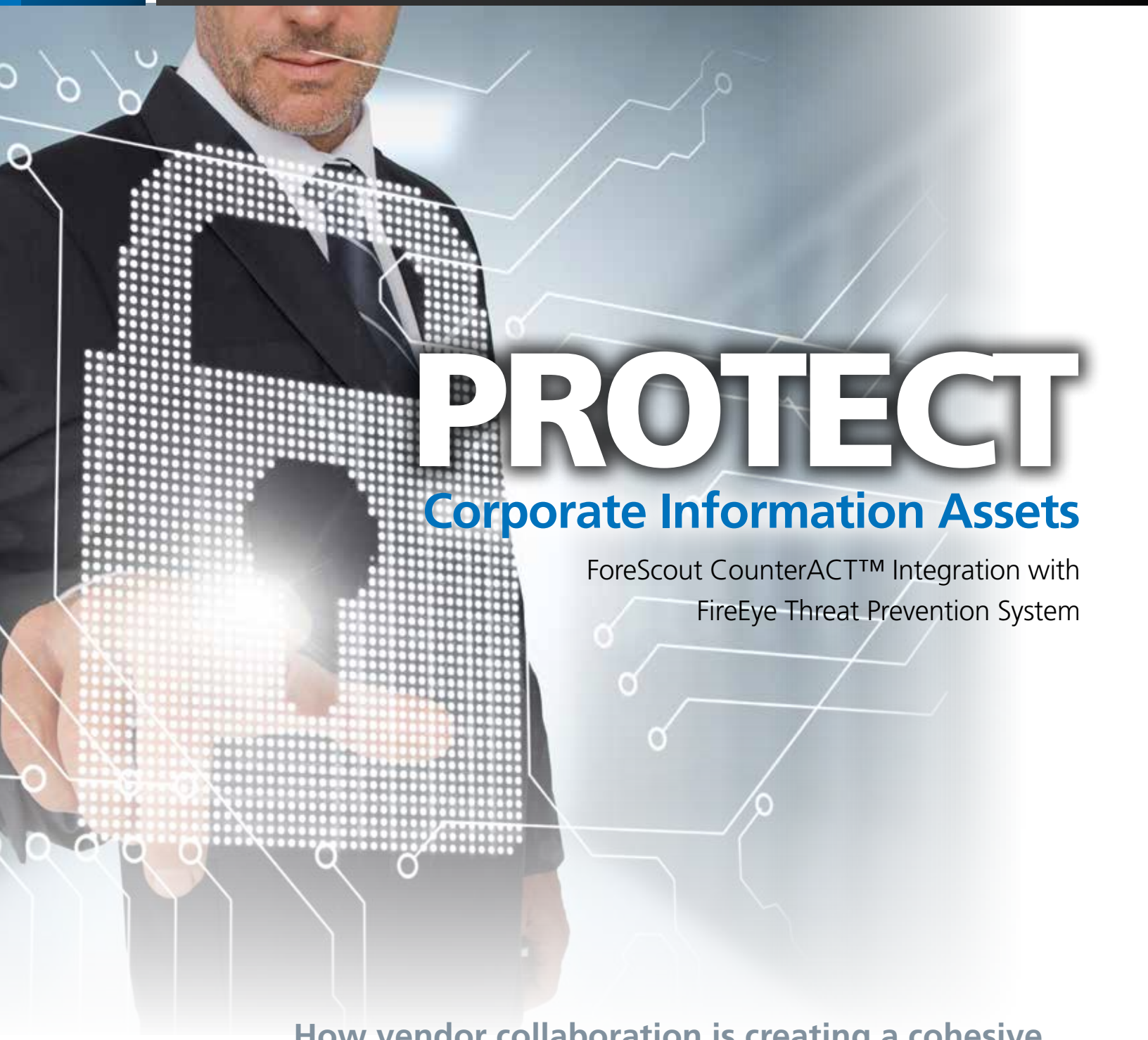
CONEXSYS
COMMUNICATIONS LIMITED



PROTECT
Corporate Information Assets

ForeScout CounterACT™ Integration with
FireEye Threat Prevention System

How vendor collaboration is creating a cohesive security ecosystem to address constant changes in today's enterprise networks.

Executive Summary

Today's enterprise security ecosystem bears absolutely no resemblance to that of even 10 years ago. Simple hacker attacks have given way to cyber criminals that are sophisticated, well-funded, and capable of causing major damage.

In almost every organization, enterprise network security is an amalgamation of devices, each geared to protect parts of the network from specific threats. Isolated security devices and systems are implemented as a result of new threats or direct hits, often driven by unsecured or uncontrolled devices attaching to the network.

To cover the entire attack continuum, organizations need solutions that can operate wherever threats exist: on the network, on endpoints, on mobile devices and in virtual environments.

There is a new approach to enterprise security that's emerging: that of vendor collaboration. Rather than perpetuate isolated silos of security solutions, vendors are working together to leverage each other's strengths and create better security solutions that are more robust, easier to manage, and more cost-effective for their customers.

Conexsys has more than three decades of implementing enterprise network and security solutions for both private and public organizations across Canada. Our value is providing the skills needed to integrate complex technologies within large enterprises for seamless transition and interoperability. We team with our OEM partners to create the optimum security ecosystem for each customer we work with, based on our experience in a wide variety of customer environments. We believe there is significant value in the collaborative efforts of security and networking vendors, as this approach will give our customers even more ways to properly protect their information assets.

In this briefing we'll discuss the first of many such vendor collaborations, involving Multi-Vector Virtual Execution(MVX) technology and Network Access Control technology.

ForeScout's unique ControlFabric™ Technology has allowed them to integrate a whole host of network and IT infrastructure devices, endpoints, and endpoint software into their CounterACT Network Access Control system, including FireEye's Threat Prevention Platform. We'll look at the business benefits of this collaborative approach, followed by an overview of the integrated solution.

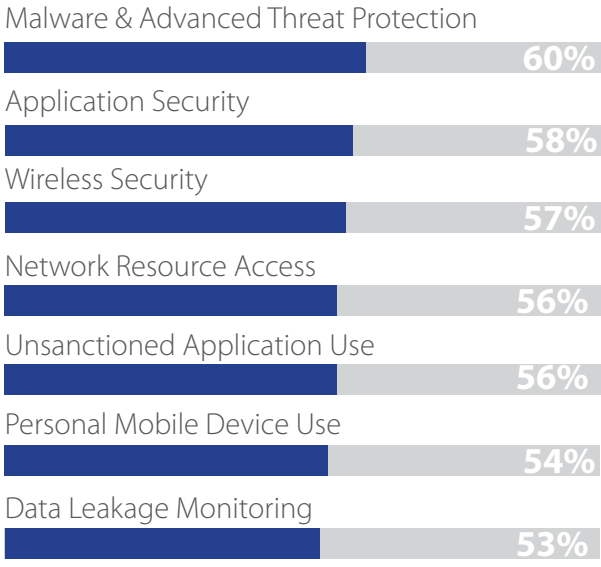
Today's Enterprise Network Challenges

In almost every organization, enterprise network security consists of unconnected standalone solutions, implemented in response to new threats, or to requirements such as BYOD (bring your own device). With the speed of technology development – and of new security threats – it becomes almost impossible to plan and create a cohesive security ecosystem that can handle current requirements and threats, while predicting future needs.

While businesses are implementing security measures as fast as they can, many haven't been able to control security to the extent they feel is necessary, mostly because of budget restrictions and the sheer workload involved. To maintain effective enterprise protection and threat mitigation in today's networks, there are three critical imperatives:

- **Knowing who's connected to your network**
  Managing security risk starts with a complete understanding of who and what is on your network, including whether these devices comply with security standards and policies. This becomes particularly important in today's BYOD environment, where employees are attaching unauthorized – and unsecured – personal devices to the network.

- **Knowing what threats exist on your network**
  Many of today's sophisticated cyber attacks easily evade traditional security defenses such as firewalls, intrusion protection systems, secure Web and email gateways, and anti-virus platforms. And with more endpoints on the network (employee personal phones and tablets, for instance), there are more opportunities for cyber criminals to find and exploit vulnerabilities.



Top Seven Areas of Security Violations
IDGConnect, ForeScout Technologies - State of IT Cyber Defense Maturity Report, July 2014

- **Better utilization of resources**
  One of the biggest challenges is the lack of resources to monitor and manage the expanding network. Much of the work required to monitor, install, reconfigure and reactivate security agents on the network may be manual, which can over-tax resources, extending the timeline to respond to threats and putting the network at risk.

Building a Cohesive Security Ecosystem

The net result of the last decade of increasing network security threats is a security environment that likely has vulnerabilities, and an IT staff that doesn't have enough resources or funding to provide airtight security. This forces organizations to continue to react to threats and vulnerabilities as they occur, instead of managing and mitigating security threats in advance.

Progressive network security vendors recognize the issues that many organizations are facing, and have begun to collaborate to create cohesive, cost-effective solutions to protect the enterprise security ecosystem. They're looking at how their solutions can interoperate, allowing for better security, with more efficient management – without requiring wholesale replacement of existing enterprise security measures.

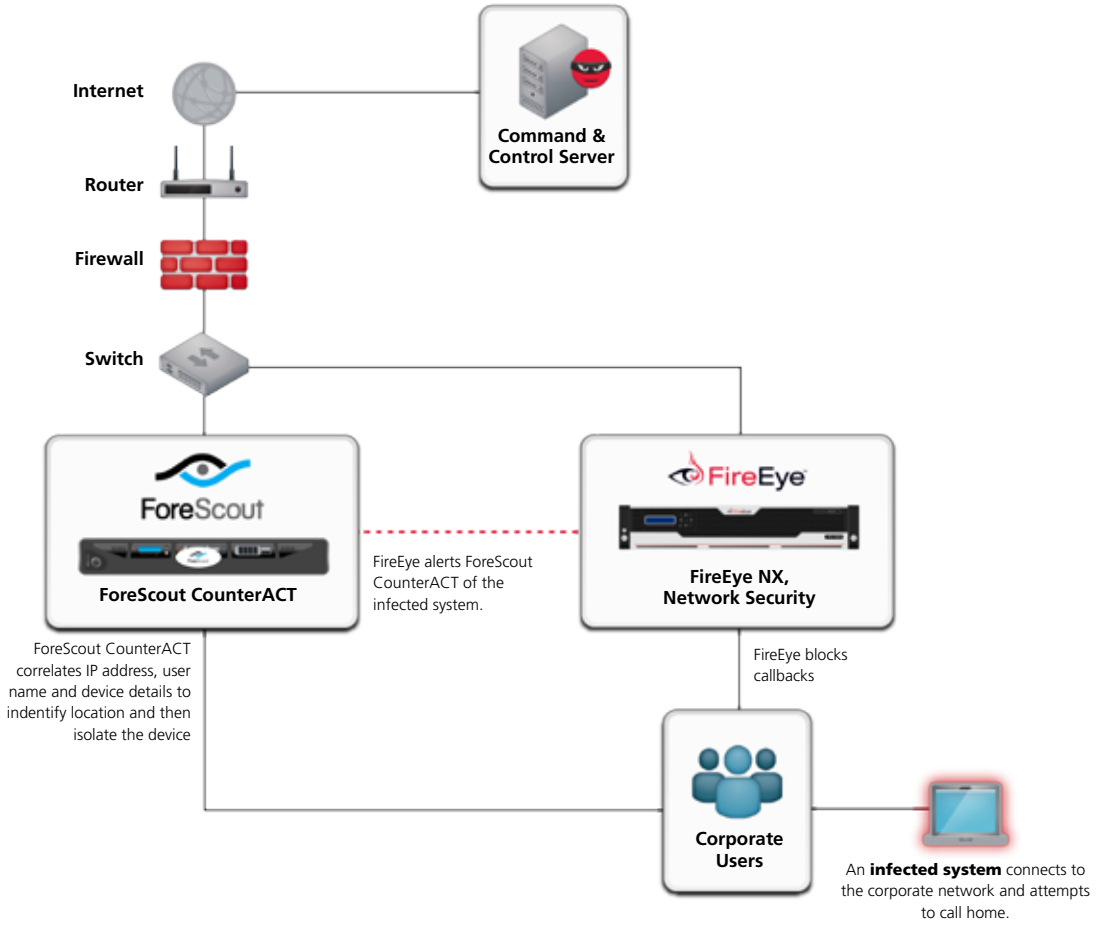
ForeScout and FireEye are leaders in this area, and are collaborating with leading security solution vendors to create cohesiveness in protection systems.

ForeScout CounterACT + FireEye Network Threat Prevention Platform

Using ForeScout ControlFabric platform, FireEye's Network Threat Prevention Platform (FireEye NX) is integrated with ForeScout CounterACT Network Access Control to deliver a unique and powerful solution for real-time monitoring and mitigation of enterprise risk associated with non-compliant and/or compromised endpoints. With this collaborative solution, you can identify, verify and quarantine a variety of serious threats in distributed environments, **reducing breaches, data loss and reputation risk while pre-empting costly investigation and remediation tasks.**

CounterACT is a real-time security platform that delivers visibility and automated control for devices, users, systems and applications connected to the network: wired or wireless, managed or unmanaged, PC or mobile. CounterACT integrates with the network infrastructure - Local Area Network (LAN), Wireless LAN (WLAN) and Virtual Private Network (VPN) - and enforces network access control policies for devices.

The FireEye NX Series stops Web-based attacks that are missed by traditional and next-generation firewalls, intrusion prevention systems (IPS), anti-virus (AV), and web gateways, and protects against zero-day web exploits and multi-vector callbacks, to keep sensitive data and systems safe.



Continuous Monitoring and Mitigation of Sophisticated Enterprise Threats

Operating together, ForeScout CounterACT and FireEye NX provide real-time visibility and compliance management of devices connected to your network, effective response to a variety of threats, and automation to efficiently and accurately mitigate threats.

When it suspects a system has been compromised, FireEye sends the internet protocol (IP) address to CounterACT, which will then take whatever actions have been pre-programmed into its policy manager, such as:

- Quarantine the endpoint using a defined method.
- Send endpoint configuration and security posture details to a Security Information and Event Management (SIEM) system, and notify ticketing systems and SIEM of policy violations and actions taken. Information can include the name of the logged on user, missing patches, antivirus status, running processes, applications installed, external devices connected, location of the endpoint, IP address and device type.
- Trigger a third-party system to initiate a vulnerability assessment scan.
- Trigger a third party endpoint remediation system.
- Notify the end-user and/or administrator via email or text message.

Working together, these solutions help create a cohesive security ecosystem:

Fast response to security breaches: FireEye NX determines that an endpoint may have been compromised, and will prevent data loss while notifying CounterACT to quarantine the endpoint and initiate remediation actions.

Real-time visibility: all devices are visible on your network, including unauthorized devices, BYOD devices, those with configuration violations and devices that have been breached.

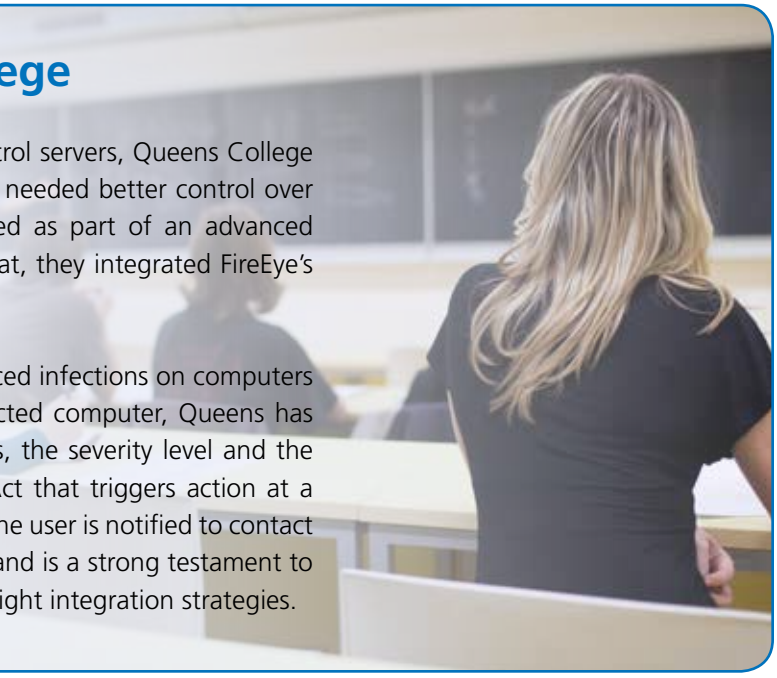
Reduced enterprise risk: endpoints have complete, updated and active defenses according to your policies.

Network access control (NAC) support: When FireEye discovers an endpoint is infected; ForeScout can automatically apply a range of techniques to quarantine the endpoint and mitigate the possible damage. ForeScout can use port blocking, access control lists, virtual LANs, and its patented virtual firewall technology to quarantine infected endpoints, and keep infections from spreading. The combined solutions can help enforce policies through device fingerprinting.

Discover and bock APTs and malware: Stop Advanced Persistent Threats (APT's) and malware, regardless of whether they are incoming, propagating or actively exfiltrating data.

Create context aware automation: upon detection, pre-defined policies are applied to automatically remove or isolate non-compliant or compromised devices from the network.

Reducing Risk at Queens College



With endpoints communicating to command and control servers, Queens College - a senior college of the City University of New York - needed better control over endpoint security to catch outliers that could be used as part of an advanced hacker's chain of attacks against the college. To do that, they integrated FireEye's patented MVX engine with their CounterACT NAC.

FireEye offers Queens more detailed flagging of advanced infections on computers than previously available. When FireEye spots an infected computer, Queens has it send a message to CounterACT with the IP address, the severity level and the infection name. They developed a policy in CounterAct that triggers action at a certain severity level so that the PC is quarantined and the user is notified to contact IT. The process has reduced risks security even further and is a strong testament to how a multi-vendor approach can work well with the right integration strategies.

ABOUT FORESCOUT

ForeScout delivers pervasive network security by allowing organizations to continuously monitor and mitigate security exposures and cyber attacks. The company's CounterACT appliance dynamically identifies and assesses network users, endpoints and applications to provide visibility, intelligence and policy-based mitigation of security issues. ForeScout's open ControlFabric technology allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout's solutions are easy to deploy, unobtrusive, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorized partners worldwide. Learn more at www.forescout.com.

ABOUT FIREEYE

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 2,200 customers across more than 60 countries, including over 130 of the Fortune 500. Learn more at www.fireeye.com.

ABOUT CONEXSYS COMMUNICATIONS

Conexsys is a leading IT solutions provider, serving business and government across Canada. With more than three decades of implementing enterprise network and security solutions, our certified professionals complete your implementation on time, on budget, and with the quality our customers have come to expect from Conexsys. Our value proposition includes local customer support, leading-edge technology, and quick, straightforward responses. As a result, our loyal and repeat customers identify Conexsys as the integrator of choice. Learn more at www.conexsys.net.

6715 Millcreek Drive, Unit 5, Mississauga, Ontario L5N 5V2
1-888-509-8452
www.conexsys.net

CONEXSYS COMMUNICATIONS LIMITED
IT Solutions To Enhance & Secure Your Business