Guardian Compliance for CMMC and NIST 800-171

How PTS Guardian tiers cover CMMC Level 2 and NIST SP 800-171 for manufacturers, DoD suppliers, and industrial SMBs.

The business problem: CMMC Level 2 became enforceable in DoD contracts in 2025, with full phase-in through November 2028. Every supplier handling Controlled Unclassified Information (CUI) must implement and prove the 110 NIST SP 800-171 controls. Beyond defense, manufacturers face cyber insurance underwriters, OEM customer questionnaires, and ransomware operators who specifically target production environments because downtime forces payment.

The PTS answer: Guardian Compliance is our tier purpose-built for manufacturers and DoD suppliers. It combines our managed help desk, cybersecurity, backup, M365 E5 cloud, and vCIO management with the documented controls, audit-ready evidence, and air-gapped recovery that CMMC assessors, cyber insurance carriers, and OEM customers expect. **Compliance is the tier built to satisfy CMMC L2 and NIST 800-171 end-to-end.**

THE SOLUTION

Why the Compliance tier

Compliance is the Guardian tier built end-to-end for CMMC L2 and NIST 800-171. Six capabilities make the difference between intent and assessor-defensible evidence:

- **M365 GCC High or commercial with Purview, DLP, and Message Encryption.** CUI data loss prevention, audit log retention, and encrypted external email. The same control set CMMC assessors and DoD program offices expect.
- **SIEM with integrated compliance logging and network monitoring.** Satisfies §3.3.1 Audit Logs, §3.3.2 User Accountability, and the §3.14.6 system monitoring requirements.
- **Air-gapped monthly server backups, performed and tested by PTS.** Demonstrable §3.8.9 information backup with documented restore testing. Ransomware-defensible and assessor-defensible.
- **Annual incident response planning and 5-year IT lifecycle plan.** Documented program under §3.6.1 and §3.6.2, not a one-time deliverable. Aligns with the System Security Plan (SSP) and Plan of Action and Milestones (POA&M) DoD expects.
- **CUI flow mapping and Business Associate / sub-processor inventory.** Annual data flow and asset inventory aligned with §3.4.1 and §3.12.4. Required for the SSP and re-required at every triennial assessment.
- **Identity hardening, MFA, and privileged-access controls.** Phishing-resistant MFA, conditional access, and least-privilege baselines under §3.5 Identification and Authentication. Closes the most-cited finding in DIBCAC assessments.

WHAT YOU GET

Inside the Compliance tier

A single managed-service bundle that delivers the help desk, security, backup, M365 E5 cloud, and vCIO management your CMMC and NIST 800-171 program depends on. Each layer is included in the monthly fee.

Service Layer	What you get
Help Desk	All remote, on-site, and emergency support within monthly limits. Acknowledge under 1 business hour, on-site under 8 business hours. 25% discount on after-hours emergency.
Cybersecurity	Advanced endpoint detection and response, 24/7 managed detection and response, phishing simulations and training, application allow-listing, DNS filtering, full-disk endpoint encryption, SIEM with compliance logging, network monitoring, OT/IT segmentation guidance.
Backup	Image-based cloud backup (workstations and servers), 3x 2TB external drives included, monthly air-gapped server backups performed by PTS, monthly restore testing.
Cloud (M365 E5)	M365 E5 licensing, Purview audit logs, DLP, Message Encryption, email and file backup, DDoS protection, DNS and domain management. GCC High available where required.
vCIO Management	Quarterly TBR, PTS firewall/network/wireless standards, vendor management, 100+ policy templates aligned to NIST 800-171, M365 hardening, white-glove MFA, annual incident response planning, 5-year IT and device lifecycle plan, annual reorientation and full documentation.

Why one bundle, not piecemeal tools

Most manufacturers run a patchwork: an MSP for the help desk, a separate backup vendor, an EDR the IT manager bought on a budget approval, and a policy template purchased from a consultant five years ago. Guardian Compliance replaces that stack with one accountable provider whose evidence binder maps directly to your CMMC SSP.

What it takes	Piecemeal	Phantom Bundle
Vendor count	6 to 10 separate contracts: MSP, SOC, EDR, backup, M365, training	One contract, one invoice, one accountable provider
Documentation	Customer assembles SSP and POA&M from each tool's documentation	PTS maintains policy library, SSP scaffold, and evidence binder
Restore testing	Backup vendor sells software; customer self-tests or skips entirely	Monthly air-gapped restore performed and logged by PTS
Assessor response	Production scrambles to collect logs and policies from each vendor	One call to PTS, evidence delivered from existing binder
Sub-processor accountability	Customer tracks every vendor's NIST 800-171 posture independently	PTS maintains the sub-processor inventory and risk assessments
Single point of escalation	Incident response routes through each vendor's separate support queue	P1-P4 escalation through one MSP, attorney-first protocol on day one

One contract. One SSP. One accountable provider. That is the difference between a tool stack and an assessor-ready program.

THE PROOF

The cost of getting it wrong

Manufacturing is the most-attacked industry for the fourth year running. Public-record cases show what one ransomware event costs a production environment. Small contract manufacturers are not exempt, they just do not appear in the headlines.

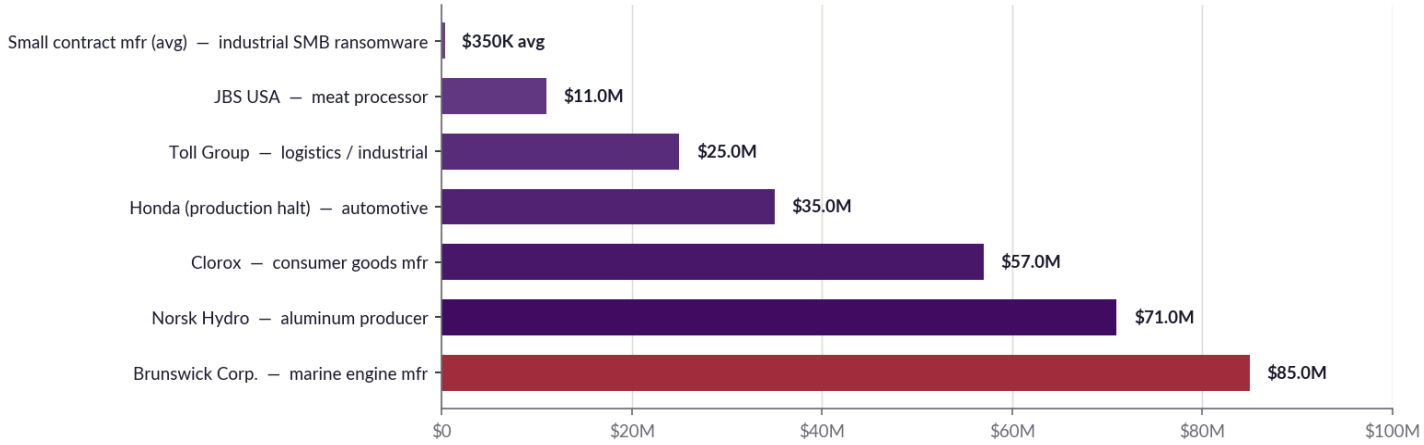
$1.9M
Average daily cost of ransomware downtime for manufacturers

11.6 days
Average production downtime per ransomware incident in 2024

199 days
Average time to identify a breach in industrial organizations

$5.6M
Average breach cost for industrial sector (IBM 2024)

Public-record manufacturer ransomware impact.



Disclosed cost figures from SEC filings, company statements, and industry press. The legal fees, lost-customer revenue, OEM qualification disruption, and reputational damage typically exceed the disclosed number. Small contract manufacturers rarely disclose, but Sophos and Comparitech data show average SMB ransomware events cost $350K and 11+ days of production.

Three patterns DIBCAC and insurers keep citing

PATTERN 01

No current System Security Plan

The most cited failure in DIBCAC assessments. §3.12.4 requires a documented, current SSP. Stale, generic, or templated-without-tailoring is the same finding.

PATTERN 02

Flat network with no OT segmentation

Engineering workstations, ERP, and shop-floor PLCs on the same VLAN. §3.13.1 boundary protection requires documented separation. Ransomware crosses flat networks in minutes.

PATTERN 03

MFA only on email, not on remote access

VPN, RDP, and admin consoles still password-only. §3.5.3 requires MFA for privileged and network access. Most-exploited gap in 2024 manufacturing ransomware cases.

THE DETAIL

Control-by-control mapping

Each row pairs a NIST SP 800-171 Rev 3 control family with the Guardian capability that satisfies it, and shows which tier delivers it. Skim the Compliance column, every YES is a CMMC L2 requirement covered out of the box.

ACCESS CONTROL 3.1

NIST §	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
§3.1.1-2	Limit access to authorized users; restrict to authorized transactions and functions.	Role-based access in M365 and Entra ID, application allow-listing, least-privilege baselines, quarterly access reviews.	NO	PART	YES
§3.1.5	Employ least privilege, including for specific security functions.	Privileged identity management, just-in-time admin access, separated admin accounts documented in SSP.	NO	PART	YES
§3.1.12	Monitor and control remote access sessions.	VPN/ZTNA with conditional access, MFA-enforced, session logging into SIEM.	NO	YES	YES
§3.1.20	Verify and control connections to and use of external systems.	Documented external system inventory, sub-processor BAAs, conditional access for unmanaged devices.	NO	PART	YES

AWARENESS AND TRAINING 3.2

§3.2.1-2	Security awareness training; insider-threat awareness.	Monthly phishing simulations, annual role-based training, documented completion records retained 6 years.	NO	YES	YES

AUDIT AND ACCOUNTABILITY 3.3

§3.3.1-2	Create and retain system audit logs; ensure individual user accountability.	SIEM with integrated compliance logging, Microsoft Purview audit log retention, identity-tied event correlation.	NO	NO	YES
§3.3.5	Correlate audit record review, analysis, and reporting.	Documented monthly log review by PTS, anomaly alerts to vCIO, quarterly TBR includes audit findings.	NO	NO	YES

CONFIGURATION MANAGEMENT 3.4

§3.4.1-2	Establish baseline configurations and inventories of organizational systems.	Documented hardening baselines via Intune/group policy, full asset inventory in a secure documentation portal, change-controlled.	NO	PART	YES
§3.4.6-7	Employ least functionality; restrict, disable, prevent the use of nonessential programs, ports, services.	Application allow-listing, port and service baselines, documented exceptions reviewed annually.	NO	PART	YES

IDENTIFICATION AND AUTHENTICATION 3.5

NIST §	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
§3.5.1-2	Identify and authenticate organizational users, processes, and devices.	M365 E5 identity, Entra ID conditional access, phishing-resistant MFA for all users, BitLocker endpoint encryption.	PART	YES	YES
§3.5.3	Use MFA for local and network access to privileged accounts; network access to non-privileged accounts.	MFA enforced for VPN, RDP, admin consoles, M365, and all SaaS via SSO. Documented exception process.	NO	YES	YES
§3.5.7-10	Password complexity, lockout, encrypted transmission and storage of passwords.	M365 password protection policy, enterprise password vault with rotation, no shared accounts.	NO	YES	YES

INCIDENT RESPONSE 3.6

§3.6.1-3	Establish IR capability; track, document, report incidents; test the IR plan.	Documented Incident Response Plan, P1-P4 playbooks, 24/7 managed detection and response, partner SOC threat response, annual tabletop exercise.	NO	PART	YES

MAINTENANCE AND MEDIA PROTECTION 3.7 / 3.8

§3.7.5	Require MFA to establish nonlocal maintenance sessions.	Vendor remote access through PTS-managed jump host with MFA and session recording.	NO	PART	YES
§3.8.3	Sanitize or destroy system media containing CUI before disposal or reuse.	Endpoint encryption, secure-wipe procedure for retired devices, documented media disposal log, encrypted external backup drives.	NO	PART	YES
§3.8.9	Protect the confidentiality of backup CUI.	Image-based encrypted cloud backup, monthly air-gapped server backups performed by PTS, monthly restore testing.	PART	PART	YES

SYSTEM AND COMMUNICATIONS PROTECTION 3.13

§3.13.1	Monitor, control, and protect communications at external boundaries and key internal boundaries.	PTS firewall standards, OT/IT segmentation guidance, DNS filtering, network monitoring (Compliance tier only).	NO	PART	YES
§3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI in transit.	TLS-enforced email, M365 Message Encryption, VPN/ZTNA where required, DNS web filtering.	NO	PART	YES
§3.13.11	Employ FIPS-validated cryptography when used to protect CUI.	FIPS-mode BitLocker and M365 cryptographic controls available in GCC High. Documented in SSP.	NO	NO	YES

SYSTEM AND INFORMATION INTEGRITY 3.14

§3.14.1-2	Identify, report, and correct system flaws; provide malicious-code protection.	Centrally managed endpoint policy with patch management, EDR, application allow-listing, vulnerability scanning.	PART	YES	YES
§3.14.6-7	Monitor systems for attacks and unauthorized use; identify unauthorized use.	SIEM with integrated compliance logging, 24/7 managed detection and response, documented monthly log review.	NO	PART	YES

THE PATH FORWARD

What working with PTS looks like

From first call to ongoing program: four clear stages, no surprises. Most manufacturers complete Discovery and Assessment within two weeks and reach a deployed Compliance posture in 60-120 days, depending on the existing environment and CUI scope.

1
Discovery
60-min CMMC and 800-171 Readiness Review. We map your current environment and CUI flow against this document's controls.

2
Assessment
CIS Controls + NIST 800-171 gap assessment. One-page snapshot, scored SSP draft, prioritized POA&M.

3
Implementation
Guardian Compliance tier deployed in 60-120 days. M365 E5, SIEM, OT/IT segmentation, air-gapped backups, policies, training.

4
Ongoing
Quarterly TBR, monthly air-gap testing, annual reorientation. Optional vCISO layer for DIBCAC assessment prep.

Add a vCISO for assessor depth

For manufacturers facing a triennial CMMC assessment, a DoD prime questionnaire, a cyber insurance renewal, or a multi-facility compliance program, a fractional **Phantom vCISO** engagement layers on SSP and POA&M ownership, board-level reporting, compliance roadmap, risk register ownership, and assessor liaison. Tiers: Foundation (quarterly), Operational (monthly), Strategic (monthly plus on-call).

Common gaps we find in manufacturers

- Flat network, no documented OT/IT segmentation
- MFA on email but not on VPN, RDP, or admin consoles
- Backups exist, but restore testing never performed
- Engineering workstations and ERP run as local admin
- Vendor remote access via persistent VPN, no jump host
- SSP missing, generic, or last updated by a former employee

Important. CMMC certification is granted by a C3PAO, not by PTS. NIST 800-171 compliance is achieved by the contractor, not by any single vendor. PTS provides the technology, documentation, and program rigor that demonstrably support your controls under NIST SP 800-171 Rev 3 and 32 CFR Part 170. Final policy adoption, CUI handling, and management attestation remain the responsibility of the contractor.

Next step: 30-minute CMMC Readiness Review

We walk your environment against this exact mapping and leave you with a one-page gap snapshot and SSP draft outline. No obligation.

Talk to PTS

hello@phantomts.com
phantomts.com/guardian

Why practices choose Phantom

Since 2010
OPERATING
Indiana-based MSP serving manufacturers, DoD suppliers, professional services, and SMB clients.

100+
POLICY TEMPLATES
NIST 800-171 and CIS-aligned policy library maintained and applied to every Guardian Compliance engagement.

24/7
MDR COVERAGE
Partner SOC monitoring, incident response runbooks, attorney-first escalation.