ciena | blueplanet
a division of ciena

INFOBRIEF

Ciena security posture overview

Ciena is driven by a relentless pursuit of network innovation, enabling our customers to adapt within ever-changing environments to deliver richer and more connected experiences for their business and users. A key driver of those ever-changing environments includes a continually evolving landscape of cyber threats. Ciena's security program is aligned to industry standards and frameworks such as ISO 27001, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), National Security Agency (NSA) "Defense in Depth" strategies, the Secure Controls Framework, the Unified Control Framework, the confidentiality, integrity, and availability (CIA) triad security model, and others. Ciena focuses its security program on these industry standards and the following framework that underpins the program:

- Diligence: Protect the company from evolving threats
- Integrity: Do the right things, and do them well
- Transparency: Build trust in our products and program
- Teamwork: Proactive relationships with our customers and suppliers

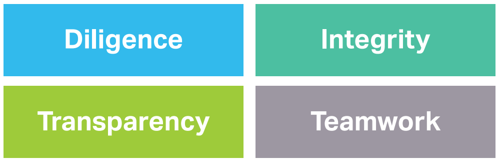

Figure 1. Standards of Ciena's security program

Ciena delivers a robust security program so that our customers can focus on providing industry-leading technology to their end-users.

Diligence

Ciena's security program aligns with the NIST CSF—among other industry frameworks—which focuses on five functional activities: identify, protect, detect, recover, respond, and govern.

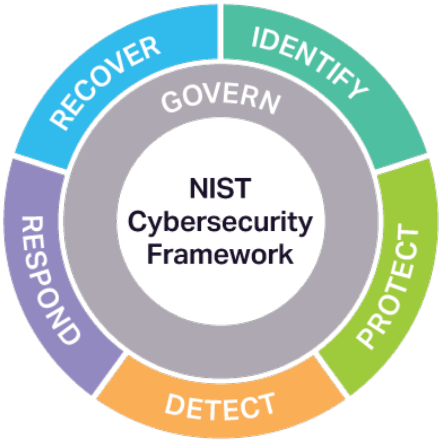

Figure 2. NIST CSF

These functional activities represent a fundamental foundation for a robust and comprehensive security program. Ciena's pursuit of program maturity is regularly assessed and measured within these functional areas.

Enterprise security: Ciena uses a comprehensive layered approach, using the NSA "Defense in Depth" methodology to protect our assets (physical, intellectual property, operational capability) and records. The following techniques are a few examples of the tooling and security that our professionals deploy to ensure we are safeguarding our environments in a holistic fashion:

- Comprehensive deployment of market-leading endpoint detection and response security agents
- Network intrusion prevention sensors at key points of network ingress and egress
- Global deployment of security-focused net flow sensors for the detection of malicious, suspicious, and anomalous network traffic
- A centralized and monitored security information event management (SIEM) platform for collection and correlation of security relevant event data
- Aligning to industry standards for encryption in transit and at rest, such as TLS 1.2, AES256, and FIPS 140-2
- A dedicated security governance function that proactively aligns security policy and controls with a consolidated Unified Control Framework
- Multiple managed security service providers that monitor our network and security controls 24 x 7 x 365
- Layered email security/anti-phishing platforms for our corporate email platform
- Comprehensive multi-factor authentication (MFA) for all email, network, and key system access
- A dedicated internal team focused on security monitoring and analysis and incident response
- A comprehensive vulnerability and exposure management function that conducts regular recurring vulnerability assessments
- Continual evaluation of our environment from an attacker's perspective
- Constant training and assessment of employees' physical and cybersecurity procedures

Physical security: Ciena controls physical security through a global workplace security team that manages physical access control, CCTV systems, personnel security, and travel security. Ciena maintains physical and environmental controls in all secured facilities in alignment with industry best practices. Physical access to corporate spaces requires keycard access, with access limited to least-privilege need in sensitive spaces. Physical access is monitored with alarm systems and corporate security guards. There are additional environmental controls and security controls for lab and IT spaces.

Integrity

Monitoring and analysis: Ciena maintains 24 x 7 x 365 'eyes on glass' to ensure we are diligent regarding incident identification and eradication. We have staff internally focused on monitoring and analysis, as well as multiple industry-leading managed security service providers (MSSPs) that monitor and alert on our environments around the clock.

Detection engineering and threat intelligence: Ciena's security team knows that the security threat landscape is ever evolving. Therefore, our team continues to use the MITRE ATT&CK framework and others to track and correlate cyber adversaries and strengthen our security posture.

Ciena maintains memberships with top-tier industry organizations to stay updated on the evolving threat landscape, thereby enhancing and disseminating security advancements. These memberships include prominent organizations such as the Cloud Security Alliance (CSA), the Information Technology - Information Sharing and Analysis Center (IT-ISAC), and the Network Security Information Exchange (NSIE).

Vulnerability and exposure management: Ciena maintains a robust functional team and process supporting vulnerability and exposure management across all enterprise assets, including routine vulnerability scans and ad-hoc scanning.
We conduct scans monthly, using various industry-leading assessment tools to conduct cloud security, container security, network detection and response, threat intelligence, application security, and data metric analysis. Ciena also conducts annual penetration testing of our systems. We maintain a comprehensive vulnerability and exposure management function that conducts regular recurring vulnerability assessments, as well as a dedicated security testing and assessment function that conducts continual evaluation of our environment from an attacker's perspective.

Please refer to our Notice of Vulnerability Disclosure Policy.

Governance, risk, and compliance: With the cybersecurity threat landscape continuing to evolve, it is important that security teams are on top of managing their program to ensure risks are reduced or eliminated expeditiously. Therefore, Ciena has a dedicated security governance, risk, and compliance team focused on ensuring our policies and controls are implemented, governed, and effective. Our risk team conducts risk-modeling exercises and assessments to validate that risks are being treated with the appropriate level of rigor.

Ciena operates a risk management function in which the security risk management team conducts initial assessments to establish risk tiers. Further due diligence is carried out based on the cyber-risk tier, and an assessment of the cyber-risk exposure is then produced for the business stakeholder. The stakeholder, together with the appropriate leadership, makes to support informed decisions regarding risk treatment (acceptance, deference, transference, mitigation) and the implementation of actions to decrease the risk tier.

The compliance readiness function operates to establish a refined and efficient process for assessing and ensuring that the security team meets or surpasses applicable regulatory requirements, customer contractual obligations, and relevant industry standards. The Unified Control Framework serves as a foundation for the compliance readiness function, offering a comprehensive perspective on the requirements and standards that Ciena needs to fulfill. As a publicly traded company and subject to the U.S. Sarbanes-Oxley (SOX) Act, the controls that ensure confidentiality and integrity of key records and financial systems are regularly validated both internally and by a third-party accounting firm before certification by our CFO and CEO.

Security architecture and engineering

Within Ciena's security organization exists a group of teams specifically dedicated to security architecture and engineering functions. These functions are security platforms and automation; cloud security; data security and privacy; identity and access management security; and infrastructure and systems security, which includes defensible network architecture and defensible build and configuration functions. These teams work tirelessly to ensure that Ciena systems and environments are designed with security in mind.

Security personnel: The security team at Ciena includes cybersecurity professionals with experience in various security fields and industry certifications—including Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), CompTIA Security+, and CompTIA Network+.

Ciena's security area of operations and functions are regularly reviewed for continual development, improvement, and alignment with Ciena's corporate security goals, regulatory and legal compliance for data privacy and confidentiality requirements, third-party cyber due diligence, and other enterprise-wide information security requirements.

Incident management: Ciena uses many controls to ensure we can adequately monitor and protect our environments. We have documented procedures to assist designated Ciena personnel in mitigating the risks from cybersecurity incidents by responding to incidents effectively and efficiently. Our team conducts weekly informal tabletop testing and review of our incident processes, as well as annual full testing of incident response activities. Incident notification timelines are typically determined within individual customer contracts, with a standard to not exceed 72 hours from confirmation of an event.

Transparency

Application and product security: Ciena is committed to ensuring our products, applications, and tools are built with security in mind. Ciena has standardized the software lifecycle and support policy across the entire product portfolio, including the embedded software in our network elements and network management and planning tools, as well as our Blue Planet portfolio. This comprehensive policy is in place for all current and future software products and releases.
Ciena develops products with a range of security requirements, which are implemented on a product-by-product basis to address their specific needs.

Customers can access specific product security information through the myCiena portal.

Customer trust and sales-enablement security: At Ciena, we know our customers' success is dependent on the confidence and trust in their suppliers. Therefore, we have established a dedicated function of cybersecurity professionals specifically to address customer questions, risk assessments, call requests, or other security needs. This team is also dedicated to developing materials to help our customers understand Ciena's security posture and allow for seamless due-diligence practices for those who matter most: our customers. The security customer trust team at Ciena is working to proactively develop materials to be used by our customers, such as:

- Standardized information gathering (SIG) assessments
- Comprehensive assessment initiative questionnaires (CAIQs)
- Pursuit of compliance certification evaluations, such as SOC 2 Type 2 and ISO 27001

Security training awareness and communication: People are our greatest asset. Unfortunately, they can also be one of our main targets for cyber-threat actors. Therefore, Ciena maintains a security training awareness and communication function to drive security and risk-aware behavior through engaging and tailored learning experiences. Each employee is required to complete annual security training, and we engage all employees in monthly role-based phishing simulative testing and training with progressive maturity. Furthermore, Ciena spotlights every October on security by celebrating Cybersecurity Awareness Month, hosted by the National Cybersecurity Alliance and the Cybersecurity and Infrastructure Agency (CISA).

Teamwork

Shared responsibility: Ciena monitors and responds to security threats related to the cloud and our environments. However, individual customers must ensure they are responsible for protecting the data they are using within our tools and environments. Security is everyone's responsibility. Therefore, Ciena ensures that we build our products and services with shared responsibility in mind. While Ciena ensures the tools, products, and services we build are secure, we also work directly with our customers to help them build security on their end.

Ciena is primarily responsible for controls within our internal systems, as well as physical layer/hardware and infrastructure security, network layer controls for the services we provide to our customers, virtualization controls, and hosting/provider security controls.

Customers are typically also responsible for secure best practices on their systems in the following areas:

- Identity and access management (IAM)
- User security and credentials
- Security awareness of customer employees
- Endpoint security
- Configurations
- APIs and middleware
- Software code

As Ciena continues to evolve our security operations, we are committed to collaborating with our customers where they need it most.

What about data privacy?

Your privacy is important to us: We respect your privacy and are committed to protecting it. We created the following notice to provide transparency surrounding how Ciena may collect, use, and share your personal information and how Ciena protects your personal information. For more information, see our Privacy Policy.