, including SPF, DKIM, DMARC, domain-spoofing exposure, forwarding, delegation, OAuth access, MFA posture, risky exceptions, allow lists, policy gaps, and control effectiveness. It provides prioritized recommendations and reporting so WVOT can reduce the attack surface over time rather than only respond to individual messages.

PhishEQ supports API-based Google Workspace and Microsoft 365 integration, historical mailbox analysis, automated remediation, mailbox-rule monitoring, time-of-click URL inspection, identity-aware detection, operational reporting, and security-hygiene improvement without requiring MX-record changes or gateway-based mail routing.

A.2 PhishFirewall Human-Risk Management and Security Awareness

PhishFirewall is a normally standalone, agentic human-risk-management and cybersecurity-awareness platform included with PhishEQ at no additional charge. It automates the continuous cycle of assessment, education, phishing simulation, remediation, measurement, and reporting across WVOT's proposed 22,000-user population, reducing the administrative workload associated with traditional campaign-based programs.

The platform delivers nano-learning modules typically lasting 30 to 60 seconds, risk-based and role-based education, randomized individual-level phishing simulations, susceptibility- and proficiency-based adaptation, just-in-time behavioral remediation, RePhish contextual simulation, mandatory and regulatory training, LMS integration, SCORM export, automated enrollment and reminders, completion monitoring, transcripts, exception reporting, supervisory reporting, and executive summaries.

PhishFirewall adapts the frequency, difficulty, and subject matter of education and simulations to each user's demonstrated behavior. Low-risk users receive maintenance-level reinforcement; moderate-risk users receive more focused education; and high-risk users receive elevated cadence and immediate remediation until improvement is demonstrated. The result is a continuous learning progression rather than repeated generic campaigns.

RePhish allows WVOT to sanitize and reconstruct a real phishing message as a safe simulation for other employees without exposing them to the original malicious links, attachments, credential-harvesting pages, or payloads. It can also transform legitimate organizational communications—such as vendor correspondence, invoices, payment-change requests, document-signing notifications, payroll messages, executive requests, and application notifications—into realistic, controlled exercises.

PhishFirewall converts risky behavior into a teachable moment. When a user interacts with a simulated phish, demonstrates difficulty with a technique, or develops an elevated-risk pattern, the platform can deliver concise contextual remediation, reinforce the desired behavior, measure subsequent performance, and adapt future training. Organizational analytics identify patterns such as low reporting rates, delayed reporting, repeated interaction with urgent financial requests, and excessive trust in familiar vendors.

PhishFirewall reporting can cover training completion, compliance by agency or department, past-due and exception status, individual transcripts, simulation results, interaction and reporting rates, repeat interactions, time-to-report, risk scores, program performance against baseline, supervisory reporting, executive trends, administrative activity, and audit records. Lora automates enrollment, reminders, follow-up, adaptive coaching, evidence collection, and reporting so State security personnel can focus on strategy and risk reduction.

A.3 Integrated Value to WVOT

The integrated platform closes the loop between technical detection and human behavior. PhishEQ detects and explains the threat, protects the inbox, retracts malicious content, identifies identity and hygiene weaknesses, and provides technical evidence. PhishFirewall uses those moments to educate users, simulate the same attack patterns safely, measure behavior, and improve reporting and resilience. CDA provides the reseller, state-champion, build, and transition role while WVOT works directly with PhishFirewall for day-to-day platform operation after transition.

The PhishFirewall value-add response identifies a standard value of $220,000 across 22,000 users. That normally standalone capability is included with PhishEQ at no additional charge.

A.4 Selected Platform Evidence

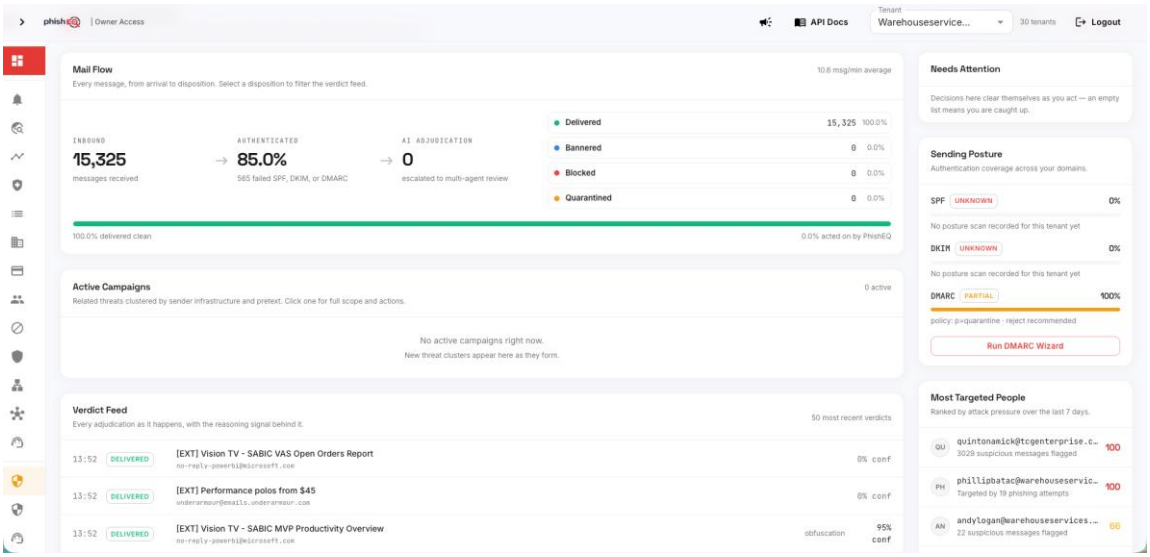
The following figures show the proposed platform's principal workflows and administrative views. Each figure is paired with operational context explaining what the interface demonstrates and how it supports WVOT's security, administration, awareness, reporting, and remediation objectives.

The complete figure set is included so evaluators can review the user, analyst, administrator, reporting, training, and integration workflows in one place.

Figure A.1 | PhishEQ security overview

The overview presents a consolidated view of email-security posture, active findings, risk indicators, and operational status. It is the starting point for understanding the state of protection across the connected environment.

WVOT relevance: WVOT administrators can prioritize investigations, remediation, and control-improvement work from a common operational view.

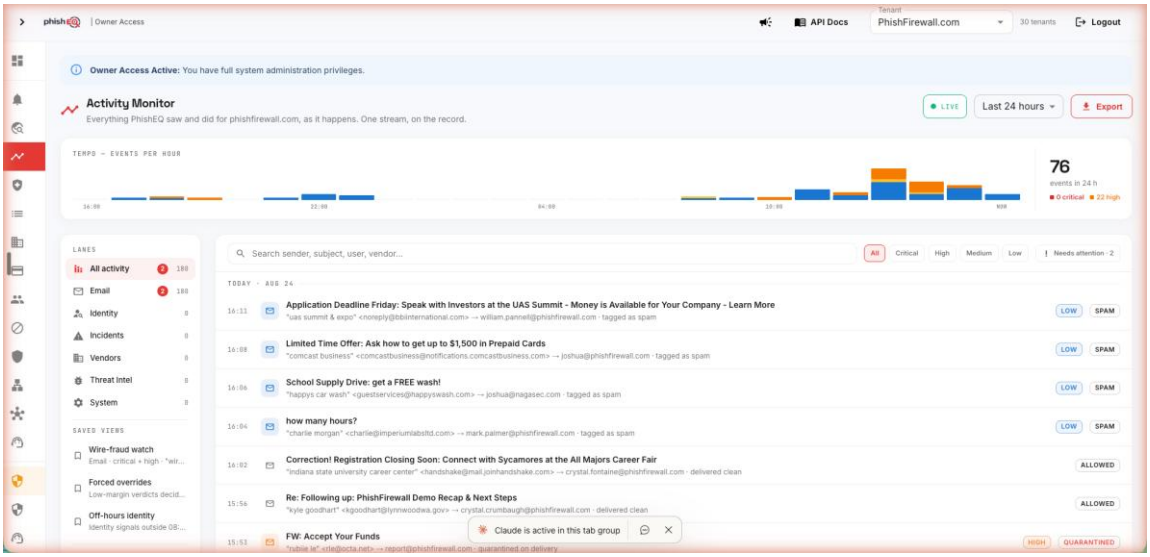


PhishEQ security overview and operational posture.

Figure A.2 | Message analysis and triage

The message-analysis queue organizes messages requiring review and gives analysts a common place to examine message risk, sender context, authentication, links, attachments, and related indicators.

WVOT relevance: This supports explainable review of phishing, BEC, impersonation, malicious links, and suspicious attachments across internal and external email.

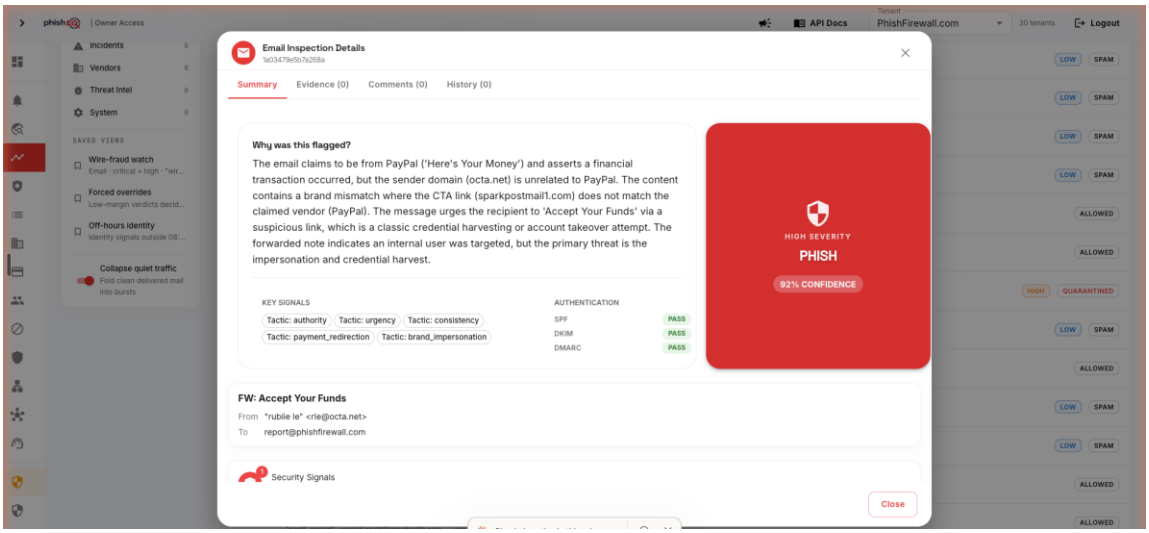


PhishEQ message-analysis and triage view.

Figure A.3 | Phishing verdict explanation

This review screen presents a human-readable explanation of a phishing determination and the indicators supporting the decision. The analyst can see why the message was isolated and what response is appropriate.

WVOT relevance: Explainable findings help WVOT validate decisions, communicate with users, preserve evidence, and apply consistent remediation.

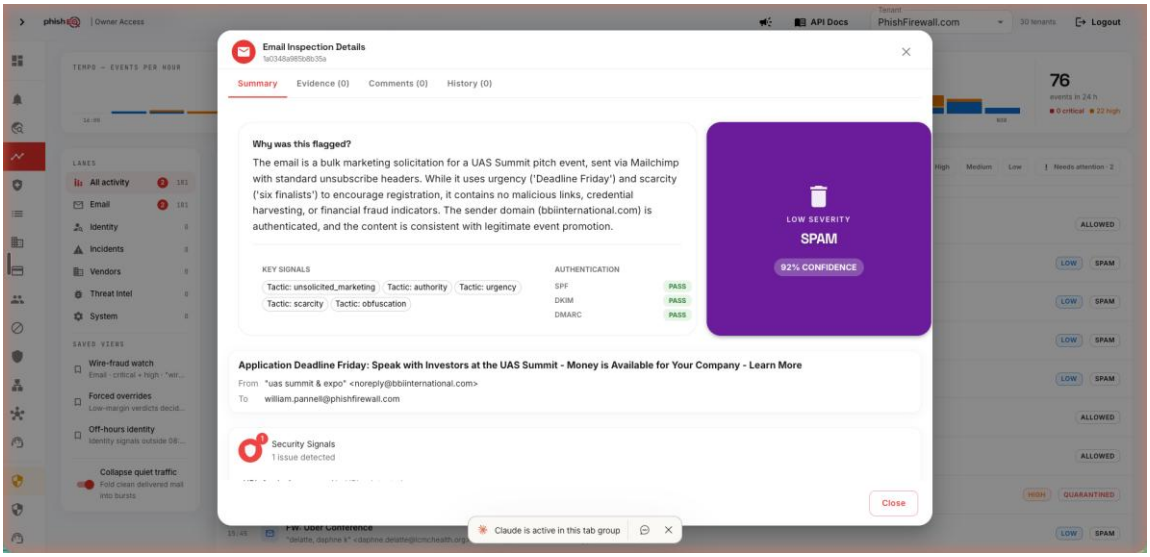


PhishEQ phishing verdict and explanation workflow.

Figure A.4 | Impersonation verdict explanation

This view illustrates analysis of an impersonation or identity-deception event. The platform presents the risk in plain language rather than relying only on a technical score or a single signature.

WVOT relevance: WVOT can investigate executive, vendor, and brand impersonation using a consistent explanation and response workflow.

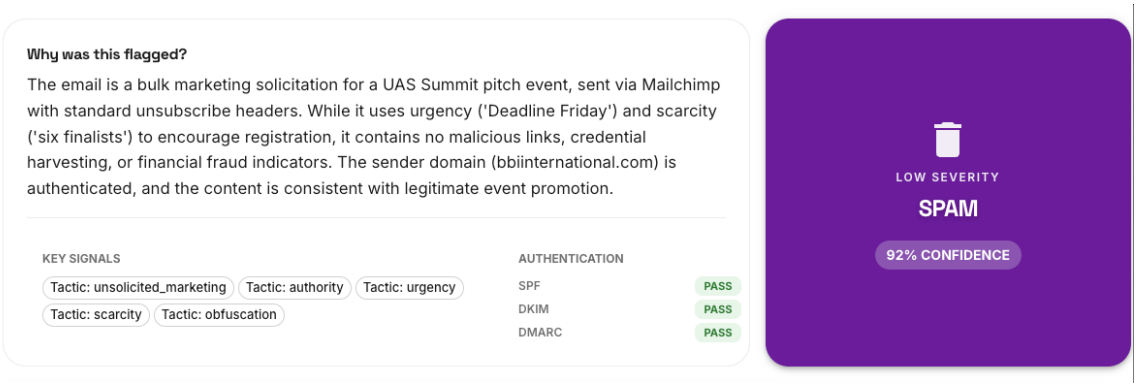


PhishEQ impersonation verdict and explanation workflow.

Figure A.5 | Spam and unwanted-message handling

The message-review workflow also supports classification and handling of unwanted or lower-confidence messages. This helps separate routine message hygiene from high-impact security investigations.

WVOT relevance: WVOT administrators can maintain a cleaner user experience while preserving security focus for phishing, BEC, and account-risk events.

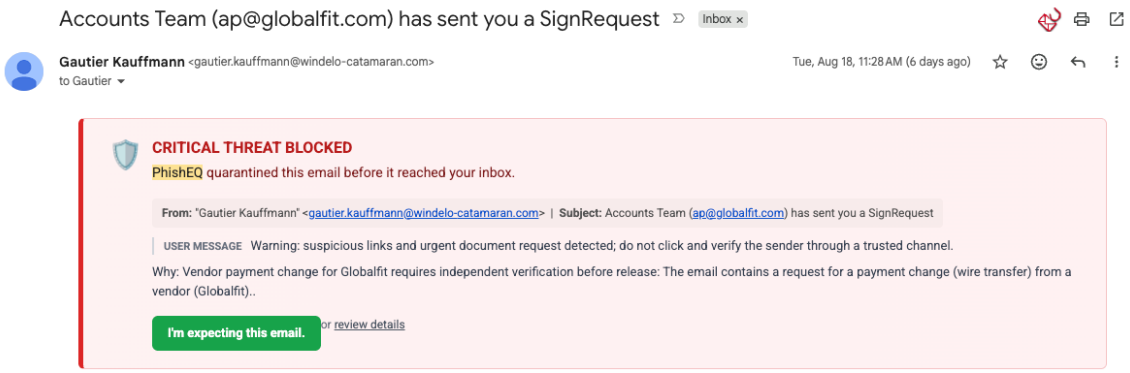


PhishEQ message classification and handling view.

Figure A.6 | Critical threat blocking

This user-facing result shows a dangerous message being blocked with an explanation of the threat and the protective action taken. The workflow communicates the decision without exposing the recipient to the malicious content.

WVOT relevance: The control provides immediate user protection and a clear explanation that can reduce help-desk confusion and unsafe release requests.

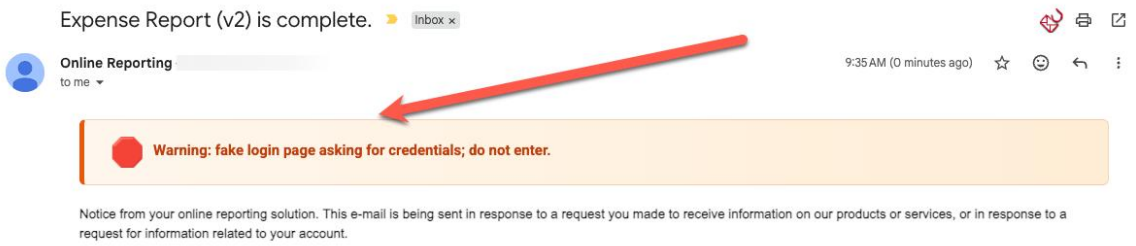


PhishEQ critical-threat blocking experience.

Figure A.7 | Message completion and delivery context

This view shows a message event together with the status and analysis information needed to understand what happened during processing. It supports review of the message, the action taken, and the associated user or sender context.

WVOT relevance: WVOT can trace security decisions and support incident review without treating message delivery as a black box.

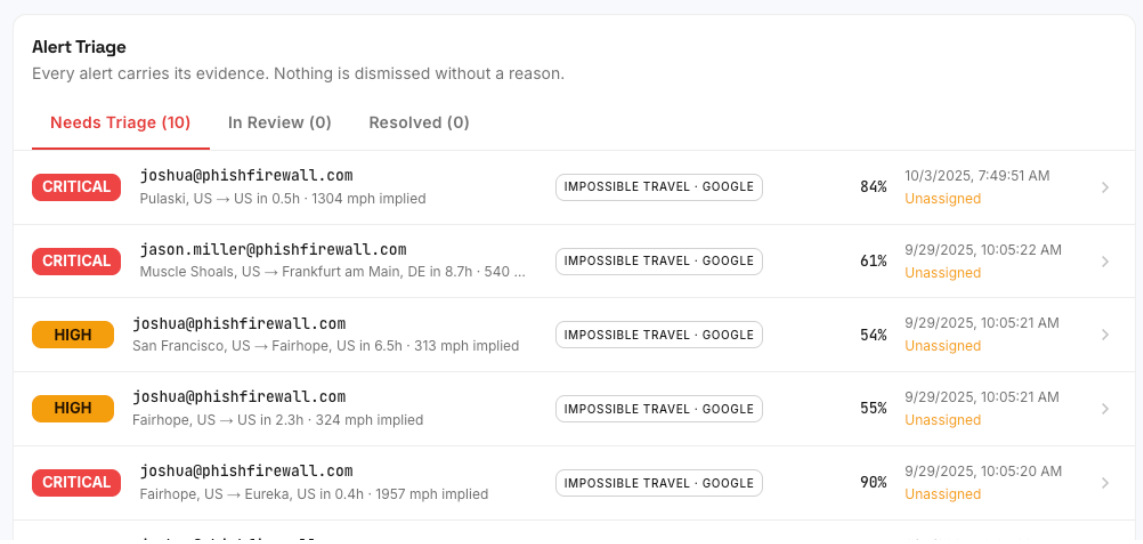


PhishEQ message event and delivery-context view.

Figure A.8 | Alert triage and threat visibility

The alert view organizes findings by severity and status so analysts can identify critical and high-risk events, review evidence, and manage the investigation queue.

WVOT relevance: This supports a manageable operating model for a large mailbox population and provides a visible path from detection to investigation and response.

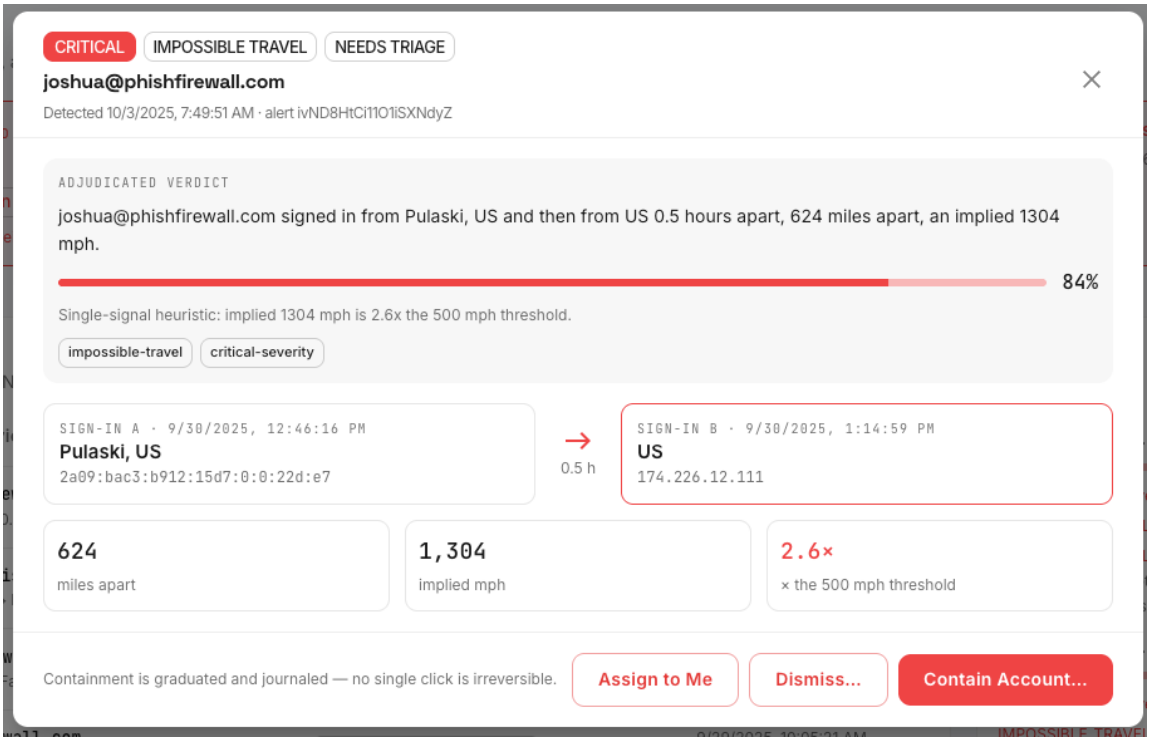


PhishEQ alert triage and threat-visibility view.

Figure A.9 | Account-takeover investigation

The account-risk view illustrates investigation of suspicious access and identity activity, including location or travel anomalies and related account signals. The platform also evaluates credential theft, MFA fatigue, anomalous outbound behavior, forwarding, delegation, OAuth access, and mailbox-rule activity.

WVOT relevance: This extends protection beyond individual messages and helps WVOT identify compromised accounts that may otherwise be used to conduct internal phishing or payment fraud.

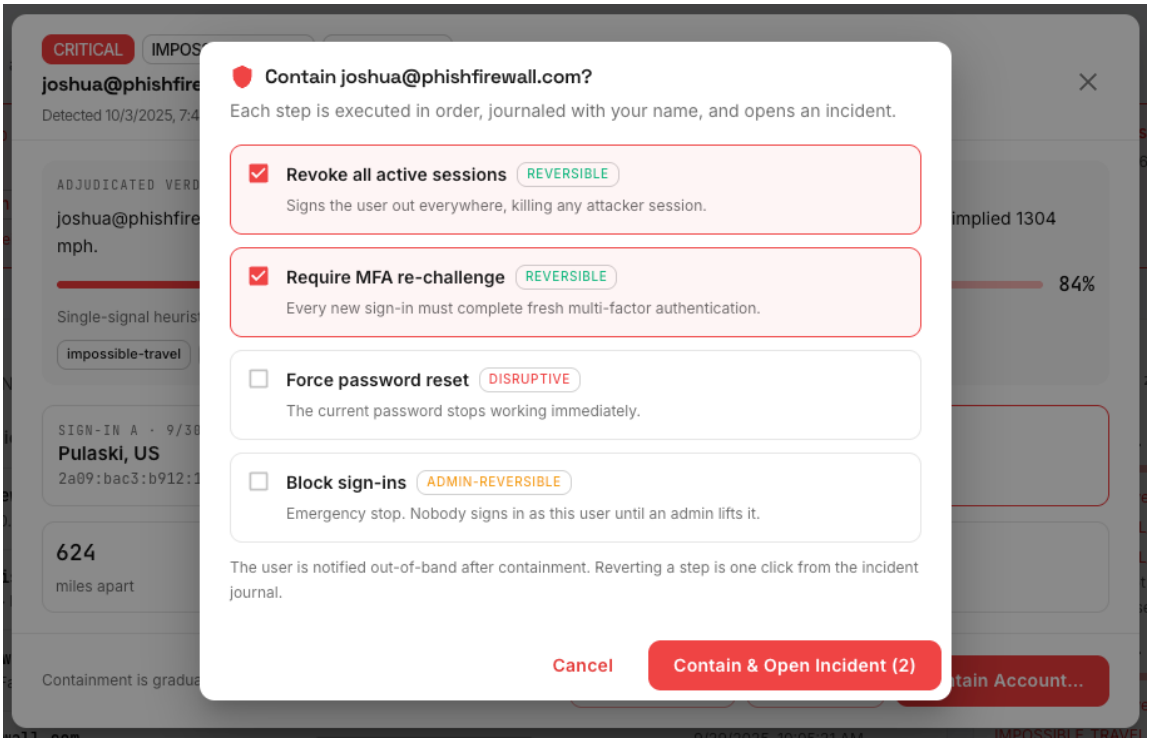


PhishEQ account-takeover and identity-risk investigation.

Figure A.10 | Account activity and containment

This workflow provides additional account-level context for reviewing risky activity and selecting containment or response actions. It connects identity signals to practical incident-response decisions.

WVOT relevance: WVOT analysts can move from an account-risk signal toward review, containment, and recovery while preserving the event context.

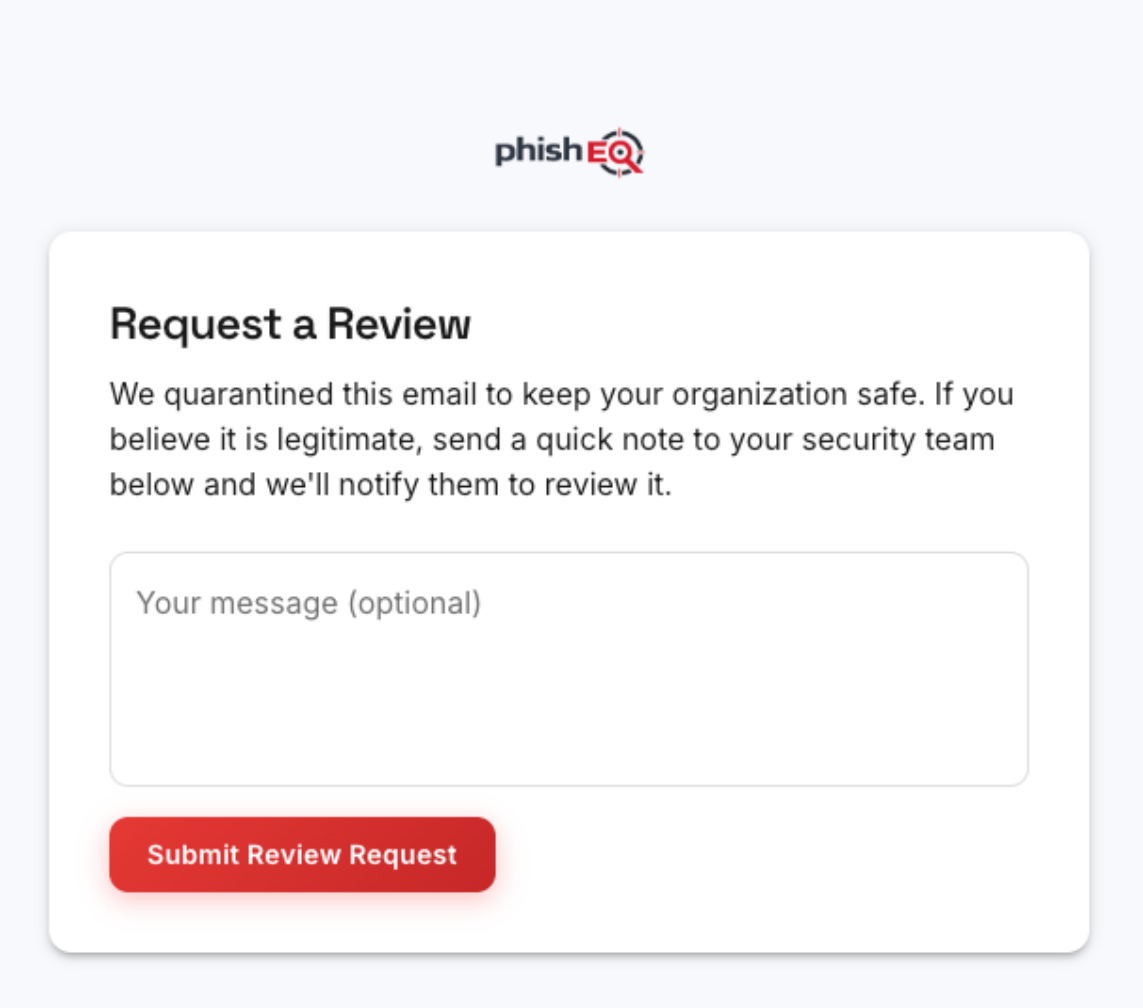


PhishEQ account activity and response workflow.

Figure A.11 | User request-for-review workflow

The request-for-review screen gives users a controlled way to ask for a message to be reconsidered. The process preserves administrator control while providing the user with a clear path to request review.

WVOT relevance: This reduces unsafe workarounds and supports an inbox-native quarantine and recovery experience for WVOT users.

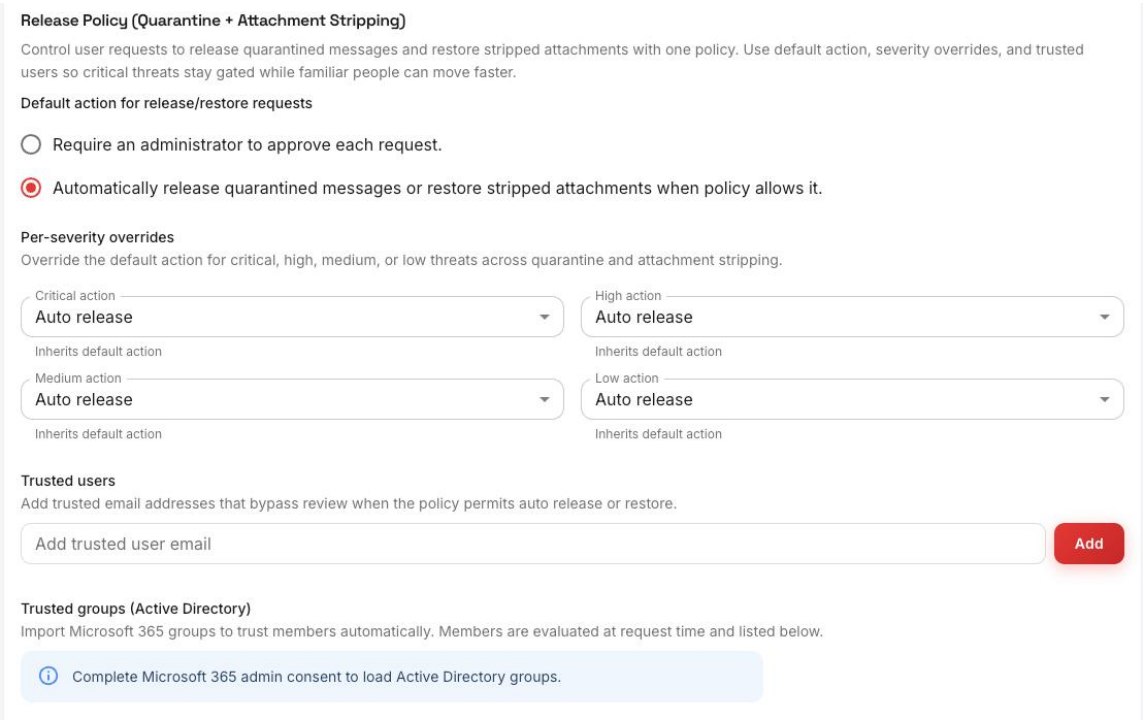


PhishEQ user request-for-review workflow.

Figure A.12 | Policy and security-hygiene controls

The policy view shows administrative controls used to manage detection and response behavior. PhishEQ supports security-hygiene scanning across SPF, DKIM, DMARC, forwarding, delegation, OAuth access, MFA posture, risky exceptions, allow lists, and policy gaps, with prioritized recommendations.

WVOT relevance: This gives WVOT a path to reduce recurring exposure and improve configuration hygiene instead of treating each malicious message as an isolated event.

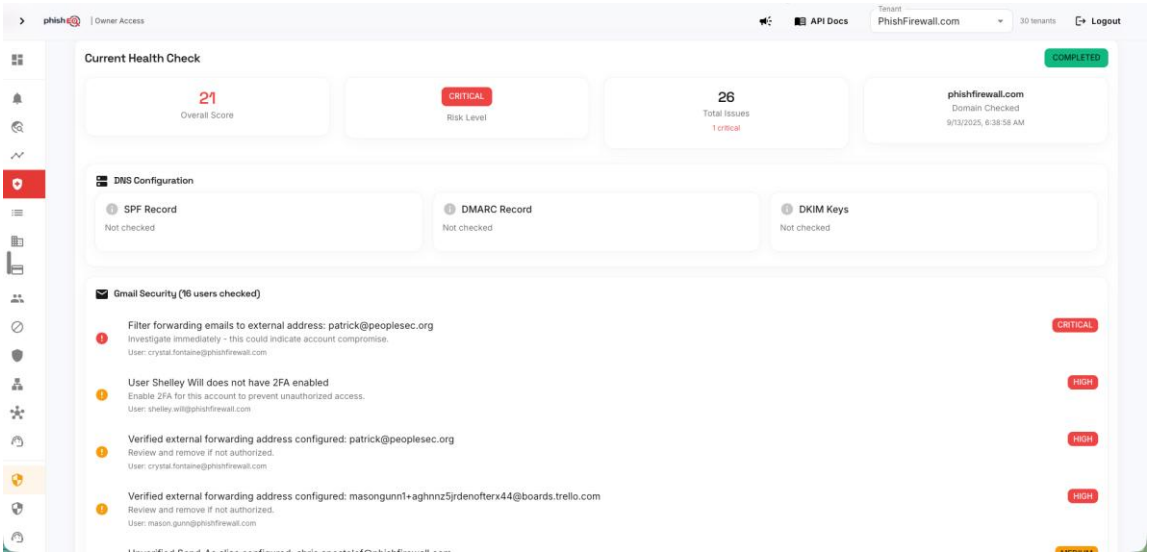


PhishEQ policy and security-hygiene controls.

Figure A.13 | Security findings and remediation status

This dashboard view presents findings and status information used to track security-control effectiveness and remediation priorities. It supports an operational review of what needs attention and what has been addressed.

WVOT relevance: WVOT can use the view for recurring security reviews and to direct remediation toward the highest-value control improvements.

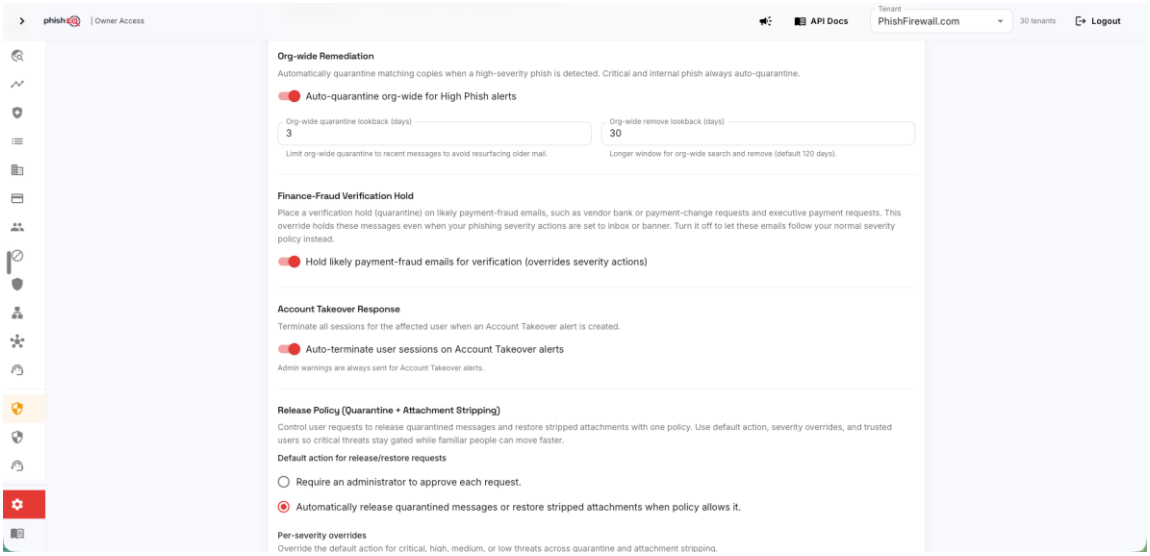


PhishEQ security findings and remediation-status view.

Figure A.14 | Security-hygiene recommendations

The recommendations view presents prioritized findings related to configuration, authentication, identity, and mail-security hygiene. It is designed to turn assessment results into specific improvement actions.

WVOT relevance: This supports continuous improvement of WVOT's Google Workspace security posture and helps document outstanding control work.

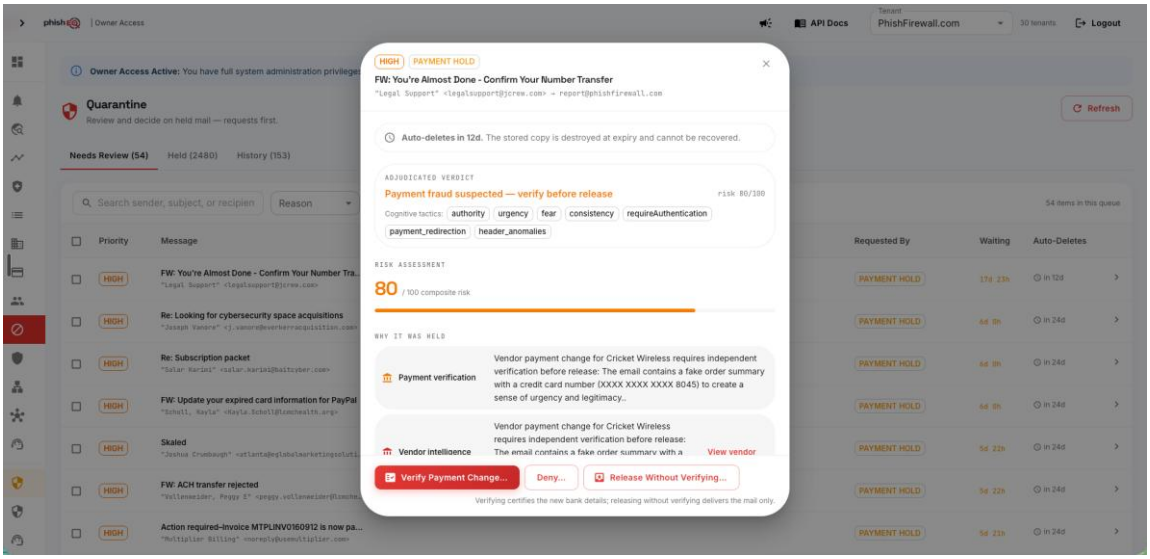


PhishEQ security-hygiene recommendations.

Figure A.15 | Quarantine and recovery actions

This review workflow shows how an administrator can inspect a message and choose an appropriate action while retaining the original context. The available workflow supports review, release, recovery, and related response decisions.

WVOT relevance: WVOT can preserve user access to legitimate messages without weakening the controls used to isolate suspicious content.

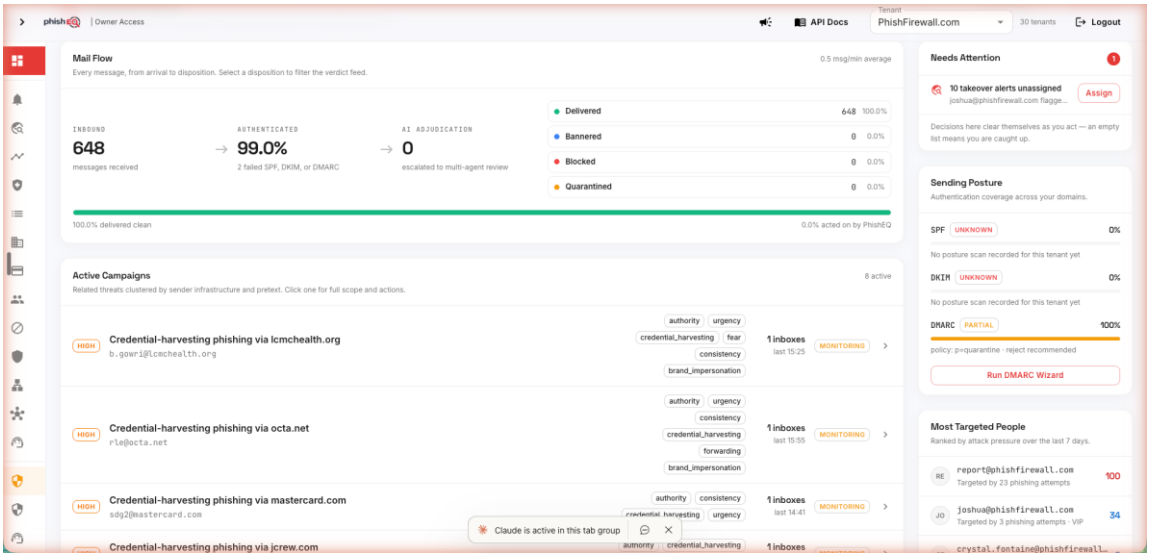


PhishEQ quarantine review and recovery actions.

Figure A.16 | Email-security operations dashboard

The operations dashboard provides a broader view of message activity, risk, and administrative status. It is intended to help security personnel understand trends and operational workload across the protected environment.

WVOT relevance: WVOT can use this view for daily monitoring, leadership updates, and prioritization of response activity.

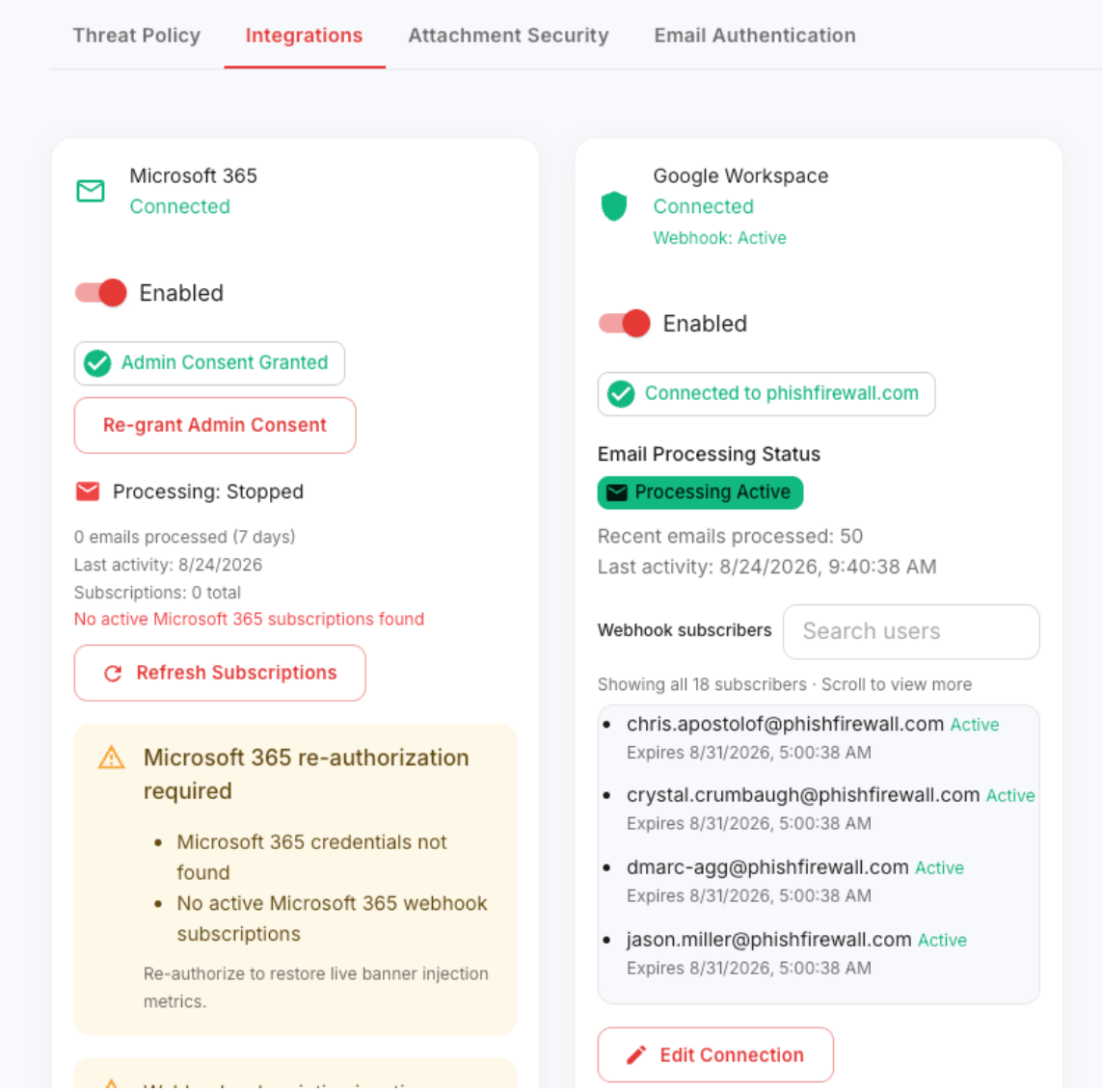


PhishEQ email-security operations dashboard.

Figure A.17 | Google Workspace and Microsoft 365 integration

The integration view identifies the connected cloud-mail environments and the authorization or configuration state for each. PhishEQ is designed for API-based integration with Google Workspace and Microsoft 365 rather than MX-record changes or intermediary gateway routing.

WVOT relevance: This supports WVOT's required native API deployment model and provides a visible administrative path for connection status and platform readiness.

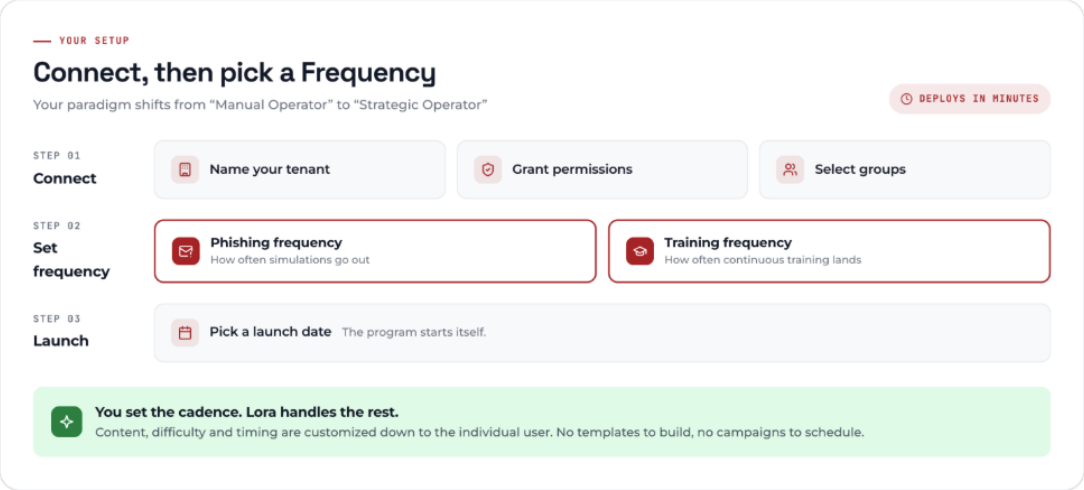


PhishEQ cloud-mail integration and authorization view.

Figure A.18 | Program setup and phishing frequency

The setup workflow lets an administrator connect users or groups to a training program and select the frequency for phishing simulations and education. It is the first step in establishing the program's operating cadence.

WVOT relevance: WVOT can configure a repeatable awareness program aligned to its organizational structure and risk priorities.

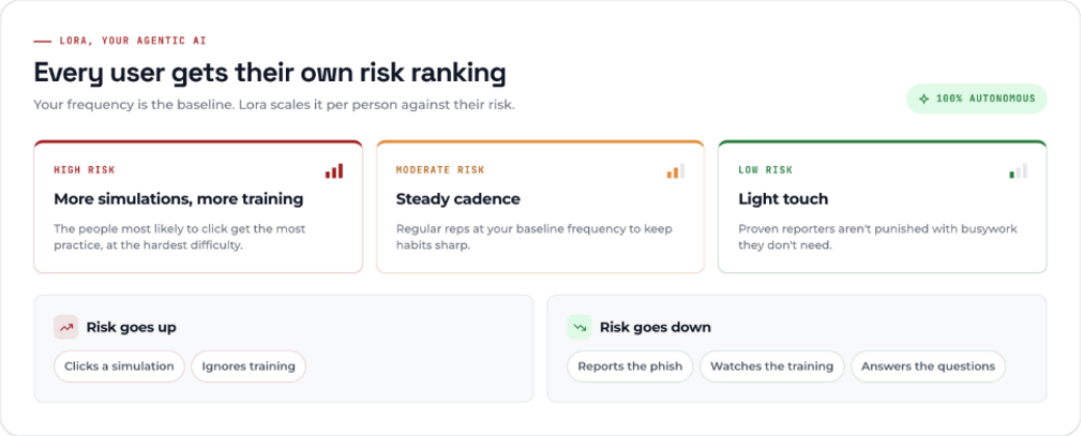


PhishFirewall program connection and frequency setup.

Figure A.19 | Adaptive user-risk ranking

PhishFirewall ranks users by demonstrated behavior and uses those results to adjust education and simulation cadence. Low-, moderate-, and high-risk populations can receive different levels of reinforcement.

WVOT relevance: WVOT can move from uniform annual training to measurable, risk-based human-risk reduction across agencies and departments.

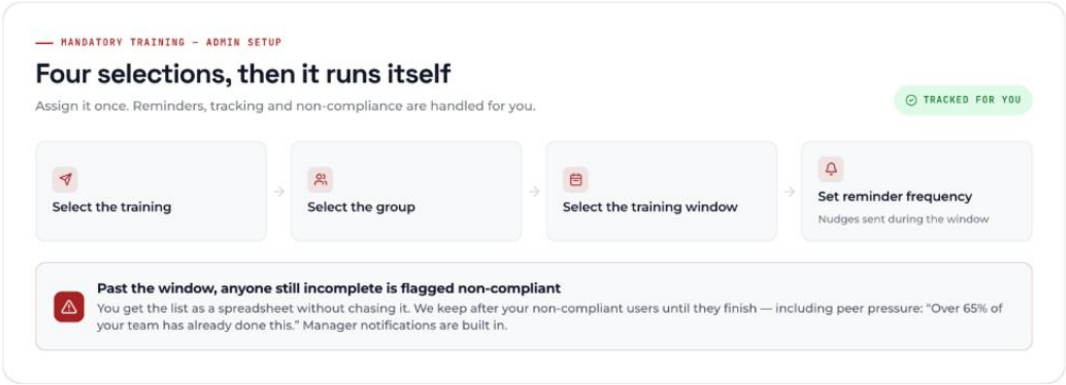


PhishFirewall user-risk ranking and adaptive program design.

Figure A.20 | Simulation design and reuse

This workflow shows how an administrator selects a simulation template, configures the exercise, and reuses a controlled scenario. The program is designed to make simulations repeatable while adapting the exercise to the user's risk and role.

WVOT relevance: WVOT can build a sustainable simulation program without manually rebuilding every campaign from the beginning.

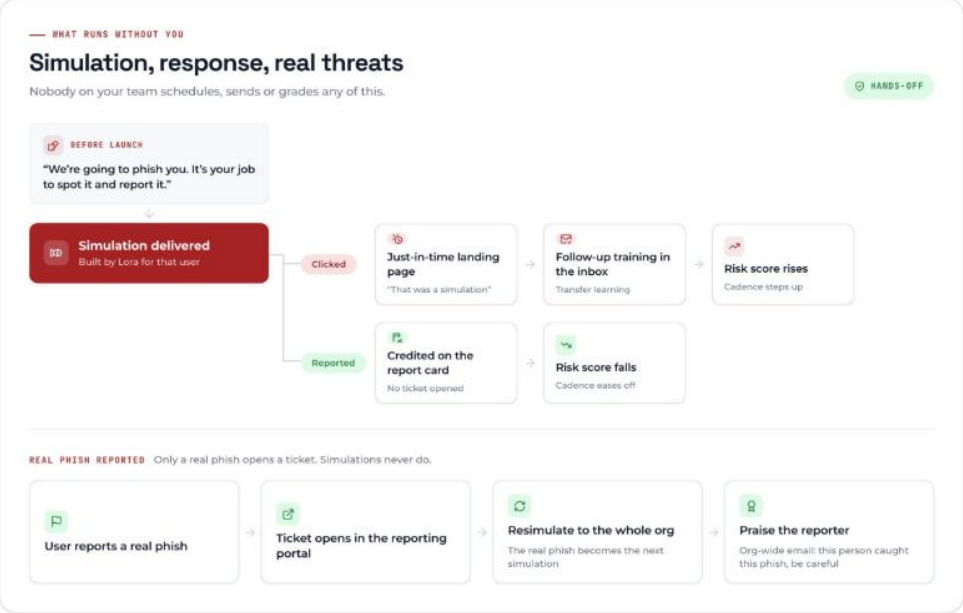


PhishFirewall simulation selection and reuse workflow.

Figure A.21 | Simulation response and threat scenarios

The simulation workflow connects a selected threat scenario with user interaction, feedback, and follow-up education. It supports exercises based on realistic attack patterns rather than generic awareness messages.

WVOT relevance: WVOT can train users against phishing, urgent requests, malicious links, payment fraud, and other social-engineering scenarios in a controlled environment.

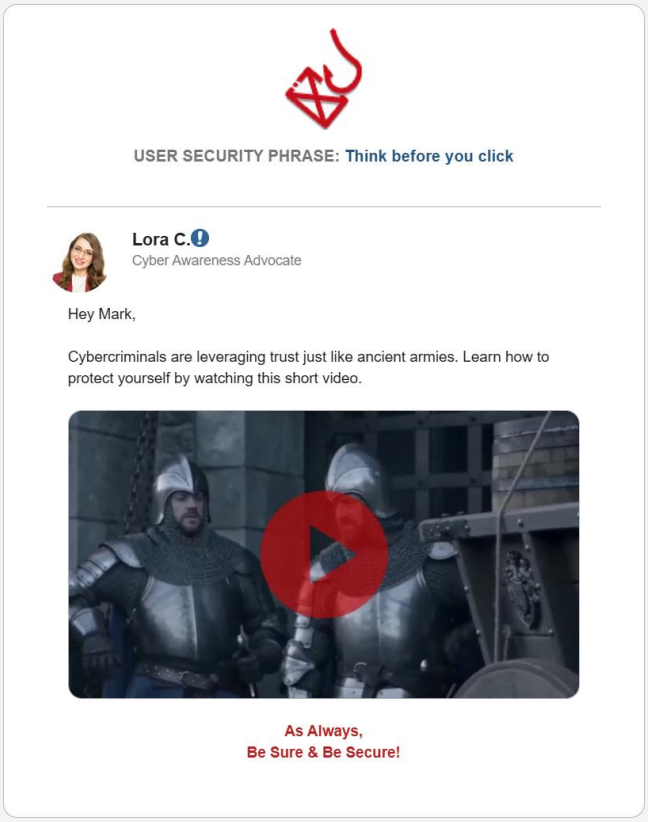


PhishFirewall simulation, response, and threat-scenario workflow.

Figure A.22 | User-facing nano-learning

The user experience delivers a concise awareness lesson directly to the employee. PhishFirewall's nano-learning model typically uses short modules focused on one threat, behavior, or security principle, reducing the time burden on employees.

WVOT relevance: WVOT can deliver frequent, focused education that is more practical for a large and distributed workforce than infrequent lengthy courses alone.

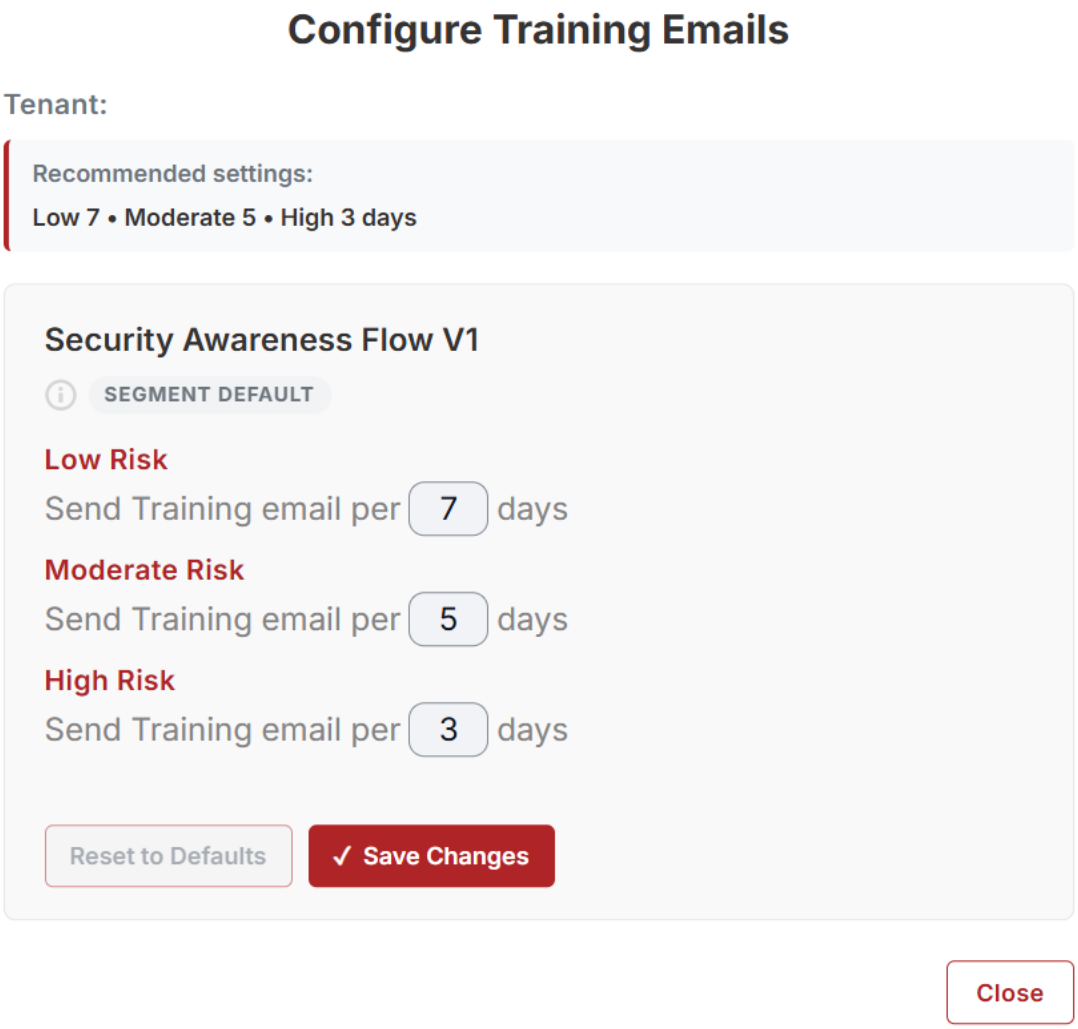


PhishFirewall user-facing nano-learning experience.

Figure A.23 | Training-email configuration

This administrative screen configures the training email cadence and content assigned to different risk levels. It supports targeted education rather than sending identical training to every employee.

WVOT relevance: WVOT can align education frequency to demonstrated risk and maintain a consistent program across departments.

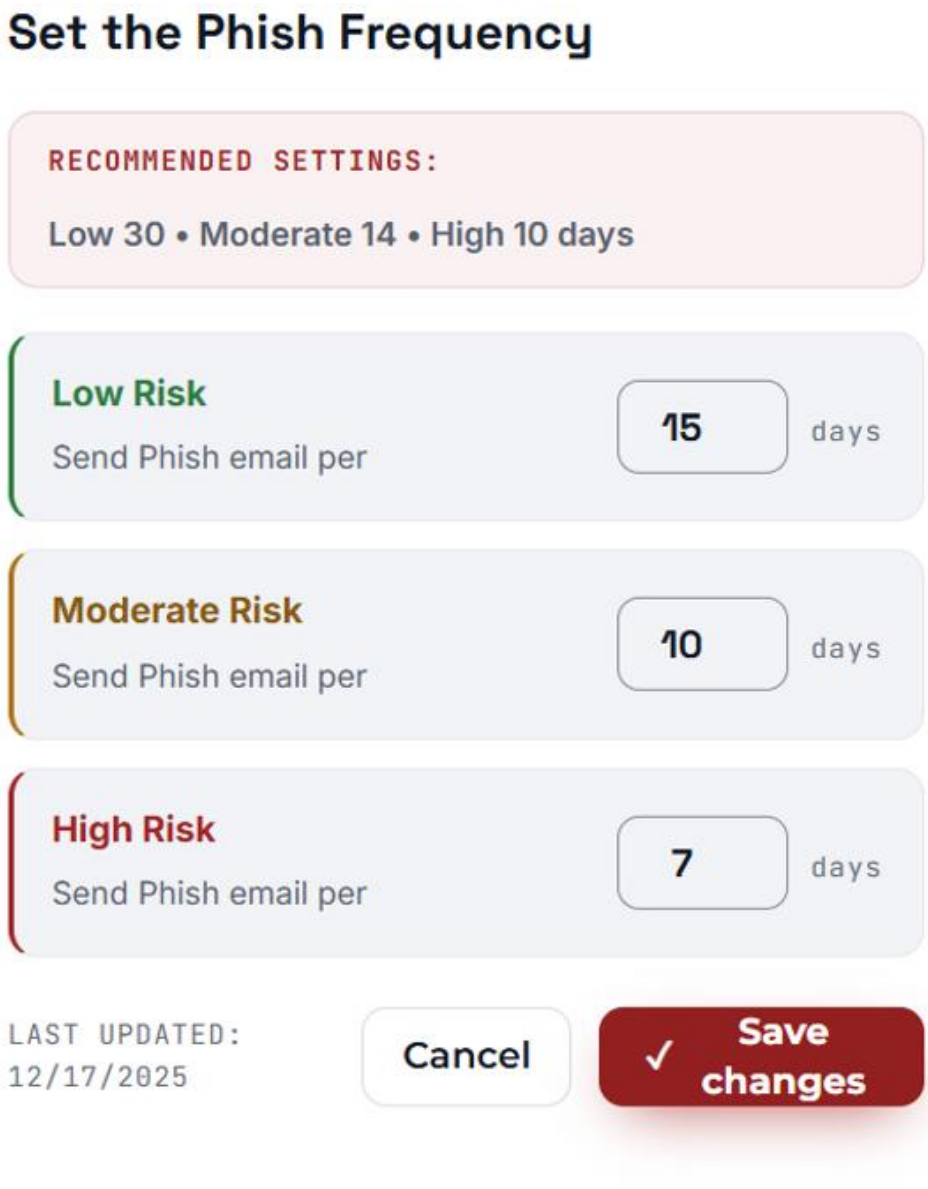


PhishFirewall training-email configuration.

Figure A.24 | Risk-based phishing frequency

The frequency settings show separate schedules for low-, moderate-, and high-risk users. The platform can increase reinforcement for users who need additional help and reduce unnecessary training for users who consistently demonstrate secure behavior.

WVOT relevance: This creates a scalable operating model that focuses State resources where behavior indicates the greatest need.

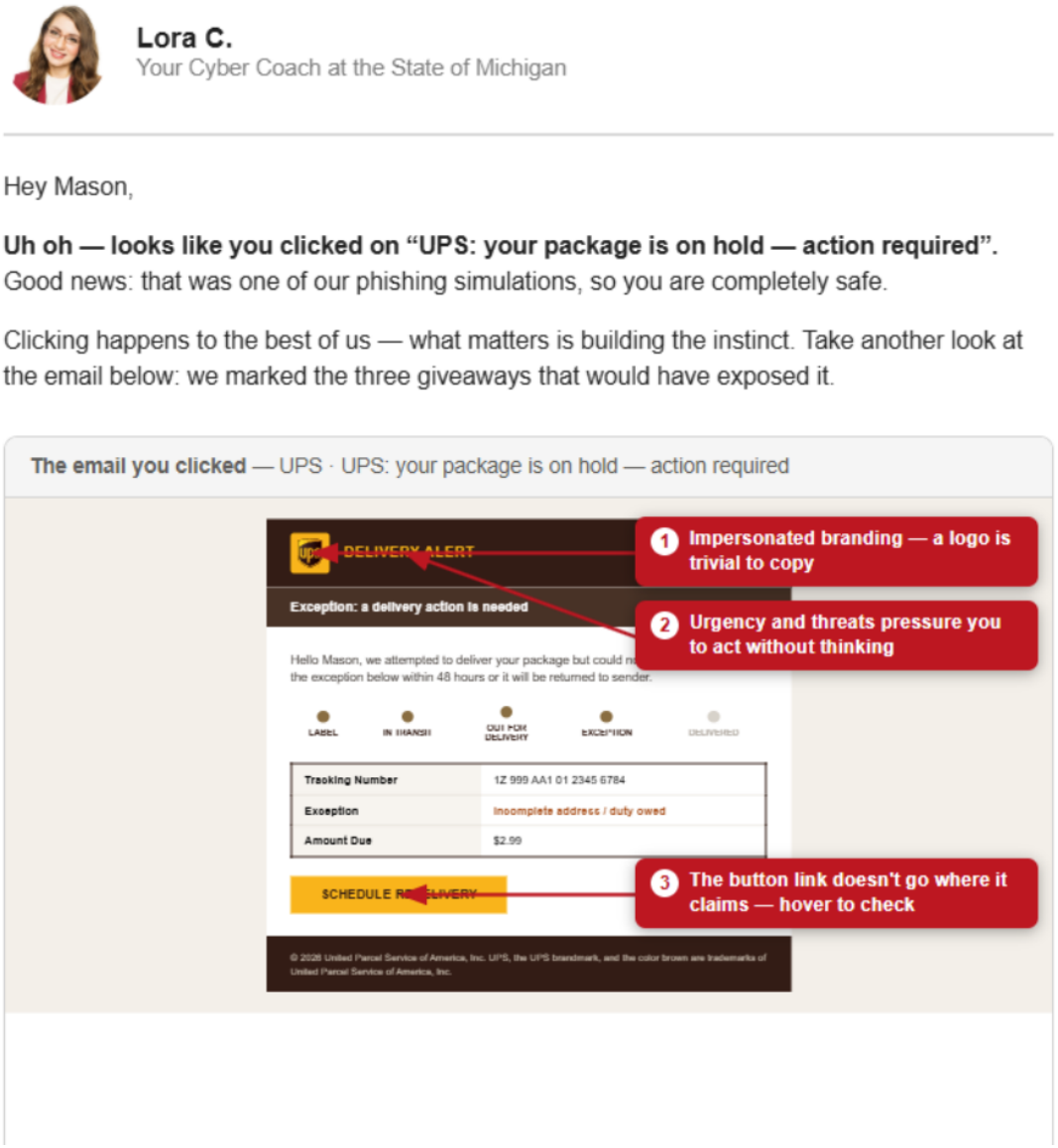


PhishFirewall risk-based phishing-frequency settings.

Figure A.25 | Personalized behavioral coaching

The coaching workflow uses a user's behavior and the specific exercise or message involved to deliver a contextual learning moment. It reinforces the desired behavior near the time the risky action is identified.

WVOT relevance: WVOT can turn a simulated interaction into immediate, relevant remediation and then measure whether behavior improves.

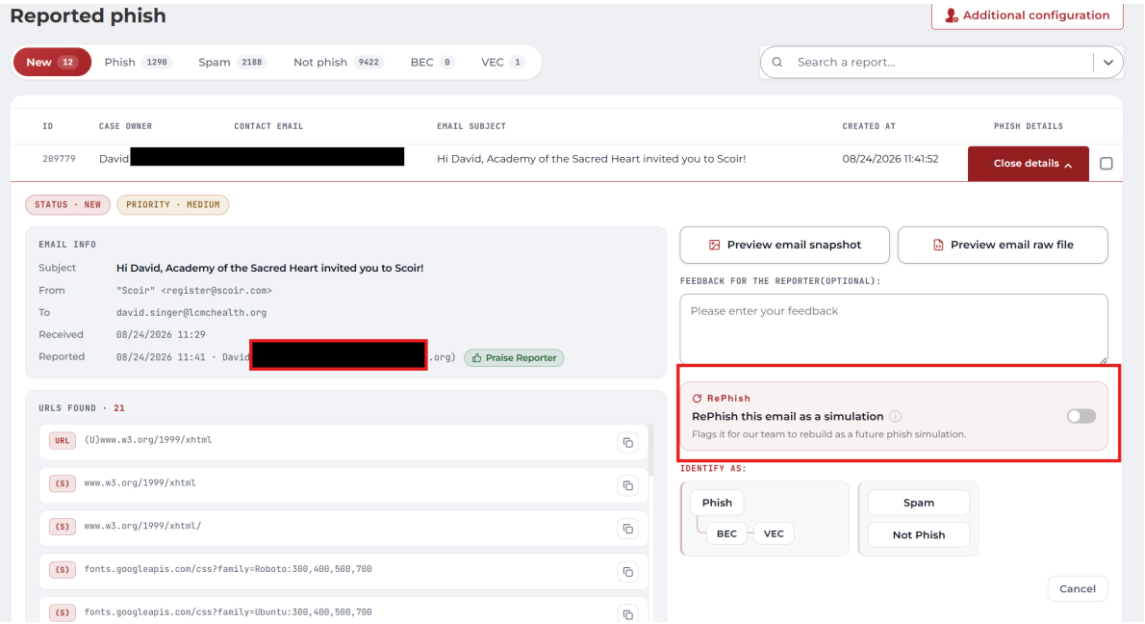


PhishFirewall personalized behavioral-coaching workflow.

Figure A.26 | Reported-phish workflow

The reported-phish view shows how a user-reported message can be reviewed, classified, and routed through analyst action. It connects user reporting with evidence review and administrative follow-up.

WVOT relevance: This supports a repeatable reporting path for WVOT employees and helps security personnel turn reports into both response actions and future awareness content.

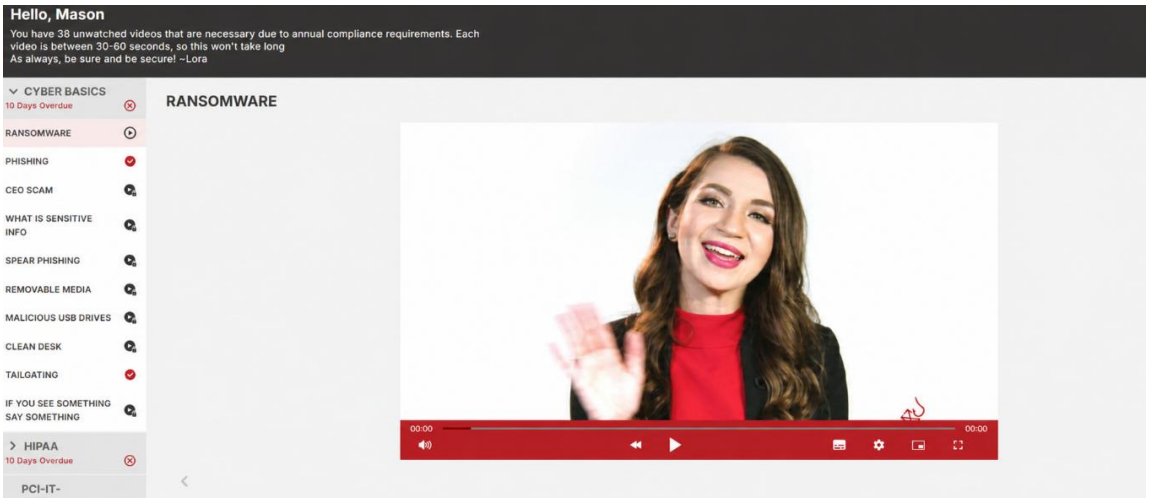


PhishFirewall reported-phish review and triage workflow.

Figure A.27 | Training content and learner experience

The training view presents the learning content delivered to users and the associated progress or completion experience. It supports focused education that can be assigned, measured, and reinforced over time.

WVOT relevance: WVOT can provide consistent awareness education while retaining visibility into participation and learning progress.

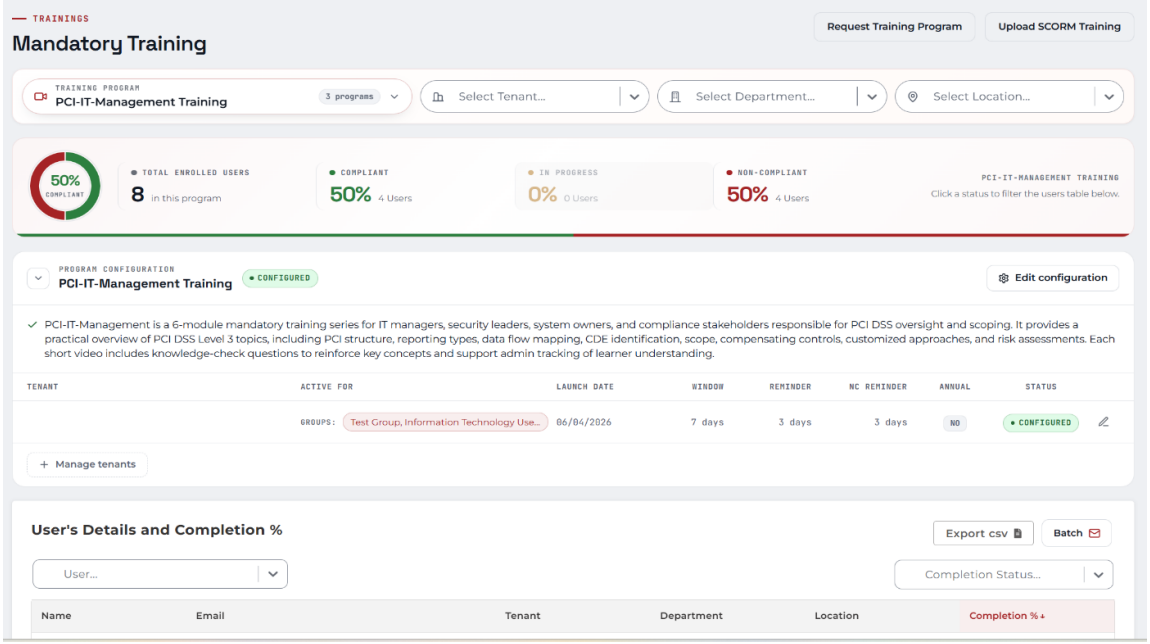


PhishFirewall training-content and learner experience.

Figure A.28 | Mandatory-training reporting

The reporting dashboard presents completion, compliance, and program-status information for administrators, including reporting by agency or department, individual transcripts, past-due and exception reporting, supervisory summaries, and executive reporting.

WVOT relevance: This provides WVOT with evidence of participation and compliance without requiring the security team to compile those measures manually.

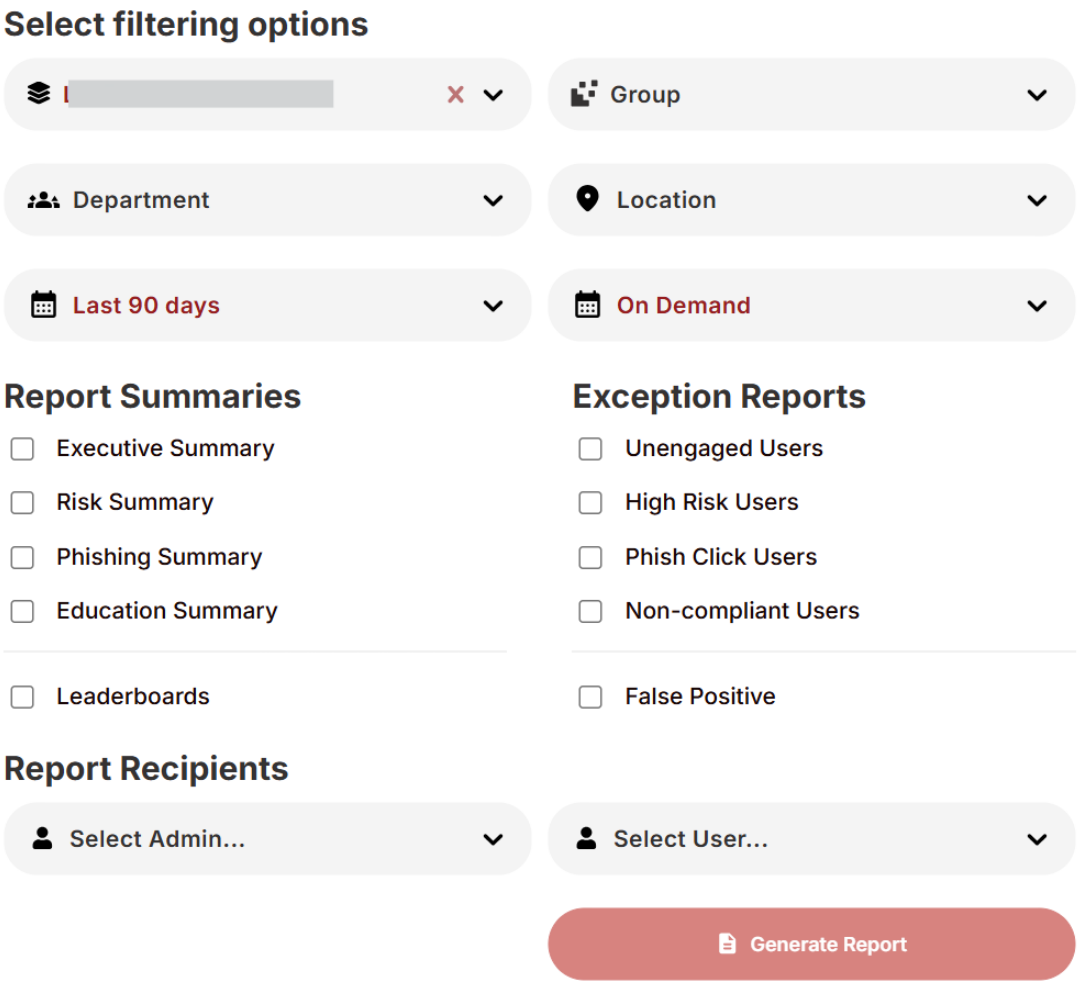


PhishFirewall mandatory-training and compliance reporting.

Figure A.29 | Organizational report filters

The report-filter interface allows administrators to select organizational and reporting dimensions before generating summaries. Reports can be tailored for operational, supervisory, exception, and executive use and aligned to the State's organizational structure.

WVOT relevance: This supports agency-level oversight and targeted reporting while allowing leadership to view program performance at the appropriate level of detail.

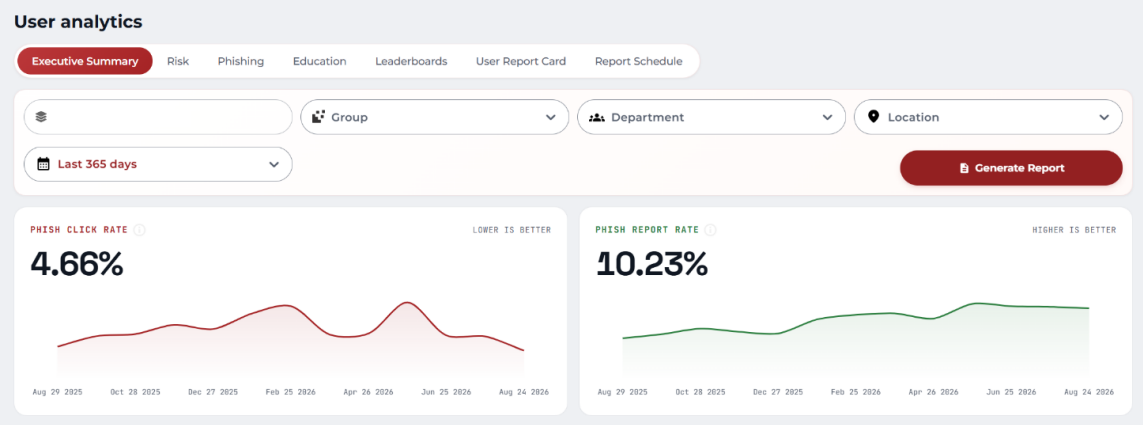


PhishFirewall report filters and organizational reporting controls.

Figure A.30 | User-level behavior analytics

The user analytics view presents trend information for individual or filtered populations, including interaction rates, reporting behavior, repeat interactions, time-to-report, risk scores, and improvement against established baselines.

WVOT relevance: WVOT can use these measures to demonstrate whether awareness activity is reducing risky behavior and improving organizational resilience over time.



PhishFirewall user-level behavior analytics and trend reporting.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Mark Hale

(Address) 100 S. Ashley Rd, Tampa, FL 33602

(Phone Number) / (Fax Number) 9376203378

(email address) mhale@cyberdefenseadvisors.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

CDA, LLC
(Company)

(Signature of Authorized Representative)

Mark Hale - VP of Partnershps and Business Development 8/24/2026
(Printed Name and Title of Authorized Representative) (Date)

9376203378
(Phone Number) (Fax Number)

mhale@cyberdefenseadvisors.com
(Email Address)

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 RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:

Vendor Name : Cyber Defense Advisors (CDA, LLC)

Address :

Street : 100 S. Ashley Rd

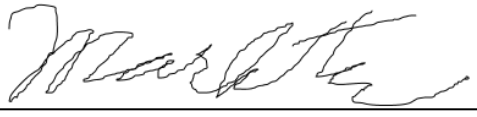
City : Tampa

State : Florida **Country :** USA **Zip :** 33602

Principal Contact : Mark Hale

Vendor Contact Phone: 937-620-3378 **Extension:**

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

Vendor Signature X  **FEIN#** 87-4233337 **DATE** 8/24/2026

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

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		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Core Detection	22000.00000	EA	$18	$396,000

Comm Code	Manufacturer	Specification	Model #
43230000	PhishFirewall	PhishEQ	

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		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Core Detection - Year 2 (Optional Renewal)	22000.00000	EA	$18	$396,000

Comm Code	Manufacturer	Specification	Model #
43230000	PhishFirewall	PhishEQ	

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	WV OFFICE OF TECHNOLOGY
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Core Detection - Year 3 (Optional Renewal)	22000.00000	EA	$18.50	$407,000

Comm Code	Manufacturer	Specification	Model #
43230000	PhishFirewall	PhishEQ	

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	WV OFFICE OF TECHNOLOGY
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Core Detection - Year 4 (Optional Renewal)	22000.00000	EA	$18.50	$407,000

Comm Code	Manufacturer	Specification	Model #
43230000	PhishFirewall	PhishEQ	

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