

The NIST Cybersecurity Framework (CSF) 2.0 provides a clear roadmap for managing and reducing cybersecurity risks. As a Cisco Premier Advisor partner, Majentai delivers tailored solutions to help organizations with NIST requirements, ensuring stronger security, seamless compliance, and operational resilience.

Engagement Scope

Majantai provides end-to-end support for achieving NIST CSF 2.0 compliance. Our services include conducting gap analyses to assess your current security posture, designing tailored solutions, and integrating advanced Cisco technologies to align with the framework's core functions. We validate use cases, optimize policies, and empower your team with the knowledge and tools needed to maintain compliance and enhance security long-term.

The following matrix shows the Cisco products that provide compliance and protection according to NIST 2.0:

Our Offerings

- NIST 2.0 Compliance Assessment
- Proof-of-Value or Pilot Deployments
- Enablement Workshops
- Implementation & Adoption Services
- Automation & Integration Services
- Managed Services

Figure 1: Cisco Capability mapping to NIST CSF 2.0

Figure 1: Cisco Capability mapping to NIST CSF 2.0

Function	Category	Network Security	Device Security	User Security	Cloud Security	App Security	Analytics	Industrial Security	Other	Splunk Capabilities	
		Cisco Firewalls Cisco Defense Orchestrator Cisco Identity Services Engine Cisco Multicloud Defense Cisco XDR Cisco Secure Client Cisco Secure Endpoint Cisco Security Connector Cisco Meraki Systems Manager Cisco Duo Cisco Secure Email Threat Defense Cisco Secure Access (SSE) Cisco Secure Web Appliance Cisco Attack Surface Management Cisco Cloud Application Security Cisco Umbrella Cisco Secure Workload Cisco Secure WAF Secure Malware Analytics Secure Network Analytics Security Analytics and Logging Cisco Telemetry Broker Cisco Industrial Threat Defense Cisco Cyber Vision Secure Equipment Access Cisco Secure DDoS Protection Cisco Vulnerability Management Splunk Core Splunk Asset & Risk Intelligence Splunk Enterprise Security Splunk Attack Analyzer Splunk User Behavior Analytics Splunk SOAR									
GOVERN (GV)		Non-technical controls									
IDENTIFY (ID)	Asset Management (ID.AM)										
	Risk Assessment (ID.RA)										
	Improvement (ID.IM)	Non-technical controls									
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AA)										
	Awareness and Training (PR.AT)	Non-technical controls									
	Data Security (PR.DS)										
	Platform Security (PR.PS)										
DETECT (DE)	Technology Infrastructure Resilience (PR.IR)										
	Continuous Monitoring (DE.CM)										
	Adverse Event Analysis (DE.AE)										
RESPOND (RS)	Incident Management (RS.MA)	Non-technical controls									
	Incident Analysis (RS.AN)										
	Incident Response Reporting and Communication (RS.CO)	Non-technical controls									
	Incident Mitigation (RS.MI)										
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)										
	Incident Recovery Communication (RC.CO)	Non-technical controls									



majentai
GUARDIANS

Majentai is a world-class Cybersecurity services provider, dedicated to implement, integrate and operate the most resilient Cybersecurity platforms using proven state-of-the-art technologies. With a team of seasoned experts and cutting-edge technology, we deliver comprehensive solutions tailored to our clients' unique needs, ensuring their digital assets remain secure in an increasingly complex cyber landscape.

For more information or to engage our services, please contact us at info@majentai.com or visit <https://majentai.com>