



Powerful Cybersecurity for Network Forensics from FireEye and Quantum StorNext

Combine “Flight Data Recorder” for your Network with High-speed Scale-out Storage

Cybercriminals are getting more sophisticated—and no industry is immune. Everyone is vulnerable, from banks to retailers, higher education to healthcare, government agencies to critical infrastructure. In addition to taking steps to prevent cyber attacks, organizations today need to prepare for the inevitable cyber intrusion, to be ready to respond to, and recover from, an incident...because there is no such thing as perfect security.

Hacktivists, state-sponsored threat actors, and financially motivated cybercriminals share a common trait: they are determined—and they will find a way in. When an intrusion is discovered, organizations need to investigate and quickly answer difficult questions, such as: How did the malware get in? How long has it been there? Is it a real threat? Has private or confidential data been exfiltrated? Is the attack over? To answer these questions, analysts need network forensics.

LOOK BACK IN TIME TO SEE HOW MALICIOUS CODE BEHAVED ON THE NETWORK

Network forensics is the practice of examining detailed network traffic data to figure out what was transferred across the network, from where to where, and when. It's similar to looking at a phone bill to interpret the pattern and flow of conversations: to see who's been talking to whom, how often, at what time of day, and for how long—except it's better, because network forensics can also shed light on what was discussed. Network forensics enables companies to look back in time to see how malware behaved on the network, so they can stop the attack, repair the damage, and strengthen cyber defenses for the future.

REDUCE TIME TO RESOLVE CYBER ATTACKS WITH NETWORK FORENSICS

Network forensics requires three things. First: an ultrafast mechanism to capture all the network traffic as it comes across. There is one chance to capture each packet and its associated metadata—miss the packet and it's gone—so the capture solution needs to be fast. Ultrafast. Second: a high-performance, scalable, reliable repository on which to store the network traffic; one that can keep up with ingest of 20Gbps per capture appliance. Third: efficient analytics to accelerate the path from detection to resolution, to answer questions in minutes that would otherwise take hours. Together, the FireEye Network Forensics Platform and Quantum StorNext® deliver this triple combo, and enable organizations to reduce the Mean-Time-To-Resolution for a cyber attack.



Security breaches are inevitable, because determined threat actors will always find a way through the gap.

- Mandiant M-Trends 2014
Beyond the Breach Report

THE FIREEYE NETWORK FORENSICS PLATFORM & QUANTUM STORNEXT

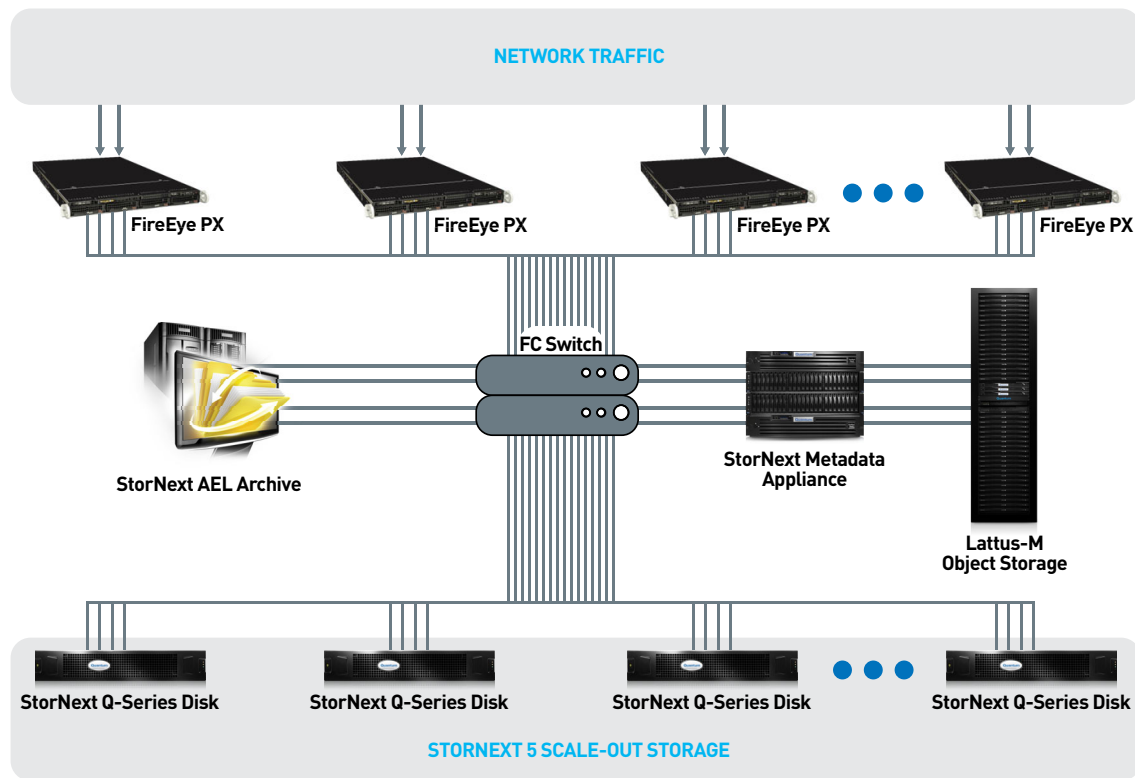
The FireEye and Quantum StorNext solution is ideal for customers who want to prepare for the inevitable cybersecurity incident, so they have the network traffic data they need for forensic analysis.

Effective network forensics requires products that capture traffic data at ultrafast speeds, for long periods of time, at scale. A single 10GbE bi-directional link generates up to 200TB of network traffic per day. FireEye and Quantum meet these demanding requirements.

FOR MORE INFO:

www.quantum.com/cybersecurity | scaleoutstorage@quantum.com
www.fireeye.com | info@fireeye.com

Quantum StorNext & FireEye Network Forensics Platform (PX) Architecture

**CAPTURE & COST-EFFECTIVELY STORE MONTHS OF NETWORK TRAFFIC DATA**

The 2014 Mandiant M-Trends *Beyond the Breach* report cited the median number of days before detection of a compromise as 229 days in 2013—yes, that's 229 days. Hence, best practices are changing. Rather than keeping days or weeks of traffic data, organizations now realize they need to preserve months of network traffic. This makes StorNext Scale-out Storage an even better fit for this use case, because in addition to delivering the fastest streaming file system performance that can keep up with the FireEye Network Forensics Platform, StorNext includes a policy-driven tiered archive. This enables customers to match the cost of the storage to the access needs of the data. Policy-driven tiered storage allows customers to store more network traffic within the same storage budget.

COMBINE ULTRAFAST CAPTURE OF NETWORK TRAFFIC WITH PETASCALE STORAGE

Companies need to prepare for today's new breed of cyber attacks such as zero-day attacks, advanced persistent threats, and polymorphic threats that can continually change shape. Network forensics gives businesses and agencies valuable tools to investigate and resolve cyber incidents. Together, FireEye and Quantum StorNext provide a combination of ultrafast packet capture—along with cost-effective scale-out storage that has been proven in the most demanding information workflows for video, satellite, intelligence, genomics, and seismic data. Together, FireEye and Quantum StorNext deliver a powerful cybersecurity solution for network forensics—with the speed, scalability, and cost-effectiveness that organizations require.

FIREEYE NETWORK FORENSICS PLATFORM

The FireEye Network Forensics Platform allows you to identify and resolve security incidents faster. With the Network Forensics Platform, organizations can detect a broad array of security incidents, improve the quality of response, and precisely quantify the impact of each incident. With a packet indexing speed of up to 30 million packets per second, it significantly reduces incident response times even in the face of large-scale searches. The FireEye Network Forensics Platform accelerates actionable intelligence and facilitates rapid incident response.

STORNEXT 5 SCALE-OUT STORAGE

StorNext 5 Scale-out Storage is found in the most demanding information workflows in Government, Defense & Intelligence, Life Sciences, and Media & Entertainment—and is designed for applications that operate on large sets of large files, for organizations that need to capture, preserve, share, and process critical data.

ABOUT QUANTUM

Quantum is a leading expert in scale-out storage, archive and data protection, providing solutions for sharing, preserving and accessing digital assets over the entire data lifecycle. From small businesses to major enterprises, more than 100,000 customers have trusted Quantum to address their most demanding data workflow challenges. With Quantum, customers can "Be Certain" they have the end-to-end storage foundation to maximize the value of their data by making it accessible whenever and wherever needed, retaining it indefinitely and reducing total cost and complexity. See how at www.quantum.com/customerstories.

©2014 Quantum Corporation. All rights reserved. Quantum, the Quantum logo and StorNext are registered trademarks of Quantum Corporation and its affiliates in the United States and/or other countries. All other trademarks are the property of their respective owners.

Quantum
BE CERTAIN

www.quantum.com • 800-677-6268

SB00073A-v05 July 2014