

# Case Study – Providence College

- **Company** - Top private college with 5,000 students in Rhode Island
- **Challenge** – Implement a security solution that was:
  - Easy to deploy
  - Had little operational overhead
  - Eliminated the short-comings of signature-based technologies which can't stop advanced malware
- **Solution** - FireEye 4000 Series Web MPS
- **Benefits** - Immediate visibility into undetected malicious code, optimization of remediation processes, zero latency



“The inline installation of the FireEye Web MPS was a quantum leap forward for us. Not only will it detect and block a threat, it does so in a very elegant manner. The appliance immediately lets a user know why a Web page was not delivered.”

– Donald J. Schattle II, Information Security Officer, Providence College



# Case Study – Regional Utility

- **Company** – One of the nation’s largest US regional utility companies providing electric and natural gas to customers
- **Challenge** – Supplement their traditional security to:
  - Stop zero-day and targeted attacks
  - Optimize efficiency of security team
  - Maximize accuracy of detection and blocking
- **Solution** - FireEye 7000 Series Web MPS
- **Benefits** – Rapid deployment, centralized management of threat monitoring, highly detailed alert reporting



“One of the big attractions of the FireEye solution is that analysis is performed in a virtual execution engine to determine if a flagged piece of code actually is a threat. The detailed information that is generated allows us to pinpoint the optimal option for resolving an issue. It puts us in the position of knowing exactly how to react.”

– Information Security Supervisor, Regional Utility Company



# Case Study – National Lab

- **Company** – National lab tasked with advancing scientific discoveries across energy, the environment and national security
- **Challenge** – Increase effectiveness of security against emerging global cyber threats to protect IP
- **Solution** – FireEye 7000 Series Web MPS
- **Benefits** – Increased speed of threat detection and resolution, increased productivity and usability with high accuracy and low false positive rates, no network or security overhead



**“FireEye is stellar! We were able to clearly demonstrate what the FireEye appliance was doing for our response times and for our abilities to expediently remediate and protect the environment from advanced malware, zero-day and targeted APT attacks.”**

*– Laboratory Lead Analyst, Cyber Defense Team*



# Case Study – Global Manufacturer

- **Company** – \$13B+ global technology leader in diversified power management, specializing in electrical, hydraulic and mechanical power
- **Challenge** – Identify and implement a malware inspection, capture and control system to combat advanced malware
- **Solution** – FireEye 4000 and 7000 Web MPS, Central Management System and Malware Protection Cloud
- **Benefits** – ROI within 20 minutes, expedient detection and mitigation of advanced threats



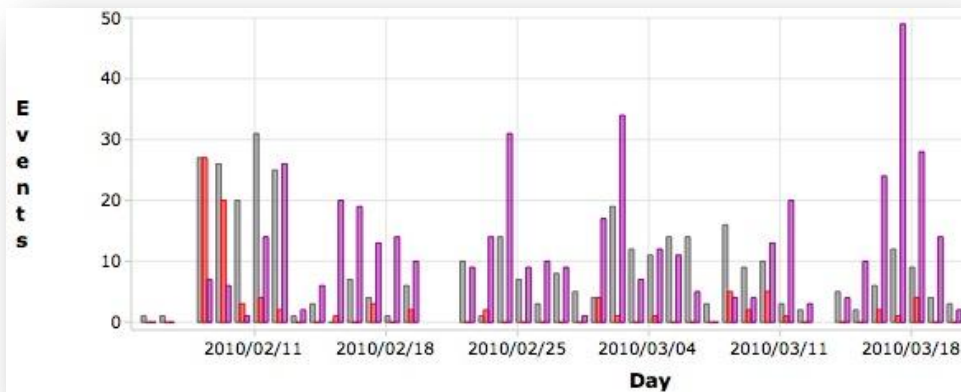
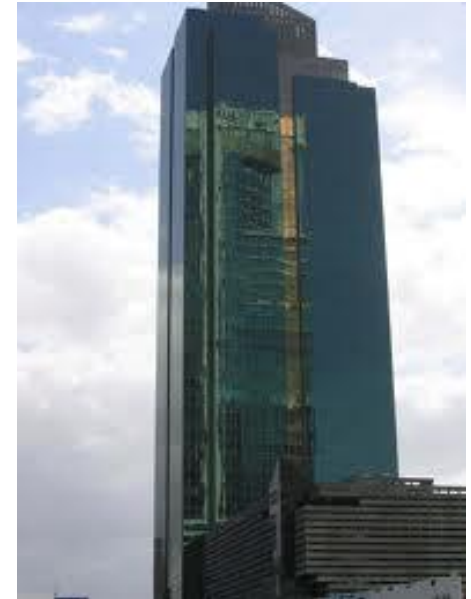
**“We experienced our first valid trapping of new malicious activity almost immediately. The appliance literally paid for itself inside the first 20 minutes!”**

*– Information Security Specialist, Global Manufacturer*



# Case Study - Global Financial Services Firm

- **Company** – Global Fortune 250 financial services firm in EMEA with over 80,000 employees; Multi-proxied arch with McAfee AV, Juniper FW, Bluecoat
- **Challenge** – Increase security and streamline arch.
  - 6 week evaluation period, found over 100 infected systems
  - Targeted, zero-day, social engineering attacks contributors
- **Solution** – FireEye Web MPS, replaced SourceFire IPS
- **Benefits** – Detected and cleaned all infected systems, blocking all future attacks, cost savings on IPS replacement



## MALWARE DETECTIONS:

- Inbound Zero-day malware
- Outbound Callbacks

