OPTIMIZING ENTERPRISE SECURITY ARCHITECTURE

Problem:
• Securing highly sensitive data across more than 680 Court locations and 94 judicial districts
• Preventing cyber attacks

Solution:
• Reduced number of cyber threats & vulnerabilities across the enterprise
• Enhanced continuity of IT resources throughout the Judiciary
• Centralized policy-based routing and networking to adapt to evolving APTs, requirements, and security mandates such as NIST and RMF across the Judiciary enterprise

Customer Challenges

The United States Courts service has a robust IT infrastructure that deals with large volumes of highly sensitive data. Our customer needed to optimize their security architecture across more than 680 Court locations and 94 judicial districts to prevent and reduce risk of cyber APTs and attacks.

AI Solution Features

AI security engineers have worked continuously with US Courts for over a decade to enhance security controls across their IT environments and re-design their enterprise security architecture to reduce the risk and impact of cyber threats. We have successfully implemented new hardware-based Firewalls at each of the Court sites through the Judiciary Firewall Service (JFS) initiative. Our work includes monitoring and evaluating traffic at each site to ensure that all mission-essential data remains available, and identifying behaviors indicative of breach attempts and external cyber-attacks. AI has implemented risk management strategies based on continuous cyber vulnerability and risk assessments, working closely with individual Courts and OEMs. We led the data center modernization program, including the design, configuration, and implementation of enhanced enterprise security architecture. AI implemented and manages the VMware NSX software defined network (SDN) environment, enabling the Judiciary to take advantage of additional security features, and designed new features to the Judiciary's mail gateway to guard against sensitive data exfiltration and external

phishing attacks.

Benefits to the Customer Mission

AI's work over the past ten years have provided multiple benefits to the Courts' mission objectives, significantly improving the overall security posture across the entire enterprise IT environment.

- Reduced number of cyber threats & vulnerabilities across the enterprise
- Enhanced continuity of IT resources throughout the Judiciary
- Enhanced network security architecture and resilience against malicious security attacks
- Centralized policy-based routing and networking to adapt to evolving APTs, requirements, and security mandates such as NIST and RMF across the Judiciary enterprise
- Enhanced cyber and network usage trend metrics
- More refined and accurate security policies and best practices for network, application, and system whitelisting