USE CASE

BRADFORD NETWORKS

Network Sentry & NATIONAL INSTITUTE OF STANDARDS CYBERSECURITY FRAMEWORK

Taking enterprise network security to the next level requires strategic planning, as well as a holistic understanding of your organization's unique risk profile, business challenges and the security lifecycle.

The current state of cybersecurity guidance can sometimes seem disjointed and composed of countless standards endorsed by different agencies, governments, and private sector groups, not all of which overlap in their advice. They all have the best intent to steer organizations beyond a "checkbox security" mentality, but sometimes they can add confusion to an already complex ecosystem.

Thankfully, efforts are underway to standardize cybersecurity guidance so security professionals across industries and verticals can speak the same language. On the forefront of this endeavor is the National Institute of Standards and Technology (NIST), which created its own Cybersecurity Framework (CSF). Initially developed to aid critical infrastructure organizations with their specific cybersecurity challenges, a U.S. Government executive order made compliance with the NIST CSF a requirement for all federal agencies in 2017. It is now being widely adopted by businesses because it provides a comprehensive inventory of every major step in the security lifecycle using industry-agnostic language.

Understanding the NIST Cybersecurity Framework

The NIST CSF divides the key components of the security lifecycle and its corresponding requirements into five core functions:

- Identify
- Protect
- Detect
- Respond
- Recover

Each of the functions contains categories and subcategories that delineate recommended processes, systems, standards and practices an organization should have in place to successfully meet specific security challenges. The NIST CSF notes that every category and subcategory is context-sensitive to an organization's unique business requirements and network infrastructure, and as such, should be adapted to the organization's requirements, and not the other way around.

Network Sentry's security automation and orchestration solution corresponds directly to each function of NIST's CSF, providing unparalleled visibility into endpoint devices, control over assets, and automated threat response and serving as a single pane of glass for agencies and organizations seeking to be in compliance.

NETWORK SENTRY CAPABILITIES AT A GLANCE

VISIBILITY

- » Provides continuous view of all endpoint devices on the network
- » Discovers all network infrastructure devices to detect and prevent risky network infrastructure changes
- » Automates guest management, offloading workload from IT staff

CONTROL

- » Continuously monitors security posture of each endpoint device to enforce compliance with regulations including NIST, HIPAA, and GDPR
- » Enables dynamic configuration using "EasyConnect" to onboard thousands of endpoint devices concurrently
- » Enables logical network segmentation to control access to sensitive data with role-based dynamic network access control

RESPONSE

- » Triages security events to generate actionable alerts and enforce endpoint containment
- » Provides context into alerted security events with detailed status of each network-connected endpoint and device, pinpointing threats quickly for faster mitigation
- » Reduces containment time from days to seconds with policy-based Automated Threat Response
- » Accelerates forensic investigations using built-in analytics of historical data tied to security events

Network Sentry prepares organizations to comply with the five functions of the NIST Cybersecurity Framework. Network Sentry's core product features that address compliance are listed in bold below:

Cybersecurity Framework from National Institute of Standards and Technology

FUNCTIONS	CATEGORIES	SUBCATEGORIES (those addressed by Network Sentry are listed in bold)
IDENTIFY	Asset management Risk assessment	**Inventory of physical devices, systems, software platforms and applications** **Provide network-aware context to help prioritize criticality of endpoints** **Identify and document asset vulnerabilities** Determine risk by measuring potential threats, vulnerabilities, likelihoods and impacts Identify and prioritize risk responses
PROTECT	Access control Data security Information protection Processes and procedures Protective technology	**Manage access of identities and credentials for authorized devices and users** **Protect network integrity** Manage and protect physical access to assets Manage remote access to assets Manage access permissions Manage assets throughout any removal, transfer or disposition process Verify software, firmware and information integrity Keep development and testing environments separated
DETECT	Anomalies and events Security continuous monitoring Detection processes	**Triage critical nature of network alerts** **Monitor network for potential events** **Aggregate and correlate event data from multiple sources and sensors** Analyze detected events to understand attack targets and methods Determine impact of events Establish incident alert thresholds Monitor physical environment for potential cybersecurity events Monitor for unauthorized personnel, connections, devices, and software Perform vulnerability scans Test detection processes Communicate event detection information to appropriate parties Continuously improve detection processes
RESPONSE	Analysis Mitigation Improvements	**Investigate notifications from detection systems** **Understand incident impacts** **Contain incidents** Perform forensics Categorize incidents within response plan parameters Mitigate or document newly-identified vulnerabilities Incorporate lessons learned into response plans Update response strategies
RECOVER	Recovery planning Improvements Communications	**Providing valuable data points for post-mortems, future response plans, and communications to stakeholders** Executing a recovery plan Incorporating lessons learned into recovery plan

If your organization is embarking on mapping your security processes to the NIST Framework, Network Sentry can help you secure your endpoints, your users and your network.

Contact Bradford Networks today to learn more or to get a hands-on demonstration of Network Sentry +1 866.990.3799, or visit www.bradfordnetworks.com

BRADFORD NETWORKS
374 Congress Street, Suite 502, Boston, MA 02210, USA
Toll Free +1 866.990.3799 | Phone +1 603.228.5300
Email info@bradfordnetworks.com
Web www.bradfordnetworks.com