Apptega

GUIDE

NIST SP 800-171 Rev. 3

Compliance Guide

For nonfederal organizations that process, store, or transmit Controlled Unclassified Information (CUI) under federal contracts or agreements

Current as of August 19, 2025

Apptega

Apptega

1. Introduction

This practical guide helps nonfederal organizations become compliant with NIST SP 800-171 Rev. 3 by aligning people, processes, technology, and third parties to the 14 control families. It provides owners, parameters, measurable acceptance criteria, evidence locations, and direct references to the §3.x family numbering used in Rev. 3. It also explains when to create and update the System Security Plan (SSP) and Plans of Action & Milestones (POA&Ms) required by the framework.

1A. Beginner Quick-Start (First 30—90 Days)

Days 1—15: Stand-up

- Appoint: Information System Owner, ISSM/ISO, IT/Cloud Owner, IAM Owner, Incident Response Lead, Records/CUI Custodian, TPRM Lead.
- Define CUI authorization boundary and draft CUI data-flows (ingress, storage, transmission, egress, archival, disposal).
- Inventory External Service Providers (ESPs) and contracts affecting CUI; note inherited vs. shared controls.
- Establish an SSP skeleton immediately (family sections, boundary narrative, roles, inherited controls). *Create SSP draft by Day 15.*

Days 16—45: Implement & tailor

- Confirm categorization of CUI and scoping; set organization-defined parameters (ODPs) for controls (timeouts, MFA scope, cipher suites, log retention).
- Stand up baselines: MFA, logging/SIEM, EDR/anti-malware, patching, backup/restore, secure configurations, change control.
- Draft family narratives (§3.1–§3.14) and update SSP accordingly. *SSP v1 complete by Day 30; POA&M opened for gaps.*

Days 46—90: Validate & evidence

- Populate the Evidence Register; conduct tabletops (credential theft, ransomware, lost device); perform internal self-assessment against §3.x objectives.
- Record gaps with owners/due dates in POA&M; update SSP v2 reflecting final scoping and inherited controls before any external assertion.

2. Scope & Alignment

Scope. All people, processes, systems, networks, mobile devices, cloud services, and third parties that create, receive, maintain, transmit, or can impact CUI. Include management systems (identity, logging, backup, orchestration) that can influence CUI confidentiality.

Key definitions

- **CUI:** Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, requiring safeguarding.
- **CUI Authorization Boundary:** The set of components and trust zones that process, store, transmit, or can materially impact CUI.
- **Organization-Defined Parameters (ODPs):** Tailorable values required by some controls; set them deliberately and record in the SSP.

Governance & roles

- Authorizing Official / Executive Sponsor (risk acceptance), Information System Owner, ISSM/ISO, CUI Custodian, TPRM Lead, Cloud/Network Owner, IR Lead, IAM Owner, Records/Legal Counsel.

3. Standards & Practices (Mapped to NIST SP 800-171 Rev. 3 Families)

For each family: Intent • Minimums • Implement (Procedural/Technical/Contractual) • Evidence • Acceptance Criteria • Common Failures • Internal QA Plan • Documentation tie-in.

3.1 Access Control (AC) — §3.1.x

Intent: Ensure only authorized users, processes, and devices access CUI based on least privilege and separation of duties.

Minimums: Role-based access; centralized IAM; enforce MFA where required; session controls; restrict remote/admin access.

Implement — Procedural: Access request/approval; JML (joiner/mover/leaver ≤24h); quarterly recertifications for privileged roles; break-glass governance.

Implement — Technical: SSO/IdP; group-based roles; PAM for admin; network segmentation; masking of CUI where feasible; session timeouts.

Implement — Contractual: ESP responsibility matrices covering IAM boundaries.

- **Evidence:** Access requests; role matrices; recert results; PAM/MFA coverage.
- **Acceptance Criteria:** 100% users mapped to roles; MFA enforced for remote/admin; quarterly recerts ≥95% on time; no orphaned accounts.
- **Common Failures:** Shared admin accounts; excessive group inheritance; stale access after transfers.
- **Internal QA Plan:** Sample 25 users & 10 admins quarterly.
- **Documentation tie-in:** Access Control Policy; JML SOP; IAM Standard.

3.2 Awareness & Training (AT) — §3.2.x

Intent: Ensure users understand security risks and their responsibilities for CUI.

Minimums: Training before access and at least annually; role-based modules for admins, developers, IR team.

Implement: LMS with baseline + phishing/secure coding; targeted refreshers after incidents; track completion and outcomes.

- **Evidence:** Rosters; training content; completion dashboards.
- **Acceptance Criteria:** 100% in-scope personnel trained before access; annual refresher on schedule.
- **Common Failures:** Contractors not enrolled; decentralized rosters.
- **Internal QA Plan:** Monthly reconciliation of HR vs. IAM vs. LMS.
- **Documentation tie-in:** Training Plan; Role Matrix.

3.3 Audit & Accountability (AU) — §3.3.x

Intent: Generate, protect, retain, and review audit events related to CUI systems.

Minimums: Time-sync; log security-relevant events (auth, admin, access, config, data actions); protect and retain logs.

Implement: Central SIEM; alerting use-cases; log integrity; restricted admin access to logs; review cadence.

- **Evidence:** SIEM configs; sample events; retention settings; review minutes/tickets.
- **Acceptance Criteria:** Required events from 100% in-scope systems; alerts triaged within SLA; retention per parameter.
- **Common Failures:** Logging enabled but unreviewed; missing admin events.
- **Internal QA Plan:** Validate 5 representative systems end-to-end.
- **Documentation tie-in:** Logging & Monitoring Standard; Review SOP.

3.4 Configuration Management (CM) — §3.4.x

Intent: Maintain secure baselines; control changes; detect unauthorized changes.

Minimums: Platform-specific baselines; image management; change approvals; FIM/drift detection.

Implement: CIS-aligned baselines; IaC with code reviews; emergency change process; exception handling with expiry and compensating controls.

- **Evidence:** Baselines; change tickets; drift/FIM reports.
- **Acceptance Criteria:** 100% systems on baseline; drift remediated or time-bound exceptions; changes approved/tested.
- **Common Failures:** "Gold image" not maintained; default services left enabled.
- **Internal QA Plan:** Monthly drift sample of 20 endpoints/servers.
- **Documentation tie-in:** Hardening Standards; Change Control SOP.

3.5 Identification & Authentication (IA) — §3.5.x

Intent: Uniquely identify and authenticate users/devices/processes.

Minimums: Unique IDs; password/lockout parameters; MFA for remote and admin access to CUI systems; service account governance.

Implement: Password vaulting; PAM; device certificates; disable shared/anonymous accounts; strong auth for APIs.

- **Evidence:** MFA coverage; PAM logs; policy configs; device cert inventory.
- **Acceptance Criteria:** 100% MFA for remote/admin; unique IDs everywhere; service accounts documented and rotated.
- **Common Failures:** Legacy VPN without MFA; shared IDs in scripts.
- **Internal QA Plan:** Audit 10 services and 3 API integrations.
- **Documentation tie-in:** Authentication Standard; PAM Procedure.

3.6 Incident Response (IR) — §3.6.x

Intent: Prepare, detect, analyze, contain, eradicate, and recover from incidents affecting CUI.

Minimums: IR plan; roles; reporting timelines; evidence handling; lessons learned.

Implement: Tabletop scenarios (phishing→CUI exfiltration, lost laptop, supply-chain compromise); forensics partners; preservation procedures.

- **Evidence:** IR plan/runbooks; tabletop reports; tickets; lessons learned.
- **Acceptance Criteria:** Escalations within SLA; corrective actions tracked; comms matrix tested.
- **Common Failures:** No call tree; late containment; weak evidence handling.
- **Internal QA Plan:** Semiannual tabletop and after-action review.
- **Documentation tie-in:** Incident Response Plan; Contact Roster.

3.7 Maintenance (MA) — §3.7.x

Intent: Perform and control system maintenance securely.

Minimums: Authorized personnel; documented approvals; remote maintenance protections; media sanitization post-maintenance.

Implement: Maintenance windows; jump hosts; monitoring of remote sessions; device return checks.

- **Evidence:** Maintenance logs; approvals; session records.
- **Acceptance Criteria:** 100% maintenance pre-approved; remote sessions encrypted/monitored; artifacts sanitized.
- **Common Failures:** Vendor remote access without control; missing logs.
- **Internal QA Plan:** Sample 10 maintenance events quarterly.
- **Documentation tie-in:** Maintenance SOP; Remote Access Standard.

3.8 Media Protection (MP) — §3.8.x

Intent: Protect CUI on physical and digital media.

Minimums: Labeling; encryption for portable media; controlled transport; secure destruction.

Implement: Chain-of-custody; approved encryption; shredding/wiping; shipping procedures.

- **Evidence:** Media inventories; transport logs; destruction certificates.
- **Acceptance Criteria:** 100% portable media encrypted; destruction certified.
- **Common Failures:** Unlogged transfers; unencrypted USBs.
- **Internal QA Plan:** Quarterly inventory and at least two destruction events audit.
- **Documentation tie-in:** Media Handling SOP.

3.9 Personnel Security (PS) — §3.9.x

Intent: Ensure individuals are screened and managed appropriately.

Minimums: Background checks; nondisclosure agreements where applicable; timely termination/offboarding; badge/credential recovery.

Implement: HR-IAM synchronization; clearances where required by contract; least privilege at onboarding.

- **Evidence:** Screening records; access change tickets; offboarding logs.
- **Acceptance Criteria:** Screening complete before access; deprovisioning ≤24h after separation.
- **Common Failures:** Contractor onboarding without screening; delays in disabling accounts.
- **Internal QA Plan:** Monthly HR vs IAM reconciliation.
- **Documentation tie-in:** Personnel Security SOP.

3.10 Physical Protection (PE) — §3.10.x

Intent: Limit physical access to CUI systems/facilities.

Minimums: Badging; visitor management; video/door logs; asset tracking.

Implement: Locked racks; escort policy; secure storage for portable devices; environmental controls.

- **Evidence:** Access lists; visitor logs; camera retention policy.
- **Acceptance Criteria:** Authorized-only access; logs retained and reviewed.
- **Common Failures:** Shared badges; missing visitor records.
- **Internal QA Plan:** Quarterly sample of access/visitor logs.
- **Documentation tie-in:** Physical Security Plan.

3.11 Risk Assessment (RA) — §3.11.x

Intent: Assess risk to operations, assets, and individuals from the operation and use of systems that process CUI.

Minimums: Risk methodology; register; periodic reviews; time-bound mitigations.

Implement: Likelihood/impact model; exception handling with expiry; treat high risks first.

- **Evidence:** Risk register; approvals; review minutes.
- **Acceptance Criteria:** High risks owned with due dates; expiries tracked.
- **Common Failures:** Permanent exceptions; stale risks.
- **Internal QA Plan:** Quarterly risk review board.
- **Documentation tie-in:** Risk Management Plan.

3.12 Security Assessment (CA) — §3.12.x

Intent: Assess and monitor controls; manage SSP and POA&M.

Minimums: System Security Plan (SSP) describing boundary, environments, roles, control implementation, and ODP values; POA&M for deficiencies; periodic assessments.

Implement:

- **SSP timing:** Draft by Day 15, v1 by Day 30, v2 by Day 60–90 after initial remediation and evidence collection; update on material change and at least annually.
- **Assessments:** Map to §3.x objectives; track findings into POA&M with owners/dates.
- **Evidence:** SSP (current + prior versions); POA&M; assessment results.
- **Acceptance Criteria:** SSP complete and current; all gaps reflected in POA&M with closure dates; reassess after significant changes.
- **Common Failures:** Outdated SSP; untracked findings.
- **Internal QA Plan:** Quarterly SSP/POA&M quality check.
- **Documentation tie-in:** SSP; POA&M; Assessment Procedure.

3.13 System & Communications Protection (SC) — §3.13.x

Intent: Protect CUI during transmission; separate duties; defend at boundaries.

Minimums: Strong cryptography; boundary protections; protocol governance; egress control.

Implement: TLS 1.2+; VPN/private links; WAF for public apps; DNS/HTTP egress allow-listing; email/file-transfer security.

- **Evidence:** Cipher scans; configs; WAF policies; egress rulesets.
- **Acceptance Criteria:** No plaintext CUI over public networks; boundary defenses active; egress restricted.
- **Common Failures:** Legacy protocols; uncontrolled outbound.
- **Internal QA Plan:** Monthly external scans; review 5 interfaces.
- **Documentation tie-in:** Transmission Security; Network Boundary Standard.

3.14 System & Information Integrity (SI) — §3.14.x

Intent: Identify, report, and correct system flaws; protect from malicious code; monitor for events.

Minimums: Vulnerability remediation; anti-malware/EDR; alerting; integrity checks.

Implement: Patch SLAs; authenticated scanning; EDR with real-time protection; integrity verification for critical files and images.

- **Evidence:** Patch dashboards; EDR coverage; vuln scans; alerts/tickets.
- **Acceptance Criteria:** Patching within SLA; 100% in-scope systems enrolled in EDR; alerts triaged.
- **Common Failures:** Exceptions without expiry; scanning gaps.
- **Internal QA Plan:** Monthly coverage audit and SLA exception review.
- **Documentation tie-in:** Vulnerability Mgmt SOP; Endpoint Protection Standard.

4. Authorization Boundary & CUI Data-Flow Mapping

Define components, interfaces, trust zones, and all CUI flows (collection, processing, storage, transmission, archival, disposal). Identify where CUI enters/exits, encryption zones, monitoring points, and dependencies/inherited controls. Keep diagrams current with change management.

5. Documentation Set — Canonical Narratives (Including SSP/POA&M)

Write cohesive narratives proving how the program satisfies §3.1–§3.14 for the defined boundary: overview & mission; boundary & inventory; CUI categories and lifecycle; roles & governance; ESPs and shared responsibility; control implementations; logging/monitoring; vulnerability/patch management; training; incident response; change management; assessment cadence; SSP and POA&M maintenance schedule.

6. Applicability & Acceptance Criteria Mapping (to NIST SP 800-171 Rev. 3)

Maintain a definitive record that, for each of the 110 requirements, states applicability, implementation summary, parameter values, measurable acceptance criteria, 171A objectives, inheritance type, and a pointer to evidence.

Excerpt:

Ref	Title	Applicable	Implementation Summary	ODPs	Acceptance Criteria	Inheritance	Evidence
§3.1.1	Limit system access to authorized users	Y	SSO/IdP; role groups; PAM for admin	Session idle 15m	All users mapped; MFA remote/admin	None	IAM/Access/
§3.12.x	SSP & POA&M	Y	SSP v2 current; POA&M tracked	Review 90d	All gaps recorded with dates	Some ESP	GRC/SSP/

7. Program Parameters (Organization-Specific Settings)

- **Authentication:** MFA for remote network access and all administrative access; password min length 12; lockout 10 attempts/30 min; session idle 15 min.
- **Cryptography:** TLS 1.2+; approved cipher suites; cert rotation ≤13 months; FIPS-validated modules where required by contract.
- **Logging:** Events (auth, admin, access to CUI, config change); retention ≥12 months; time sync drift ≤5 minutes; alert SLA defined.
- **Patching:** Critical ≤15 business days; High ≤30; Medium ≤60; Low ≤90; exceptions time-bound with compensating controls.
- **Backups:** 3-2-1 model; quarterly restore tests; encryption at rest & in transit.
- **Segmentation:** Deny-by-default; CUI network zones; controlled admin paths; egress allow-listing.
- **Data Handling:** Approved export channels; data minimization; cryptographic erasure or secure destruction at end of life.
- **Third Parties:** Responsibility matrices; incident notice ≤72h; right-to-audit for material services.

Apptega

8. Evidence Register

Artifact	Families	Location/Path	Owner	Format	Retention
Boundary Diagram & CUI Data-Flows	All	171/Boundary/	System Owner	PDF/PNG	Current + 1 yr
Access Requests & Recerts	AC/IA	IAM/Access/	IAM Lead	CSV/PDF	1–2 yrs
MFA/PAM Coverage	AC/IA	IAM/MFA/	IAM Lead	CSV/PNG	1–2 yrs
Baselines, Change Tickets, FIM	CM	Build/	Platform	PDF/CSV	1–2 yrs
SIEM Configs, Alerts, Reviews	AU/SI	SecOps/SIEM/	SecOps	JSON/PDF	1–2 yrs
Patch Dashboards & Exceptions	SI	VM/Patch/	SecOps	CSV/PDF	1–2 yrs
EDR Coverage & Alerts	SI	SecOps/EDR/	SecOps	CSV/PNG	1–2 yrs
Backup/Restore Evidence	CP/SI	Ops/Backup/	Ops Lead	PDF/CSV	1–2 yrs
IR Plan & Tabletop Reports	IR	IR/	IR Lead	PDF	3 yrs
Media Inventory & Destruction Certs	MP	Facilities/Media/	Facilities	PDF	3 yrs
Physical Access & Visitor Logs	PE	Facilities/Access/	Facilities	CSV/PDF	1 yr
Screening & Offboarding Records	PS	HR/Security/	HR	PDF	Per policy
Risk Register & Reviews	RA	GRC/Risk/	ISO	CSV/PDF	3 yrs
SSP (current + prior)	CA	GRC/SSP/	ISO	DOC/PDF	Current + 1 yr
POA&M Register	CA	GRC/POAM/	ISO	XLSX	Life of item + 1 yr
ESP Responsibility Matrices	All	TPRM/171/	TPRM	PDF/XLSX	Active + 1 yr

9. Continuous Monitoring

- **Daily:** SIEM ingestion health; high/critical alerts triage; EDR/MFA coverage gaps; failed backups.
- **Weekly:** Vulnerability scan review; IAM anomalies; certificate expiry <30 days; egress rule changes.
- **Monthly:** Access recert roll-up; baseline drift review; patch SLA dashboard; ESP incident notifications.
- **Quarterly:** Ruleset review; recovery test; management KPI review; reassess ODPs as needed.
- **Automation:** Open tickets for ingestion failures, MFA/PAM gaps, crypto drift, expired exceptions, failed restores, or unreviewed alerts.

10. Remediation & Risk Acceptance Workflow

- Identify → Log (severity, owner, due date, milestones) → Treat (process, tech, training, vendor) → Verify with evidence → Report to governance.
- Risk acceptance only by designated officials, with explicit expiry and compensating controls. All gaps reflected in the POA&M until closed.

11. External Service Providers & Flow-Down

Inventory all ESPs (cloud, MSP, SaaS, identity, logging, backup). For each: define shared responsibilities, confirm control inheritance, obtain attestations, and ensure incident-notice timelines. Ensure CUI handling, encryption, logging, retention, and subcontractor flow-down are specified. Update SSP with inherited controls and evidence locations.

12. Training & Awareness (Role-Based)

Tracks for workforce, helpdesk, admins, developers, SOC/IR, leadership, and vendors with access to CUI. Onboarding before access; annual refresher; targeted refreshers after incidents. Metrics: completion ≥98% and declining repeat findings.

13. Change Management for Security Impact

Assess NIST 800-171 impact for product/process/network changes, new providers, cloud moves, or mobile rollouts. Update boundary diagrams, role matrices, logging scope, MFA coverage, and SSP/POA&M.

14. Evidence Sampling Plans (Internal QA)

- **Access (AC/IA):** Sample 25 users and 10 admins; verify least privilege, MFA, timely deprovisioning.
- **Logging (AU/SI):** Sample 5 systems; verify required events, retention, and alert handling.
- **Config/Patching (CM/SI):** Sample 10 changes and 20 hosts; confirm approvals, baseline compliance, and patch SLAs.
- **Crypto/Boundary (SC):** Validate 3 TLS endpoints and boundary rules; check egress allow-lists.
- **IR (IR):** Review last tabletop; verify action items closed.
- **Physical/Media (PE/MP):** Review one month of visitor logs and two destruction events

15. Common Pitfalls

- Treating cloud provider attestations as full inheritance; missing shared-responsibility details in SSP.
- MFA gaps for remote/admin access; shared administrator accounts.
- Logging turned on but not reviewed or missing admin/config/data-access events.
- Outdated SSP; POA&M not tracking all gaps with owners/dates.
- Uncontrolled egress allowing exfiltration; legacy protocols carrying CUI.
- Contractors without onboarding training or screening where required.

16. Quick Reference Summary

Area	Core Artifacts	Examples
AC/IA	Role matrix; MFA/PAM logs	JML ≤24h; JIT elevation
AU	SIEM configs; alerts; reviews	Admin/auth/data events; NTP
CM	Baselines; FIM/drift; change tickets	CIS alignment; emergency change controls
IR	IR plan; tabletop AARs	Call trees; evidence handling
SC	TLS configs; egress allow-lists	WAF; VPN/private connectivity
SI	Patch dashboards; EDR coverage	Auth scans; SLA exceptions
CA	SSP & POA&M	Assessment cadence; gap closures
TPRM	Responsibility matrices	Provider attestations; incident notice

17. Self-Assessment & Leadership Attestation

Use status: **Compliant (C) / Partially Compliant (PC) / Not Compliant (NC) / Not Applicable (N/A).**

Tracker (illustrative):

Requirement (Rev. 3)	Status	Rationale (for N/A or gaps)	Evidence Link	Owner	Notes/POA&M ID
§3.1.x – Access Control	PC	Excessive group membership in legacy OU	IAM/Recerts_Q3.csv	IAM Lead	ACT-2025-017
§3.12.x – SSP & POA&M	C	SSP v2 published; gaps tracked	GRC/SSP/	ISO	—
§3.13.x – Transmission Security	C	TLS scans clean	Net/TLS/Scan_2025Q3.pdf	NetSec	—

Leadership attests that scope is complete, evidence exists for each "C," and PC/NC items have owners and due dates in the POA&M.

18. SPRS Scoring

When you must post: If DFARS 252.204-7019/7020 apply, you must have a current NIST SP 800-171 DoD Assessment summary score posted in SPRS to be eligible for award (not older than 3 years unless the solicitation specifies a shorter interval).

Prerequisites (before entering SPRS)

- Complete your NIST SP 800-171 assessment, determine your score, and complete your SSP. SPRS stores the results; the Basic Assessment itself is performed offline.

Scoring model (current DoD baseline)

- Use the **DoD NIST SP 800-171 Assessment Methodology, v1.2.1 (June 24, 2020).**
- **Score range: –203 to +110**, with **110** as the maximum (no deductions).
- **Assessment levels recorded in SPRS: Basic** (contractor self-assessment), **Medium** (DoD review), **High** (DoD on-site/virtual).

Rev. 3 vs. scoring baseline

- The official DoD scoring methodology remains anchored to the 110 requirements in Rev. 2. If you implement Rev. 3, maintain a clear crosswalk in your SSP from Rev. 3 requirements to the Rev. 2 scoring elements used to compute the SPRS score, until DoD updates the methodology.

What to record in SPRS

- Summary score, assessment level (Basic/Medium/High), assessment date, CAGE code, and relevant system identifier(s). Update upon material changes or per contractual cadence to keep the score current.

Key cautions

- Do **not** submit a score without an SSP that justifies each requirement's implementation and any POA&M items.
- For Medium/High assessments, DoD may validate and post the summary score (with rebuttal opportunities) under 7020.

19. References & Resources

NIST SP 800-171 Rev. 3 (Protecting CUI in Nonfederal Systems and Organizations)
https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/final

NIST SP 800-171A Rev. 3 (Assessment Procedures)
https://csrc.nist.gov/publications/detail/sp/800-171a/rev-3/final

NIST CUI Program (General)
https://www.archives.gov/cui

DoD NIST SP 800-171 Assessment Methodology & SPRS
https://www.acq.osd.mil/cmmc/

Self-check: This guide is written to be implementable for organizations aiming to become compliant with NIST SP 800-171 Rev. 3, using your approved structure with clear narratives, timing for the SSP, measurable acceptance criteria, and evidence mapping.

Apptega

Apptega Product Features

16+ Security Frameworks

One-Click Reporting

Automated Alerts & Notifications

API & Application Connectors

Automated Framework Crosswalking

Real-Time Compliance Scoring

Restricted Auditor View

Single Sign-On Connectivity

Policy & Plan Templates

Automated Risk Assessments

Document Repository for Artifacts

Multi-Tenant Environment

Apptega

About Apptega

A perennial G2 leader across various cybersecurity categories, Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.
2. Build and manage world-class cybersecurity and compliance programs for their clients.
3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.
4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit apptega.com

Visit apptega.com