FireEye
SECURITY REIMAGINED

FireEye helps City of Miramar boost security and manage costs

CUSTOMER STORY

SECURITY REIMAGINED

KEY COMPONENTS

- FireEye® Network Threat Prevention Platform (NX Series)
- FireEye® Multi-Vector Virtual Execution (MVX) architecture

Do more with less. That's the mantra of the City of Miramar, Florida, which, like most municipalities, must constantly balance the dueling demands of keeping taxes low and public services running smoothly.

Situated in the heart of South Florida's fast-growing business district, the city is responsible for protecting the data for the city's 122,000 residents and that of its employees and businesses.

For Vladislav Ryaboy, the city's information security officer, that tension means combatting a rising deluge of cyber attacks with a smaller staff. Even as malware was growing more frequent, sophisticated, and dangerous, Ryaboy has had to cut his budget. The old approach to security—assigning lots of people to the problem—was no longer feasible.

"It was very time intensive and employee intensive," said Ryaboy, describing his security procedures before enlisting FireEye. "It took up so much of our time that it became very unproductive. I was desperately looking to automate whatever layers of security we had in place.

PUTTING FIREEYE THROUGH THE PACES

The issue came to a head when Ryaboy spotted suspicious network activity but could not get to the bottom of the

COMPANY	City of Miramar
INDUSTRY	Municipal Government
DESCRIPTION	The City of Miramar, Florida, provides a variety of municipal services to a growing local population of over 122,000 residents.
CHALLENGES	• Keep critical systems safe from a growing complexity of cyber threats (APT, zero-day, etc.) and increased surface of attack vectors (BYOD, etc.) • Reduce labor-intensive processes • Minimize false positives • Integrate and automate existing security tools
SOLUTION	• FireEye Network Threat Prevention platform (NX Series) • FireEye Multi-Vector Virtual Execution (MVX) architecture
BENEFITS	• New and previously unknown malware detected and blocked • Near-zero false positives • Easy management • Integration with legacy security

MIRAMAR
BEAUTY AND PROGRESS
EST 1955

> "FireEye gives me a better vantage point — a perspective of the battlefield that I never had before. I can make better decisions."
>
> — **Vladislav Ryaboy,** Information Security Officer, City of Miramar

problem with his legacy signature-based security tools. His staff spent hours manually blocking suspicious connections.

"We were a sitting duck," Ryaboy said. His existing infrastructure left his team blind to a constant stream of attacks.

The city tested several IPS/IDS type of solutions, including Symantec, Palo Alto Networks, and Cisco—and found them all inadequate for the security challenge the city faced.

Ryaboy, who has a military background, closely watches federal spending to see where the smart money is investing its security budget. He noticed more and more deals going to FireEye, and decided to try the FireEye Network Threat Prevention Platform.

The city piloted a proof-of-concept trial. Installation took less than an hour, and almost immediately, the FireEye Network Threat Prevention Platform began providing valuable insight into what was going on in the network —no heavy adminstration required.

The city had planned to test the FireEye Network Threat Prevention Platform for 15 days; Ryaboy knew within the first 24 hours that the solution delivered on its promise. "I realized that I can't get any better bang for the buck," he said.

BETTER PROTECTION, LOWER COST

Used in-line, the FireEye Network Threat Prevention Platform provides the insight Miramar needs to stay ahead of advanced threats.

The platform monitors Web traffic, by far the most common threat vector used in malware attacks. The city is alerted to zero-day exploits and fast-morphing malware to keep sensitive data and systems safe. At the same time, the Network Threat Prevention Platform is capable of shutting down communications with malicious URLs used in targeted attacks.

Thanks to the FireEye Multi-Vector Virtual Execution (MVX) architecture, Miramar's security team can spot malware hidden in malicious images, PDFs, Flash, and ZIP/RAR/TNEF archives.

Easy-to-digest email alerts validate true threats and help guide Miramar's incident response. And a browser-based dashboard cuts through the clutter with clear, actionable information about malware activity.

"By every measure, the FireEye Network Threat Prevention Platform has exceeded the city's expectations," Ryaboy said. The platform requires little ongoing adminstration and does not waste the security team's time with false positives.

Instead of chasing down every ambiguous alert, Ryaboy can spend more time on long-term preparedness and nurturing his security staff. For the City of Miramar, that means better service at a lower cost.

"FireEye is one of my few "go-to" products when I start my day," Ryaboy said. "The business benefits are far reaching."

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**