



APPLICATION FORM

All applications must include the following information. Separate applications must be submitted for each eligible program. **Deadline: June 1, 2018.** Please include this application form with electronic entry. If you do not receive an email confirming receipt of your entry within 3 days of submission, please contact [Gage Harter](#).

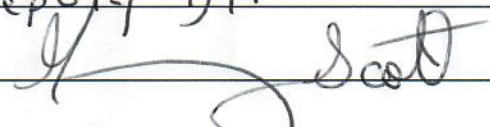
PROGRAM INFORMATION

County: Fairfax County, Virginia
Program Title: Next Generation Security Program
Program Category: Information Technology

CONTACT INFORMATION

Name: Michael T Dent
Title: Chief Information Security Officer
Department: Department of Information Technology
Telephone: 703-324-2755 Website: https://www.fairfaxcounty.gov
Email: michael.dent@fairfaxcounty.gov

SIGNATURE OF COUNTY ADMINISTRATOR OR DEPUTY/ASSISTANT COUNTY ADMINISTRATOR

Name: Gregory Scott
Title: Deputy Dir
Signature: 

Executive Summary

As a County Government servicing about 1.5 million citizens, we have the utmost responsibility to protect the well-being of citizens. Fairfax is also home to some Fortune 500 and large Government Contractors. We protect Businesses and Citizen's data with regards to taxes, sensitive personal information, businesses permits, land, Critical Infrastructure, Health and Human services and Public Safety. The Fairfax County Next Generation Security Program is part of the main Cyber Security program. Its mission is to Protect Citizen's data, develop and enforce Security policies and use technology that best protect data assets that will be on pace with modern and emerging security threats to maintain the County's no data breach, business continuity and service delivery performance record. The program follows a Security Defense-in-Depth architecture approach by deploying NextGen application aware security technologies to detect, block and alert threats where data moves both inside and outside the network.

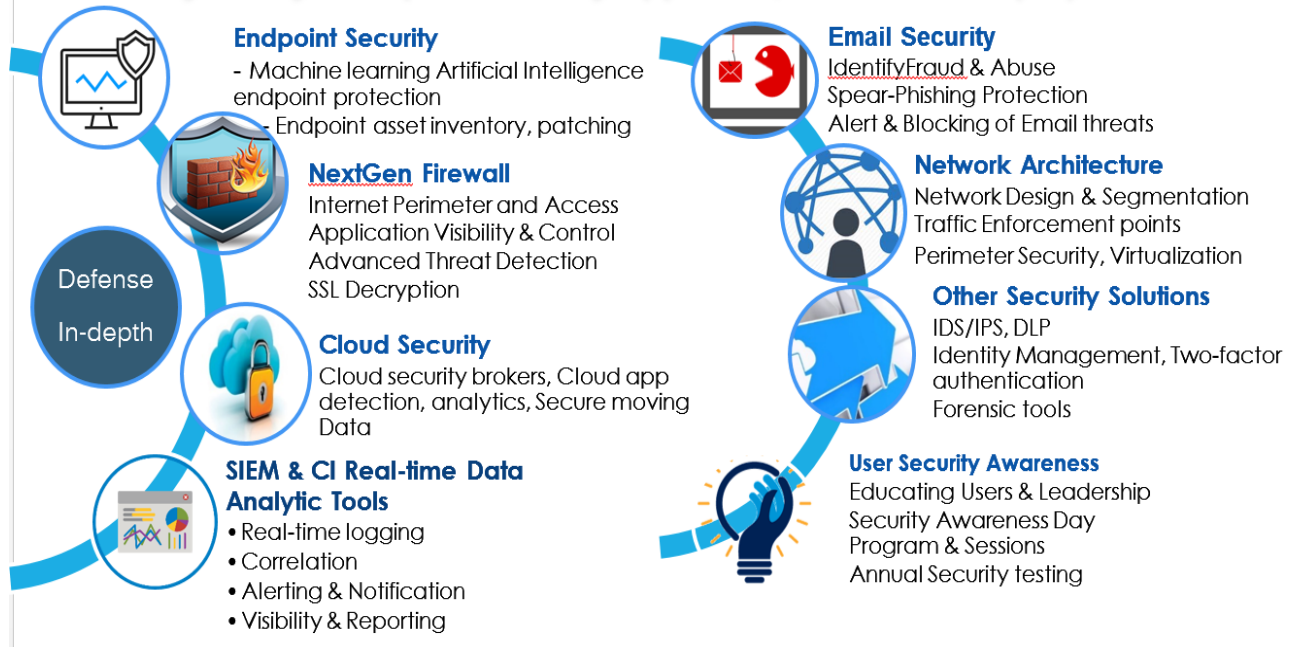
Program Overview

The Next Generation Security Program was developed to satisfy Fairfax County's Virtualization, Mobility, Cloud, IT Modernization, Internet of Things (IoT) and Security Posture initiatives. These initiatives have made securing every part of the IT Infrastructure extremely challenging. Technology is changing the way the County does business. The use of Social Media, Collaboration apps, Cloud-based apps and services are new ways to deliver critical services to Constituents and employees. The legacy security systems provided poor threat detection, poor application visibility, no SSL decryption, and scalability. In the past, Fairfax County had stringent access policies for majority of its user base and all Social Media and Cloud-based sites were

blocked. In addition to a growth in mobility needs, during the last 3 years ISO has seen a 131% increase in employees attempting to use of Cloud-based resources classified and a 170% increase in social networking applications. Enterprises today are also faced with modern threats and challenges. Malware, Ransomware, Spear Phishing, Spyware, BotNets, Internet of things (IoT), Mobile Device vulnerabilities and other application attack vectors are some of the threats Enterprises need to protect against. Data is now always on the move with the heavy use of mobile devices and hybrid on-premise and Cloud services. Numerous security zones need to be protected and monitored as the Network Architecture implemented under this project was architected to segment Internet bound traffic, public facing applications, remote access, partner access, IoT access and critical public safety services. Initial focus was to make sure the Network Architecture satisfies the placement of the different security solutions to cover exit points, flow of traffic and security zones.

Implementing these NextGen Security solutions at every layer of the Enterprise is key to detect and proactively react to modern security threats. Careful planning, evaluation of solutions, proper design and implementation were exercised during program.

Security Ecosystem (Our Security Approach, Defense In-depth)



Network Architecture:

The Information Security and Network Engineering team initially focused on designing and implementing a Network Architecture that is able to satisfy logical segmentation of security zones most importantly for Virtual Server computing environments, segmentation of Business units (E-Commerce, Partner Access, Remote Access, Public Access, Wireless Access, Public Safety, etc.), IoT environments, PCI, HIPAA, and Public Safety environments. Network technologies such as MPLS, Optical DWDM, Data Center Switch Virtualization and Dynamic routing protocols were utilized then the proper NextGen Security solutions and technologies were overlaid to cover traffic exit points, borders and traffic flow.

Next Generation Security Solutions:

The following technologies and solutions were successfully implemented:

- NextGen Firewalls for Internet Perimeter
- Machine learning Artificial Intelligence Endpoint Security
- Data Leakage Protection
- Cloud Security
- Email Security
- Two-factor Authentication
- Security Information and Events Management (SIEM)

Traditional Stateful Firewalls were replaced by Next Generation Firewalls at the Internet perimeter. The NextGen Firewalls provide SSL decryption, application visibility, application control, threat intelligence and the ability to adapt to new threats.

Traditional Antivirus and endpoint protection is not effective anymore outside of known signatures and heuristics. Machine learning Artificial Intelligence based Endpoint Security is now deployed to prevent malware, advanced persistent threats and malicious code from executing on endpoints in real-time before they execute. Zero-day attacks are highly prevented at the endpoint level in case threats were able to circumvent Security measures from the perimeter firewall and network security level.

Remote and portal access are secured with two-factor authentication. Data on the move and the protection of PII and other sensitive data are being handled by Data Leakage Protection, Cloud Security brokers and Mobile Device Management systems.

Email is the number threat vector used by Cyber Criminals. Majority of Security incidents originates from Phishing, Malware, Malicious, Ransomware and SPAM executed by the user community. An Email Trust platform was deployed which effectively stops phishing by

identifying the true sender of emails. This was integrated with Secure Email Gateways that serves as email delivery platforms on-premise and to the Cloud.

A SIEM system was also implemented to ingest logs and events from all security and major infrastructure systems for correlation, real-time notification and proactive response to critical security events.

Security Information and Events Management (SIEM)

A new SIEM system capable of ingesting analytical Big Data from a large number of Security devices, network devices, and critical server computing and application sources was implemented. The new SIEM data analytics provides real time health monitoring, Security threat detection, rapid Incident notification and response, Log collection and retention, Reporting, and better communications for the Security Operations team. It has elevated troubleshooting and mitigation efficiencies and has given better analysis tools for key IT departments, in addition to providing the IT Security team with the resources they need to proactively react to ever evolving threats to the Fairfax County network.

The Problem or Need for the Program

We now face an evolution of a new connected landscape. Everything is now connected. Smart Cities, Healthcare, Public Safety, Transportation, Critical Infrastructure, IoT, Security &

Surveillance, E-Commerce and Government to name a few. Users are becoming more mobile, Virtual Computing is rapidly being deployed, business complexity is growing, Cloud Computing use is expanding and now the threat landscape is evolving. Critical data is always on the move and it is the Fairfax Information Security Office's job to provide the necessary security controls and protection. Fairfax has seen a 131% increase in employees attempting to use internet resources classified as "online storage" (examples are Google Docs, DropBox, Box, OneDrive) and a 170% increase in social networking applications. Protecting systems and data that cross boundaries and perimeters is key to determine how fast Fairfax can move to a hybrid on-premise and cloud environment, how to provide better services to Citizens, how to prepare for compliance with current and pending data privacy regulations and how much business risk to take on. The need for a Security In-depth architecture and strategy is key to address these issues and is part of Fairfax's Next Generation Security program.

Cyber Threats

Connected Landscape

- Smart Cities
- Healthcare
- Public Safety
- Transportation
- Critical Infrastructure
- Security & Surveillance
- Consumer & Home



Start of Modern Cyber Attacks

- Sophisticated, Government Targets
- Malware, Spyware, BOINets, DDOS, Ransomware
- Email (Spam, Phishing, Spear Phishing)
- Public and Private sector breaches
- Application-based threats
- Identity thefts



New Threat Landscape

- **Critical Infrastructure**
- CLOUD Computing
- Mobile Computing
- Internet of Things (IOT)
- Transportation, Healthcare, Smartcity, Retail, banking, industrial, etc...



How the Program Fulfilled Awards Criteria

The next generation security program provides a unique solution to a current problem faced by many Federal, State, and Local government entities. It recognizes the value of doing business and providing critical services with the new connected landscape and to protect against evolving Cyber Threats. The County has provided a platform for the next generation of business applications and employees provide fast, reliable and secure technology and services. Fairfax County is a large and prestigious County Government and is often looked to as a model County by other State and Local jurisdictions. CISO, Michael Dent, is very active in the Cyber Security Community and is an active participant of local and regional Security conferences as a speaker and as a member of panel discussions. Fairfax County's Cybersecurity program has been shared and emulated by other State and Local County Governments. A big part of the program is the Security Awareness Day which gives an opportunity for Fairfax employees, agencies, partners and other jurisdictions to attend sessions conducted by Security experts from Government, academia, and private industry to ensure their use of technology is safe and secure.

How Program Was Carried Out

The Information Security team is headed by CSO Michael Dent. He leads a 12 person team of Security Analysts, Security Engineers and Network Engineers. Initial focus was to make sure the Network Architecture satisfies the placement of the different layers of Security solutions to cover exit points, flow of traffic and security zones. The project started early 2014 and was a collaborative effort between the Information Security department and the Network Engineering department. Both teams initially focused on designing and implementing a Network Architecture that is able to satisfy logical segmentation of security zones most

importantly for Virtual Server computing environments, segmentation of Business units (E-Commerce, Partner Access, Remote Access, Public Access, Wireless Access, Public Safety, etc.), IoT environments, PCI, HIPAA, and Public Safety environments. Network technologies such as MPLS, Optical DWDM, Data Center Switch Virtualization and Dynamic routing protocols were utilized then the proper NextGen Security solutions and technologies were overlaid to cover traffic exit points, borders and traffic flow. The Information Security Office also maintains good relationships with key agencies to determine business needs and security requirements. The Security department reached out to the market leaders in the Security solutions industry and began proof of concept testing and evaluation. Once the technology solutions were selected, the team reached out to key agencies to participate in testing new security rules and policies. Another critical part was for the Information Security Department to work with key agencies to learn mission critical systems and applications to be able to develop Security Incident and Events correlation rules, policies, alerts and monitoring.

Funding for the Network Architecture project was partly from a 2012 Federal Stimulus for energy consolidation initiative and also from a Network Modernization project called I-NET (Institutional Network) allocated by the County. This resulted in drastic reduction of physical server hardware and high-end data center switches. The migration from paid carrier WAN circuits to County owned dark fiber and new Metro Area Network has saved tons of operational costs.

Below is the cost of the main Security technologies implemented in the Next Generation Security Program:

	Initial Cost	Implementation Cost	Additional Costs	Current Yearly Maintenance	TCO To Date
NextGen Firewalls	\$184,084.04	\$119,236.00	\$2,400.00	\$346,880.00	\$1,693,240.04
SIEM	\$393,843.33	0	0	\$393,843.33	\$1,181,529.99
Email Security	\$249,025.26	0	0	\$249,025.26	\$249,025.26
AI Endpoint Security	\$746,900.00	\$100,000.00	0	\$250,000.00	\$1,596,900.00

Program Results

The Business results and stats show that Security incidents have dropped dramatically and detection rates increased dramatically.

Business results generated were the following:

Increased Security threat detection rate and protection between 30-40% which proves that the new Security solutions in place are catching threats. Allowing secure access now to Cloud and Social Media apps have increased bandwidth consumption to a little over 60%, but gained the County to offer services via Social media and the use of cost saving Cloud services for some Departments. The County averages over 500 million firewall transactions per day with an average of approximately 30% dropped each day for unwanted or potentially malicious traffic. Average blocked internet websites classified as malware per month at 436,000. Blocked Malware at Email Gateway average of 3000+ per month. Prior to the Email Trust solution being put in place, we were seeing 2-4 large scale Phishing/Malicious email campaigns per month, with few so called "Spear Phishing"(targeted, low volume) emails scattered in. Since January

29, 2018, the new email trust system collected(quarantined) 390 email messages, all being either Phishing, malicious, SPAM or otherwise untrusted/unwanted emails. Endpoint Security threat detections average 31 per day.

Increased End-User and IT Staff Productivity: Prior to the solutions implemented in the program, the County had spent a lot of manual time chasing down security issues and reimaging machines. This cost not only reduced end user productivity, but also tied up internal IT and Security staff mitigating issues. With proactive solutions in place, it now frees up resources and provides peace of mind as it comes to security threats in the environment. Quantified benefits from the new Machine learning Artificial Intelligence Endpoint Security solution include cost avoidance due to preventive and real-time detection of incidents before they can cause harm, reduced endpoint reimaging and remediation costs, and IT and Security full-time equivalent (FTE) productivity. Benefits of \$7,699,000 versus costs of \$2,195,000 over three years.

Fast and efficient incident response and mitigation: The new SIEM's Enterprise Security Console gives real time view of many areas of concern, but also provides very important trending information on load and usage, if spikes appear in our averages (outside of normal seasonal activity such as tax season) it can give a glimpse as to if an attack or denial of service is starting to ramp up. It also provides as fast analysis on infected desktops so that they can be cleaned or re-imaged quickly to allow maintaining the health and security of computing operations. The new SIEM is now capable of ingesting all logs and events from all Security systems, Network devices, Servers and critical applications at high capacity message rates. With

its built-in correlation rules, some custom rules and extensive reporting capabilities, the SIEM now allows Fairfax to quickly respond to incidents and fix problematic systems.