FireEye®
SECURITY REIMAGINED

FireEye Network Threat Prevention Platform (NX Series) and Tenable® Network Security

Continuous Monitoring of Threats and Vulnerabilities

SOLUTION BRIEF

SECURITY
REIMAGINED

INTEGRATED SOLUTION HIGHLIGHTS

- **Improve security** by identifying advanced malware along with critical vulnerabilities.
- **Expand visibility** by detecting unprotected, compromised, and vulnerable endpoints.
- **Prioritize response efforts** by identifying the most critical risk.
- **Strengthen existing security defenses** by identifying deployment weaknesses and misconfigurations.
- **Meet compliance requirements** with endpoint and network context and assessment.

OVERVIEW

Today's IT landscape of mobile users, virtual machines, and cloud-based applications offers efficiencies, cost savings, and a dynamic, agile infrastructure.

Securing the new IT environment, however, requires a variety of security and compliance management solutions. These are often individually deployed and separately managed by different parts of the business.

The dynamic nature of the new IT landscape requires a continuous process of monitoring for advanced threats as well as identifying what's vulnerable, misconfigured, and non-compliant.

THE CHALLENGE

Effectively managing vulnerabilities, exploits, and breaches on modern networks is a difficult task as organizations face challenges in the following areas:

tenable®
network security

- **Visibility:** Lack of centralized and continuous visibility into unprotected, vulnerable, and compromised devices connecting to the network.
- **Context:** Inability to identify advanced malware threats and relate them to critical vulnerabilities in the network.
- **Priority:** Inability to prioritize the most critical risks and determine how best to remediate in a timely fashion.
- **Strength:** Ensuring that security defenses, network infrastructure, and endpoints are correctly configured and hardened to prevent compromise.

THE INTEGRATED SOLUTION

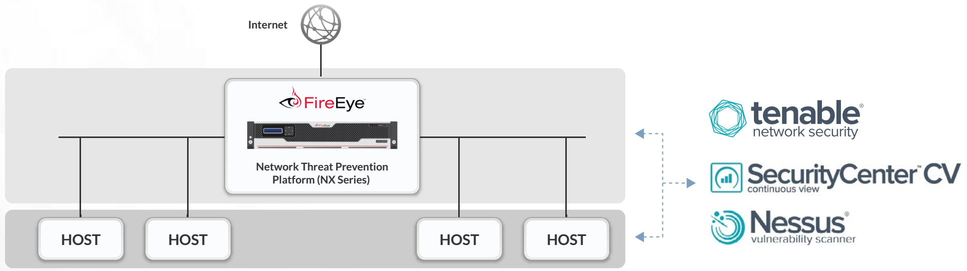
By deploying a FireEye Network Threat Prevention Platform (NX Series) solution with Tenable solutions, customers not only identify advanced malware but they also prioritize critical vulnerabilities and proactively remediate unprotected systems.

The FireEye Network Threat Prevention Platform (NX Series) solution identifies advanced threats using the signature-less FireEye Multi-vector Virtual Execution (MVX) engine to block web exploits and outbound multi-protocol callbacks. It pinpoints threats not detected by legacy security solutions including signature-based anti-virus and network intrusion detection systems.

Tenable solutions supplement FireEye threat inspection with continuous endpoint visibility and vulnerability, configuration, and compliance assessments.

Tenable Nessus scans networks and endpoints to identify vulnerabilities on systems targeted by advanced malware. It also audits endpoints, network infrastructure, and security defenses for misconfigured and unpatched systems that provide attackers an easy entry into your network.

Tenable SecurityCenter Continuous View (CV) adds network traffic profiling and event analysis to Nessus scans, enabling organizations to supplement FireEye Network Threat Prevention Platform (NX Series) inspection with continuous endpoint visibility and vulnerability and compliance


Internet
FireEye
Network Threat Prevention Platform (NX Series)
HOST
HOST
HOST
HOST
tenable network security
SecurityCenter CV continuous view
Nessus vulnerability scanner

FIREEYE PRODUCT AND VERSION

FireEye Network Threat Prevention Platform (NX Series)

TENEBLE PRODUCT AND VERSION

Tenable Nessus® (6.x)
Tenable SecurityCenter Continuous View™ (CV) (5.x)

assessments. It also collects FireEye events to summarize threat information, compromised hosts, and vulnerabilities via dashboards.

HOW THE JOINT SOLUTION WORKS TOGETHER

When FireEye platforms and Tenable Nessus or SecurityCenter CV solutions deploy together, they provide better visibility of security, compliance, and incident response effectiveness.

FireEye Network Threat Prevention Platform (NX Series) is deployed at the perimeter or key points inside the network to monitor for suspicious traffic.

Nessus scans endpoints and network infrastructure periodically to identify vulnerabilities on hosts and network infrastructure, ensuring host protection by FireEye. Nessus also checks for malware detected by the FireEye Network Threat Prevention Platform (NX Series) by looking for malicious patterns on endpoints. This detection helps verify a compromise has occurred enabling prioritized remediation.

Nessus audits the FireEye platforms to ensure that best-practice standards harden them in areas such as identification and authentication, appliance management, Intelligent Platform Management Interface (IPMI), encrypted communications, and malware detection system configuration.

SecurityCenter CV continuously monitors traffic to identify new hosts and associated vulnerabilities between scans. Organizations with FireEye Network Threat Prevention Platform (NX Series) can use this information to identify unprotected hosts or compromised hosts that connect inside their network.

Nessus aggregates events from FireEye to centralize threat indicators including infections, malware objects, and malware callbacks. This aggregation provides a centralized way to view FireEye detected threats and Tenable vulnerability scans.

SecurityCenter CV performs trending and event analysis so that as vulnerable systems are patched or remediated, organizations can gain visibility into their rate of remediation and response.

THE VALUE OF THIS PARTNERSHIP

FireEye and Tenable have collaborated to supplement each partner's solutions strength and to provide a comprehensive network security threat protection environment. The joint deployment of FireEye and Tenable continuously monitors both networks and endpoints to identify and detect advanced malware, identify vulnerabilities and misconfigurations, and ensure compliance with corporate and industry requirements.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. The FireEye Global Defense Community includes 3,700 customers across 67 countries, including 675 of the Forbes Global 2000.

ABOUT TENABLE

Tenable® Network Security provides continuous network monitoring that identifies vulnerabilities, reduces risk, and ensures compliance. The Tenable family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is trusted by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, please visit tenable.com.

For more information contact CSC@fireeye.com.