Creating a Security Conscious Environment with Compliance
Going Beyond Minimums With FireEye Endpoint Security

Toby Barber
Information Security Architect, UCSF

Jim Waggoner
Senior Director of PM, FireEye

Robert Kusters
Product Marketing, FireEye
$50,000 to $$Millions per Breach

$5,000 to $100,000 a month

€20 million or 4% annual revenue
Providing Regulatory Compliance and Protecting Users

Toby Barber – Information Security Architect

University of California San Francisco
advancing health worldwide
Toby Barber

23 Years protecting the enterprise & patient information

Silicon Valley → Stanford → UCSF

Passion for the fascinating challenges in cyber security
UCSF Background

- Public Education and Healthcare
  - University of California
  - 17 Campuses and Medical Centers
  - Combined both Campus and Medical Center computing
  - Merged patient care and research computing environments

- Award Winning
  - Top 10 Medical Center, U.S. News & World Report
  - “Most Wired” multiple times
UCSF Environment

- Academic freedom fuels research and patient care
- Creates an unusual cyber security challenge
  - Endpoints + medical, IoT, ICS and mobile devices
  - Users and servers
  - World-wide faculty and staff
  - Patient care focus with troves of PHI
    - Research data + patient health data
Our Experience

Visibility Gaps
ContinuousAttacks
HIPAACompliance
InvestigationTime
Our Challenges

External
- Compliance with Regulations
- Third party data use agreements
- Breach Notification Rules
- Students and Health Professionals
- Partner research institutions
- Clinical affiliates with the hospital
- Healthcare cost and reimbursement rates

Internal
- University Budget
- Staffing constraints
- Talent acquisition in the Bay Area
- Shifting from old educational mindset of all open networks
- Freedom of research focus creates a challenging acceptable use environment
- BYOD
- Funding silos for research projects
Our Need

- **Visibility**
  - All endpoints; clients, servers, on network or off

- **Understand**
  - Risk of data
  - Risk of systems

- **Comply with Regulation (HIPAA)**
  - Context on probability of compromise

- **Reduce**
  - Time spent performing forensics
  - Time of incident response
  - Impact to user
Our Goals

- Common view of system-wide security
  - Inform readiness
  - Allocate budget
  - Measure risk reduction strategies

- Single tool, manage & reduce cybersecurity risk

- Consistently spot bad actors
- Uniformly respond quickly to threats
- Ensure return on investment
- Mature incident response
- Reduce friction in response
  - User and cyber security team
Awareness Approach

- Pop-up security campaign
- Campaign: Plug Your Security Holes
  “It’s OK to have a hole in your donut, but not in your security!”
- Outreach drove action!
  “Between January 1, 2019, and April 10, 2019, there were 39,962 security software downloads, with only 1.9 % resulting in Service Desk tickets.”
Testing

- Started with Internet facing hosts
- Security and IT eat our own dog food
- Lots of client testing reducing perceived security agent overload
- Performance baselining
- Privacy, legal and risk discussions
- Identifying indicators obtained by the FireEye agent
Implementation

- Training IT teams
- Baseline reporting of incidents
- Pre-staging policies for issue
- Phased rollout, 40,000 endpoints
- Daily and Weekly stand ups
- Leadership reporting
- Pass through version upgrade cycle
What’s changed

Contact user
Physically collect system Triage
Perform forensics
Provide loaner machine

Automatic triage collection
Remote containment
User only interrupted after issue confirmation

Machines would “build up” waiting for security analysis

Investigation speed translates to team availability

Multi-system issues would remove security staff from other duties

Automation opportunities
Our Current State

- Lowered network detection tickets by 50%
- Improving Four-Factor Breach Risk Assessment as required by HIPAA
- Moving into high performance computing and IaaS workloads
- Maturing analysis and playbooks
- Leveraging MITRE ATT&CK for validation and threat intel
Next Steps and Lessons Learned

Next Steps
- FireEye Orchestrator
- New Linux support
- Helix workflow for endpoint investigations
- Develop and test cloud workload protection

What We Learned
- Awareness works
- EDR is a key capability
- Integration saves time and improves efficacy
- Talent issues can be partially addressed with technology
Endpoint Security
The FireEye Ecosystem
How We Do It

Protect Against Threats
- Malware Protection
- MalwareGuard
- ExploitGuard
- Platform Interaction

Detect the Breaches
- Event Recording
- Indicators of Compromise
- Enterprise Search
- Investigative Data Acquisition

Respond to Incidents
- Auto Remediation
- Containment
- On/off network
- Respond at scale
Industry Validation - Protection

99.6% SE Labs Forthcoming

99.1% VirusTotal 100% Certified

Ultra Low False Rate

Test Yourself
Investigations and Response

Acquisitions
On the box inspection
- Activity that is too expensive to stream
- All registry changes
- All new files

Streams
Off the box inspection
- Metadata that can be stored for months
Introduction to Modules

- Future of agent innovation
- Scales for in-field, on-demand features
- Primary driver: Consultant driven features for current engagements
- Customer benefit: Field tested features proven to find threat actors
Module Examples

- Identifying new potential risky processes
- Identify new or unexpected credentials
- Blocking credential dumping
- Provide intelligence context for all alerts

Investigative Modules used by Mandiant
- Installed and recently run applications
- Recently access application files and actions (like RDP)
- Parse Windows shortcut files
- Parse shellbags from reg hive for evidence of folders accessed on local machine
- Identify GUI program execution
- Identify WMI persistence items and convert data storage
Modules in Action

Select a module to load into FireEye Endpoint Security

Modules work across all deployment environments

Enable by policy per host set or across your console
Expansive Linux Detection

- **Support** on major Linux distributions
- **Real time alerting** on active threats
- **Streaming** of data for investigations
- **Enrichment** of suspicious files
- **MVX submissions** on Linux binaries
- **Acquisitions** on data sets
Endpoint Security – What’s Next

Innovation Architecture

Protection, Detection, Response

Endpoint Protection Suite

Simplified Management

Platform Coverage

Evergreen
Let’s Wrap This Up
FireEye Helix, A Contextualized View

Integrates disparate security tools and augments them with next generation SIEM, orchestration, and threat intelligence capabilities.

Workflow and Case Management  
Contextual Intelligence  
Compliance Reporting

“Holistic approach that enhances our overall security ecosystem and makes it easy to show security compliance”
Managed Defense, A Force Multiplier

FireEye Managed Defense for Endpoint is an endpoint detection and response service that provides 24 x 7 protection against threats, combining front line experience with industry leading technology and intelligence.

Analyst Driven Detection + Threat Focused Defense = Answers, not Alerts

“A level of coverage and visibility that organizations could not duplicate by other means”
Expertise on Demand, A Team Amplification

An annual subscription that extends the capabilities of security teams with services and threat intelligence expertise including intelligence, investigation and training.

“Cyber security programs perform at their top potential when expertise works seamlessly with technologies and processes.”
Expertise on Demand in Action
Call to Action

Visit the **Solution Showcase**

Thinking about Endpoint Security
- MITRE ATT&CK Reference
- Self-guided tour
- Try it for yourself

Current Customers
- Try a Module from the Market
- Become a Lighthouse Reference
- Provide a review, Gartner peer reviews booth
Thank you.
Insert headline here and

use medium for emphasis
What Customers Are Saying

“Lorem ipsum dolor sit amet, consectetur adipiscing elit. In cursus fermentum elit, nec porta ligula.”

— Name
Title, Company
Table Example

<table>
<thead>
<tr>
<th>COLUMN TITLE</th>
<th>COLUMN TITLE</th>
<th>COLUMN TITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Row text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Row text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Row text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Row text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Row text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Row text</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Insert text about solution

Insert supporting charts, diagrams or details about solution
Links to Other Presentation Assets

- Pictogram Library
- Icon Library
- Heroes
- Other Brand Resources
Icons Library

- FireEye Email Security
- FireEye Endpoint Security
- FireEye Network Security
- FireEye Helix
- FireEye Intelligence
- FireEye Mandiant
- FireEye Security Suite
- FireEye Cloud Security
- FireEye Managed Defense
- FireEye Expertise On-Demand
0.75in Icons Library

FireEye Email Security

FireEye Endpoint Security

FireEye Network Security

FireEye Helix

FireEye Intelligence

FireEye Mandiant

FireEye Security Suite

FireEye Cloud Security

FireEye Managed Defense

FireEye Expertise On-Demand