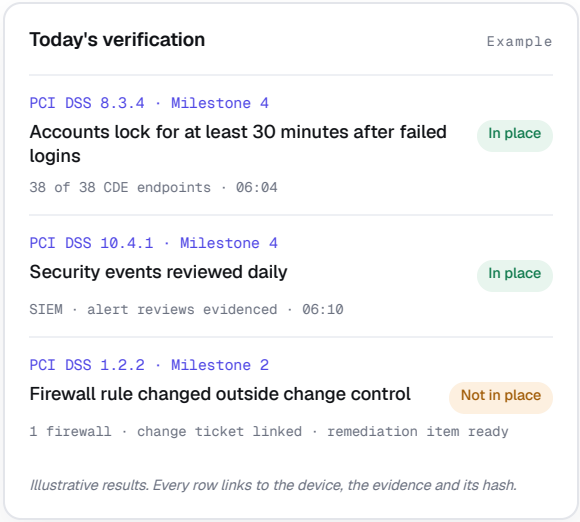
PCI DSS EDITION · NOVEMBER 2026

Stay PCI compliant every day, not just at assessment time.

Continu-US checks your cardholder data environment from the systems you already run: endpoints and payment workstations, firewalls and switches, cloud, ticketing and your SIEM. It shows where you stand against every PCI DSS v4.0.1 requirement in the scope of the method you validate under, and keeps the evidence to prove it — whether you complete a self-assessment questionnaire or a QSA writes your Report on Compliance. It runs in your own Azure environment.



260
PCI DSS v4.0.1 requirements mapped, down to the sub-requirement

12
validation methods built in: ten SAQs and both Reports on Compliance

40
recurring PCI activities scheduled: scans, tests, reviews and inspections

0
keys or passwords stored for your clouds; it runs in your Azure

SCOPE

The requirements your method actually contains

Validation method

Record how you validate — any of the ten self-assessment questionnaires, or either Report on Compliance — and the requirement list narrows to that method's own. A reduced SAQ scopes out what it does not contain, rather than leaving you to mark requirements not applicable by hand.

Entity profile

Merchant, service provider, or both. The profile decides what attaches to who you are rather than how you validate: the service-provider-only requirements, and Appendix A1 and A2, follow from it rather than from the questionnaire, so a reduced SAQ does not drop them. A service provider recorded against a merchant questionnaire is flagged as a mis-selection, not a scoping decision.

Indicated brand level

Enter annual transaction volumes by brand and the indicated level for each is worked out from that brand's own published thresholds, for merchants and for service providers, with your service-provider category — payment gateway, token service, payment facilitator and the rest — recorded alongside.

PROGRAM RECORDS

The records PCI expects you to keep, kept

Program registers

The registers an entity is expected to maintain — system components, media, wireless access points, point-of-interaction devices, third-party providers, the responsibility matrix, targeted risk analyses, scope, segmentation and the operational review — each tied to its requirement.

Critical control failure log

Requirement 10.7: each failure of a critical security control recorded with when it was detected, the cause, what was restored and how long it took, with your response captured against it.

Service provider obligations

If you are a service provider, the additional cadence PCI puts on you is scheduled and evidenced, and a customer evidence packet is produced that you can hand to your own customers.

Assessment readiness

Days remaining to your assessment date, progress against each milestone, the registers still to be completed, and alerts where a third-party service provider's own validation has lapsed.

WHAT IT DOES

Know where you stand on every requirement, all year

Continuous verification

Endpoints, payment workstations, network devices, cloud, ticketing and SIEM evidence checked on a set cadence, each result mapped to the PCI DSS requirement it supports.

Cardholder data environment scoping

Tag each device as in the CDE, connected-to or security-impacting, or out of scope. Out-of-scope devices are left out of PCI results and reports.

Compensating control worksheets

Record a complete worksheet for a requirement met through a compensating control: constraints, objective, risk, controls, validation and maintenance. If evidence for that requirement starts failing, it's flagged as a conflict.

Drift alerts

A setting that moves from its approved value shows up the day it happens, with the device and the before and after values, instead of at your next assessment.

Policies and procedures

Your security policies and operational procedures mapped to the requirements they support, with versions, owners, review dates and overdue reminders.

Findings and dispositions

Every failing check with its affected devices. Record not-applicable, informational or false-positive decisions with a reason, scope and review date.

PCI's own values, applied

Where PCI DSS is stricter than a general baseline, results are judged against PCI's figure. A 30-minute lockout duration (8.3.4) is checked as 30 minutes, not a shorter default.

Prioritized Approach workbook

Progress against all six milestones on one page, and a filled copy of PCI SSC's Prioritized Approach Tool for v4.0.1: status, stage of implementation and estimated dates from your remediation plan, each marked for assessor confirmation.

PCI activity calendar

The periodic work PCI DSS expects, scheduled and tracked with evidence: penetration and segmentation tests, ASV scans, access reviews, risk analyses, payment terminal inspections, rogue wireless checks and more, at frequencies within PCI's limits.

Remediation tracking

Raise a remediation item in one click from any failing finding, pre-filled with the weakness, plan and milestones. Owners, dates, change history and spreadsheet export.

Annual assessment report and evidence

An annual PCI DSS report in PCI terms (milestones, compensating controls, activities and deficiencies) and a hashed evidence package organized by requirement that your assessor can verify independently.

One location or many

Monitor a single merchant environment, or many: a service provider across its customers, or an organization with several entities, each with its own scope.

RESULTS IN PCI'S TERMS

Every requirement gets an indicated result your assessor recognizes

Continu-US indicates; your assessor decides. Each requirement is shown with the result its evidence points to, using the same terms as PCI DSS reporting.

In Place	In Place with CCW	Not in Place	Not Applicable	Not Tested
Passing checks, current activities or documents, and nothing failing.	Met through a recorded compensating control worksheet.	Failing or overdue evidence, or an open remediation item.	Outside your scope: not contained in your validation method, or tied to an entity type you are not.	Nothing decisive collected yet.

EVIDENCE SOURCES

Works from the systems you already run

No new platform to adopt. A lightweight, signed check script on endpoints; everything else comes from what you have.

ENDPOINTS

Windows and Linux, including payment workstations

Hardening, encryption, logging, patching, accounts, anti-malware and services, reported daily over an encrypted channel by a tamper-checked script.

NETWORK

Firewalls, routers and switches

Configurations evaluated for network security controls, segmentation and secure administration, with passwords and keys stripped before upload.

CLOUD

Microsoft 365, Azure, AWS, Google Cloud and Workspace

Identity, MFA, logging, data protection and configuration. Uploaded, or collected from connected accounts with no stored keys; hash-manifested.

PROCESS

Ticketing system

Change and vulnerability remediation records, so change control and patching requirements are verified from real tickets.

MONITORING

SIEM

Alert and case handling, so daily log review and incident response are backed by actual activity.

PEOPLE

Your team's records

Policies, procedures, scan and test reports, and recurring activities, kept beside the technical results. Word and Excel evidence attaches to the activity it supports.

FRAMEWORKS

PCI DSS first, with room for the rest of your obligations

FRAMEWORK	MAPPED TO
PCI DSS v4.0.1	260 requirements, each with its Prioritized Approach milestone, scoped to your validation method
NIST SP 800-53 Rev 5 Moderate	The 1,824 determination statements of NIST SP 800-53A
CMMC Level 2 / NIST SP 800-171 Rev 2	The 320 assessment objectives of NIST SP 800-171A

Also handle government or defense work? Switch views without re-collecting anything. Other frameworks, and your organization's own baseline, can be mapped during onboarding.

DEPLOYMENT AND SECURITY

Inside your environment, under your controls

YOUR AZURE SUBSCRIPTION

Continu-US managed application

Dashboard | Administration | Check-in service | Connectors | Immutable backups | Your Key Vault

Signs in through your Microsoft Entra tenant. AWS and Google are read through short-lived, read-only federated sign-ins your administrators set up, with no keys stored. Continu-US collects configuration and activity evidence, never cardholder data. Nothing is hosted by ATLLC and nothing calls home.

- **Your sign-in rules apply**
  Your MFA and Conditional Access policies govern access. Roles for administrators, activity recorders and read-only viewers.
- **You choose vendor access**
  A Supported plan with just-in-time access you approve each time, or a plan with no vendor access at all.
- **Built to protect evidence**
  Managed identities only (no storage keys), keys in your Key Vault, end-to-end encrypted check-ins, nightly immutable backups and an audit trail of every administrative action.
- **Locked installation**
  Deployed resources can't be altered outside the application, which keeps it supported and intact.
- **Licensed per organization**
  A signed license tied to your tenant, sized to your environment. If it lapses, the platform becomes read-only until it's renewed: your results and evidence stay viewable and exportable.

GETTING STARTED

Two ways to use it, one guided onboarding

MANAGED SERVICE

ATLLC runs it for you

Included in ATLLC's managed security services. You receive ongoing reports and remediation tracking without running the platform yourself.

LICENSED PLATFORM

Your team runs it day to day

Installed in your Azure subscription and used by your team, with ATLLC support when you need it.

Step 1

Discovery

Your cardholder data environment, scope, entity type and validation method, and baseline.

Step 2

Mapping

Checks, sources and devices aligned to the requirements that apply to you.

Step 3

Pilot

A small set of CDE devices and sources, verified with your team.

Step 4

Production

Full rollout, connectors on, activity calendar and reporting cadence agreed.

Onboarding time depends on the size and complexity of your cardholder data environment; we agree the plan during discovery.

ABOUT ANTHONY TIMBERS LLC

Built by assessors who know what evidence holds up

A cybersecurity and compliance firm in Fredericksburg, Virginia. ATLLC never assesses an organization it provides consulting or managed services to, so Continu-US is offered independently of any assessment engagement.

QSA	PCI Qualified Security Assessor company
C3PAO	Authorized CMMC Third-Party Assessment Organization
3PAO	FedRAMP Third-Party Assessment Organization
17020	ISO/IEC 17020 accredited
HACS	GSA Highly Adaptive Cybersecurity Services schedule

See it on your environment

Ask for a live demo at anthonytimbers.com.

The verification panel shows illustrative results, not client data. Continu-US indicates results; determinations of compliance are made by your assessor. PCI DSS is a standard of the PCI Security Standards Council. Capabilities described as of November 2026.