CMMC EDITION · NOVEMBER 2026

Prove your controls work every day, not once a year.

Continu-US checks your security controls from the systems you already run: endpoints, network devices, Microsoft 365 and Azure, AWS, Google Cloud and Google Workspace. It maps every result to the 320 assessment objectives of NIST SP 800-171A, keeps the evidence to prove it, and builds the system security plan and assessment artifacts from the same material. It runs in your own Azure environment, commercial or government.

Today's verification Example

3.13.11[a] · SC.L2-3.13.11
FIPS-validated cryptography enabled — Verified
42 of 42 endpoints · 06:04

3.1.3[e] · AC.L2-3.1.3
Data loss prevention enforced on Drive and Gmail — Verified
Google Workspace · connected account · 06:02

3.4.2[b] · CM.L2-3.4.2
Firewall rule changed from baseline — Drifted
1 firewall · change ticket linked · POA&M ready

Illustrative results. Every row links to the device, the evidence and its hash.

320
NIST SP 800-171A objectives mapped for CMMC Level 2

16
recurring activities scheduled: reviews, tests, trainings and tabletops

70
cloud and tenant configuration checks across Microsoft 365, Azure, AWS and Google

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

ASSESSMENT ARTIFACTS

The documents your assessment turns on, built from the evidence

System security plan

Your SSP generated as a Word document from the built-in template — structure and writing prompts, no one else's compliance text — or from your own, and filled with what the platform already holds: each family's requirements and objectives with their implementation statements beside the verified result, the CUI, Security Protection, Contractor Risk Managed and Specialized asset tables from the inventory, contacts, network and CUI flow diagrams, an inherited controls section naming each provider and its responsibility matrix, and a change log row for the version. Anything the platform can't fill is highlighted and listed before the document is produced, rather than shipped blank.

SPRS score

Your supplier performance risk score calculated from the same objective results the rest of the platform reports, so the figure you submit and the evidence behind it cannot drift apart.

POA&M register

Create items in one click from any failing finding or endpoint, network or cloud check, pre-filled with weakness, plan and milestones. 180-day clock, change history and spreadsheet export.

Reports and evidence packages

Assessment-period reports, per-device results and hashed evidence packages an assessor can verify independently, organized by objective.

Inherited controls and CRMs

Objectives provided wholly or partly by a provider are recorded with that provider and its customer responsibility matrix from the document register, and carried into the plan's inherited controls section rather than evidenced again locally.

Asset categories

CUI, Security Protection, Contractor Risk Managed and Specialized assets are categorised in the inventory, which decides both what counts toward your results and the asset tables written into the plan — including the authorized CUI user count.

WHAT IT DOES

An assessment-ready view of every control, kept current automatically

Continuous verification

Endpoints, cloud tenants and accounts, network devices, ticketing and SIEM evidence checked on a set cadence, each result mapped to its objective.

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.

Findings and dispositions

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

Stated vs. verified

Import your implementation statements and see where what you wrote differs from what your systems show — the gap an assessor finds first.

Scoping and tailoring

Asset categories plus inherited and not-applicable objectives, so results reflect your actual boundary rather than the whole catalog.

Document register

Policies, procedures and plans mapped to objectives, with versions, owners, review dates and overdue reminders.

Recurring activities

Reviews, tests and trainings scheduled and tracked with evidence, so periodic controls don't slip between assessments.

Baseline compliance

Bring your own STIG, CIS or Group Policy baseline. Results grouped by benchmark or GPO with CAT I/II/III severity, and STIG Viewer checklists (.ckl, .cklb) exported per device.

Connected cloud accounts

AWS, Google Cloud and Google Workspace collected through workload identity federation: short-lived, read-only access, no keys or passwords stored.

Credential expiry

Application secrets and certificates nearing expiry are named with their days remaining, so a connected integration doesn't lapse quietly and leave a gap in the evidence.

Tenant configuration

Conditional Access, privileged roles, authentication methods, logging and diagnostics evaluated against the configuration a Level 2 environment is expected to hold.

One organization or many

Monitor your own environment, or many: an MSP across its customers, or a prime watching its suppliers, each with its own scope and framework.

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

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

CLOUD

Microsoft 365, Azure, AWS, Google Cloud and Workspace

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

NETWORK

Firewalls and switches

Configurations evaluated against your baseline, with passwords and keys stripped before upload.

PROCESS

Ticketing system

Vulnerability remediation and change records, so process controls are verified from real tickets.

MONITORING

SIEM

Alert and case handling, so monitoring and incident response are backed by actual activity.

PEOPLE

Your team's records

Documents, recurring activities and implementation statements, kept beside the technical results. Word and Excel evidence attaches to the activity it supports.

FRAMEWORKS

One set of evidence, mapped to the framework you're assessed against

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

Switch views without re-collecting anything. Other frameworks, and your organization's own baseline, can be mapped during onboarding.

DEPLOYMENT AND SECURITY

Inside your boundary, 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. Azure Commercial or Azure Government. AWS and Google are read through short-lived, read-only federated sign-ins your administrators set up, with no keys stored. 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 are never locked away and 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 POA&M 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

What you run, your scope and your baseline.

Step 2

Mapping

Checks and sources aligned to your framework and configuration.

Step 3

Pilot

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

Step 4

Production

Full rollout, connectors on, reporting cadence agreed.

A typical small or mid-size defense supplier is fully onboarded in 4 to 6 weeks.

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.

C3PAO	Authorized CMMC Third-Party Assessment Organization, with CMMC Certified Assessors
3PAO	FedRAMP Third-Party Assessment Organization
QSA	PCI Qualified Security Assessor company
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. Capabilities described as of November 2026.