

# Turning Compliance Readiness into Competitive Advantage

Cybersecurity Maturity Model Certification (CMMC) makes cybersecurity a contractual requirement across the defense supply chain. While MSPs are not required to certify, those managing systems containing CUI or FCI must demonstrate alignment to CMMC Level 2 to support defense contractors. NinjaOne helps MSPs meet these requirements through a FedRAMP®-Authorized platform built for secure, multi-tenant managed services.

## Platform security and compliance



### Support CMMC readiness

- + Unified visibility and control across in-scope customer environments
- + Proactive remediation and automated patching aligned to CMMC Level 2
- + Centralized asset inventory to support audit readiness

### Protect against cyber attacks

- + Centralized security policy management
- + Role-based access control (RBAC), MFA, and SSO integration across managed environments
- + AI-driven patch intelligence and secure data backups
- + Rapid deployment and technician proficiency within 10 days

### Prove and maintain compliance

- + Continuous monitoring across in-scope systems
- + Automated response workflows to reduce audit and operational risk
- + Centralized dashboards and reports to demonstrate control alignment

**CMMC isn't just a mandate — it's a market shift that rewards MSPs who lead with trust, security, and strategy**

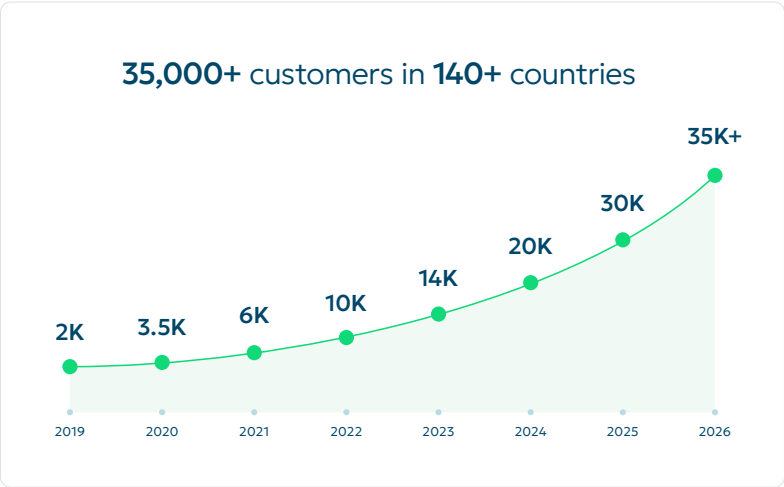
- + Support high-value defense clients and deliver premium, compliance-ready services
- + Differentiate by guiding clients through CMMC readiness — not just selling IT
- + Help clients retain contracts, reduce insurance risk, and win more business



NinjaOne  
named a  
Leader by  
Gartner®



Read the  
2026 Gartner® Magic  
Quadrant™ for  
Endpoint Management.



## Unify IT to simplify work.

The NinjaOne Unified IT Operations Platform delivers endpoint management, autonomous patching, backup, and remote access in a single console to cut spend, increase resilience, and improve efficiency. The platform eliminates IT complexity by bringing these capabilities together in an intuitive interface that teams can easily master. By automating routine work and reducing tool sprawl, organizations gain rapid time to value and deliver a better technology experience for employees. NinjaOne remains committed to customer success and has maintained a 98 percent satisfaction score for more than five years.

Seamless. Powerful. Effortless. That's NinjaOne.  
Learn more at <https://www.ninjaone.com/msp/>

## CMMC Overview

Most organizations will begin their journey at Level 2, which represents broad protection of CUI.

LEVEL 1	Basic safeguarding of FCI	
MODEL	ASSESSMENT	REQUIREMENTS
<b>15 REQ.</b> Aligned with FAR 52.204-21	<ul style="list-style-type: none"> <li>Annual Self Assessment</li> <li>Annual Affirmation</li> </ul>	<ul style="list-style-type: none"> <li>Annual self-assessment and annual affirmation of compliance with the 15 security requirements in FAR clause 52.204-21.</li> </ul>
LEVEL 2	Broad protection of CUI	
MODEL	ASSESSMENT	REQUIREMENTS
<b>110 REQ.</b> Aligned with NIST 52.204-21	<ul style="list-style-type: none"> <li>C3PAO certification assessment every 3 years, or</li> <li>Self assessment every 3 years of select programs</li> <li>Annual Affirmation</li> </ul>	<ul style="list-style-type: none"> <li>Either a self-assessment or a C3PAO assessment every three years, as specified in the solicitation.</li> <li>Decided by the type of information processed, transmitted, or stored on the contractor or subcontractor information systems.</li> <li>Annual affirmation, verify compliance with the 110 security requirements in NIST SP 800-171 Revision 2.</li> </ul>
LEVEL 3	Advanced protection of CUI (with third-party assessment)	
MODEL	ASSESSMENT	REQUIREMENTS
<b>134 REQ.</b> 110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172	<ul style="list-style-type: none"> <li>DIBCAC certification assessment every 3 years</li> <li>Annual Affirmation</li> </ul>	<ul style="list-style-type: none"> <li>Achieve CMMC Status of Final Level 2.</li> <li>Undergo an assessment every three years by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).</li> <li>Provide an annual affirmation verifying compliance with the 24 identified requirements from NIST SP 800-172.</li> </ul>