Network and Endpoint Security

You need the capability for employees to work from anywhere using various devices. You want people to securely authenticate and be identified from the devices they're using.

Every device that employees use to connect to enterprise networks represents a potential risk that cyber criminals can exploit to steal your organization's data. The number and variety of end-users is growing, so the task of continuously securing them becomes increasingly more challenging. As your security perimeter expands, organizations realize the necessity of developing and implementing a comprehensive cybersecurity strategy that integrates their network security and endpoint security efforts.

Zero Trust is the coordinated use of multiple security countermeasures to better protect the integrity of the network and its users, data, and assets from cybercriminals. A Zero Trust strategy is capable of defending you against a diverse and sophisticated threat landscape.

Choosing the wrong network and endpoint security solutions can leave your users vulnerable to threats and impede, or undo, the significant work that has gone into securing network. Your Zero Trust strategy should secure all endpoints continuously, as well as bring additional capabilities to your organization and improve your network security posture.

NFF Approach to Network and Endpoint Security Transformation

Building a high-performing security solution requires a new approach to looking at network infrastructure and operations. As a performance-focused integrator, Networking For Future (NFF) provides expertise, consulting, and solution design to transform security with a Zero Trust strategy. We'll deliver a solid network and endpoint security roadmap and a clear path forward, from strategy and consulting to implementation and managed services that provides you with greater agility, reliability, performance, and lower IT costs.

With a proven methodology, expert certified IT professionals, and managed services, we help you select, procure, implement, manage, and support the network and endpoint security solutions best suited to your workload and business requirements.

Looking To Solve:

- **Zero Trust Strategy Development**
- **Cybersecurity Threats**
- **Ransomware Mitigation**
- **DDOS Attack Threats**
- **Network Security Management**
- **Endpoint Protection and Encryption**
- **Internet of Things (IoT) Protection**

Key elements of our methodology and capabilities include determining business requirements and their impact on the IT architecture framework and how to translate your organization's Zero Trust strategy into future IT requirements. The NFF approach can be summarized as follows:

Initial Assessment

NFF begins with understanding your business objectives and vision, ascertaining your risk and technology profile, and developing a gap analysis from your current network and endpoint security resources and utilization states.

Network and Endpoint Security

NFF integrates business, risks, technology, and network infrastructure strategic planning capabilities. Our delivery framework is based around a unique ability to create relevant elements that enable an integrated, predictable, and right-sized Zero Trust strategy over time.

Transitioning from a traditional network and endpoint security framework to a Zero Trust architecture requires careful management from application owners, infrastructure engineers, and information security specialists to be successful.

NFF involves you and your team in determining risk tolerances derived from each stakeholder. We assist you in removing the constraints of your existing network infrastructure and help you rationalize your future security needs versus IT needs and service objectives. This sets the stage for the manner in which IT teams and network and endpoint security solutions are properly planned, built, and managed for the long term.

Future Model

The main objective of this stage is to develop the future network and endpoint security demand model in terms of security data analytics, trusted identity services, content filtering, and security threat defenses. From this, the future topology and the required resiliency for each cybersecurity solution under consideration can be established.

NFF has in-depth expertise in future Zero Trust strategic planning. Network and endpoint attributes include the understanding and development of reliability and availability requirements for IT architecture, infrastructure, and applications. It is very important to understand how both the technology and security infrastructures interact within the areas of risk tolerances, availability, and reliability requirements to properly develop the right-sized future models.

Based on our expertise and past experience, we can rationalize and predict the impact from risks, make technology recommendations for network and endpoint security sourcing options, and assist in determining how the IT infrastructure and security environments are chosen, sized, and managed over time. The proposed security solutions will enable high levels of predictability, agility, and manageability.

Proposed Transformation Roadmap

Understanding the model implications and possible consolidation and/or optimization savings over time are core components to enhancing your current and future capabilities. NFF will develop a proposed transformation roadmap with reviews of sourcing options, operating models, and migration strategies. The proposed roadmap contains cost modeling and ROI analysis for your future network and endpoint security framework.

Professional Services

Network and endpoint security transformation, consolidation, and Zero Trust migration projects often stretch a client's IT operations team. The proposed transformation roadmap will provide insight to the future architecture and engineering services requirements for fulfilling the Zero Trust strategy and to meet your business objectives. NFF has been providing network and security services for over 25 years.

Result

Our customized network and endpoint security roadmap helps ensure the optimum security posture for your organization. A strong security posture minimizes risk, which means you have the necessary processes in place to protect your applications, your assets, and your business from vulnerabilities and threats.

Network and Endpoint Security

Below are some examples of the Network and Endpoint Security projects we've completed for our clients.

The MITRE Corporation (MITRE)

NFF has been engaged with MITRE for security network design consulting services to develop a Cisco Identity Services Engine (ISE) Lab. This project provides a functional testing environment for advanced security options in which multiple designs and scenarios for Cisco ISE can be tested prior to implementation in their nationwide corporate locations.

NFF facilitated multiple design workshops to develop the workflow of features with focus on EAP-TLS authentication on MITRE's wireless networks, guest management, BYOD and mobile provisioning, Mac provisioning and profiling services. As a result, MITRE will have a functional ISE Lab in which they can demonstrate ISE functionality via network switches, wireless LAN controllers, Cisco VPN AnyConnect software endpoints and integration with PKI.

District of Columbia Metropolitan Police Department (DC MPD)

NFF engineers implemented MPD's secure communication link to the United States Secret Service's Multi-Agency Coordination Center (MACC) in Herndon, VA in support of the 55th Presidential Inauguration. These separate data paths were used to transport streaming video feeds from both MPD and from DC Government's Wireless Accelerated Responder Network (WARN), Naval Research Lab (NRL), and Department of Homeland Security (DHS).

MPD and the Secret Service were able to monitor Inaugural activities from the ground with fixed cameras and roving vehicles, and in the air from helicopters provided by the U.S. Capitol and U.S. Park Police. Due to NFF's efforts and technical design, as well as the unique collaboration between the District and Federal governments, the 55th Presidential Inauguration took place under the most technologically advanced security umbrella in United States Inaugural history.

Washington Metropolitan Transit Authority (WMATA)

NFF has provided a wide array of security services for the Washington Metropolitan Area Transit Authority (WMATA):

- Led the development of WMATA's IT Security Compliance Programs.
- Incorporating security requirements and standards for agency-wide acceptance and distribution, NFF reviewed, updated, and wrote the security policy and instructions.
- NFF's Assessment Survey documented IT business requirements and developed the WMATA IT Security Department Continuity of Operations (COOP) Plan.
- Acted as the WMATA Security Division representative for Disaster Recovery (DR) planning meetings.
- Certification and Accreditation: Evaluated and tracked the Plan of Action and Milestones that resulted in the Security division General Support System certification and accreditation.
- Audit Coordination and Response: Internal OIG: Responded to audit requests by the agency Office of the Inspector General internal audit. Guided agency through the annual external audit, met with the auditors, gathered artifacts requested by the auditor, responded to auditor requests and closed out audit findings by acquiring and providing proper evidence to show compliance.
- Developed IT Non-Compliance Reports for systems identified by the Security Division as not meeting agency information security standards.

Network and Endpoint Security

Government of the District of Columbia (DCGOV)

As the acting DCGOV Chief Information Security Officer (CISO), the NFF consultant designed and executed plans for staffing, organizing, and directing the Chief Information Security Officer Organization. Responsible for technical solution design, development, implementation, and enterprise architecture governance of 85 DC agencies, the CISO assesses overarching security requirements as they relate to solution delivery and network operations.

- Reviewed skills, experience, roles, and responsibilities of current security operations and policy development staff.
- Reorganized security operations and governance function.
- Established IT security policy creation priorities to close mission critical policy gaps in network, system, and application security.
- Planned and executed HIPAA security compliance assessments targeting allied government entities.
- Established a policy creation framework leveraging government and industry-wide standards frameworks (e.g., FISMA, ISO, and COBIT).
- Refined the organization's policy review board (PRB) charter, created policy governance procedures, and started disciplined security architecture processes.
- Developed IT security program communications strategy targeting key stakeholders and customers of IT services.
- Conducted FISMA compliance analysis of the DCGOV network security architecture and infrastructure.
- Developed a white paper regarding development and implementation of a HIPAA-compliant private cloud computing solution.

United States Census Bureau

NFF has been architecting, implementing, and supporting critical enterprise solutions for the U.S. Census Bureau for 10 years, including: nationwide information security architecture, hands on solutions integration and testing, design and implementation of web/email filtering solutions, preparation of disaster recovery plans for network and security devices, IPv6 testing and transition planning.

NFF deployed a full Cisco Identity Services Engine (ISE) solution for all wireless networks and manages seven ISE appliances to support wireless users and 10,000 VPN AnyConnect remote users. A large scale ISE solution for all wired networked devices to support an additional 30,000 licenses is in process.

SureScripts

SureScripts is the nation's largest E-prescription network, specializing in online prescription ordering. NFF implemented Cisco Network Admission Control (NAC) and wireless LAN controller systems mitigating SureScripts' virus and malware-based security threats by monitoring security protection on endpoint devices and enforcing security policies. This resulted in fewer virus infections, fewer help desk calls, and a more resilient secure network infrastructure.

Request a network and endpoint security meeting at **sales@nffinc.com**.