Let’s Get Right To The Endpoint

Leveraging Endpoint Data to Expose, Validate, Triage, and Remediate Security Breaches
Ultimate Goal of Security

Company Data: Epicenter of Risk

- Business Intelligence
- Intellectual Property
- Customer Data
- Cardholder and Financial Data
- Authentication Credentials
- Human Resources
- Electronic Health Records
What are Your Challenges?

- Securing company assets and data in an every changing world
- Understanding where company sensitive data resides
- Keeping up with the ever changing landscape of threats
- Increasing number of alerts
- Prioritizing and responding to alerts
- Controlling post-breach consulting costs
- Auditing against and enforcing sensitive data policies
- Being right 100% of the time…

Would it be valuable to have a view of what was occurring on potentially affected endpoints?
Unfortunately - Nothing Is Foolproof

- Locks on Doors and Windows
- Alarm System
- Video Surveillance System
- Signage, Fences, etc.
How Effective Is Your Security Posture?

Preventive measures are important, but…

Now What?
Malvertising Stays One Step Ahead

Borrowing targeting technology from the advertising industry, the bad guys are also customizing when — and to whom — they deliver malvertisement.

Of course, the bad guys have swiftly jumped ahead. The latest Web infections are designed to play possum when a search engine or antivirus Web crawler comes calling. Bad guys do this by employing a black list of their own, one that contains the known IP addresses of the good-guy crawlers.

And Time is of the Essence!

<table>
<thead>
<tr>
<th></th>
<th>Seconds</th>
<th>Minutes</th>
<th>Hours</th>
<th>Days</th>
<th>Weeks</th>
<th>Months</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Attack to Initial Compromise</td>
<td>10%</td>
<td>75%</td>
<td>12%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Initial Compromise to Data Exfiltration</td>
<td>8%</td>
<td>38%</td>
<td>14%</td>
<td>25%</td>
<td>8%</td>
<td>8%</td>
<td>0%</td>
</tr>
<tr>
<td>Initial Compromise to Discovery</td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
<td>13%</td>
<td>29%</td>
<td>54%+</td>
<td>2%</td>
</tr>
<tr>
<td>Discovery to Containment/Restoration</td>
<td>0%</td>
<td>1%</td>
<td>9%</td>
<td>32%</td>
<td>38%</td>
<td>17%</td>
<td>4%</td>
</tr>
</tbody>
</table>

*Source: 2012 Verizon DBIR

The attackers are here
While the responders are way over here
There Is Always The Human Element

Don’t Ignore the Warnings


Candid Wueest  SYMANTEC EMPLOYEE

Be honest. Do you really read the warning messages that your browser displays to you? Or do you blindly click the phishing site warnings or the SSL mismatch dialog away? Apparently most users don’t seem to care too much about those warnings and click through them quickly. And I doubt that they have memorized the meaning of the warnings and reflect on the consequences each time.

An interesting study from Google and Berkeley University analyzed 25.4 million warnings from the Google Chrome and Mozilla Firefox browsers. According to their research, on average, 15.1 percent of the users click through the warning for malware-infected sites. Interestingly enough, Mozilla Firefox users on Windows have a click-through rate of only 7.1 percent compared to Google Chrome users on Windows with a 23.5 percent click-through rate, about three times as click-happy.

For phishing site warnings, the average click-through rate is 20.4 percent. In this phishing category, Linux users, with 32.9 percent, click through the warnings a lot more often than the others. Maybe they are more tech-savvy and

“...it's apparent that we need to review our firewalls to ensure that basic configuration settings such as antispooing and anti-DDoS are enabled...”

EnCase... found something consistent with malware that was previously identified as opening connections to a server in Vietnam from multiple spoofed IP addresses... Running a companywide inventory, we found the same malware on some other overseas machines, and on some in our corporate office.”

“[T]he incident also makes clear that we need to address some inconsistencies in our endpoint protection compliance...”

SOURCE: http://www.computerworld.com/s/article/9240737/Security_Manager_s_Journal_Suddenly_our_firewall_audit_can_t_wait
Improving Your Security Response

Important Things To Consider
Faster Intelligence Gathering

Traditional Incident Response Timeline

- **Alert Received**
  - Undetermined amount of time passes

- **Day X**
  - User calls help desk due to computer malfunction

- **Day X+2**
  - Trouble ticket created and placed in queue

- **Day X+4**
  - Trouble ticket reviewed

- Tier-one security analyst sent on site to manually gather event data

---

*Guidance Software*
Key Requirements

- Broad Encryption support
- Broad OS support
- Ease, Speed and Flexibility of deployment and configuration
- Forensic-grade visibility
- Review capability
- Policy enforcement mechanism
Protecting Company Data Is Number One Goal!

Compliance
- HIPAA, PCI-DSS, Data breach notification laws, risk mitigation
- Intellectual Property handling policies
- Proliferation of laptops/tablets has increased risk of data loss

Eliminate risk of sensitive data in unauthorized locations

Prioritize incident response

Enable definitive policy enforcement
Help Is Available

For The “Now What?”
The EnCase Cybersecurity Solution

- Endpoint Incident Response
  - Mitigate the RISK of successful attacks through rapid validation, comprehensive scope assessment, and containment of security incidents
  - Reduce the TIME delay between compromise, detection and response
  - Reduce the COST and overhead of incident response leveraging existing people and technologies

- Endpoint Sensitive Data Discovery
  - Mitigate the RISK of sensitive data in unauthorized locations
  - Reduce the TIME it takes to locate sensitive data and enforce regulatory and policy compliance
  - Reduce the COST associated with data discovery processes that don’t easily scale and lack definitive enforcement
How EnCase Helps Mitigate the Risks of a Breach

• **System Integrity Assessments** – Expose unknowns and known bad via scheduled audits

• **Large scale volatile data analysis** – Discover system anomalies and similarities, expose attack artifacts

• **Near-match analysis** – expose iterations of morphed code and variations of detected threats

• **Deep forensic analysis** – completely and thoroughly investigate any anomaly or breach

• **Remediation** – immediate address risk by killing running process and wiping related disk artifacts

• **Integration with SIEM and alerting systems** – visibility into potentially affected hosts the moment an alert is generated
Automating Incident Response Data Collection

Incident Response Timeline **without** EnCase Cybersecurity Automated Response:

- **DAY X**: Attack Occurs
  - Undetermined amount of time passes

- **DAY X+2**: User calls help desk due to computer malfunction
  - Trouble ticket created and placed in queue

- **DAY X+4**: Trouble ticket reviewed
  - Tier-one security analyst sent on site to manually gather event data

- **DAY X+8**: Analysis performed on collected data

- **DAY X+14**: Manual forensic analysis performed on machine
  - Weeks to months
  - One Machine analyzed
  - Critical data lost
  - Full extent of breach unknown

---

**Minutes...**

- **With** EnCase Cybersecurity Automated Response:
  - Entire process takes minutes
  - All potentially affected machines analyzed
  - Critical data preserved
  - Full extent of breach realized

---

- SIEM invokes cyber-response
- Event validated, details captured
- Forensic analysis performed on all potentially affected machines
- Detailed web-based reports generated
Comprehensive visibility

- Covers multiple operating and file systems, including email and document repositories
- Kernel level scans – locates deleted, in use and otherwise hard to see data locations
- Analyze metadata to quickly determine origin and where else errant sensitive data may reside

Built in templates for PCI and PII data, configurable for other data formats (account numbers, electronic health records, IP, etc.)

Scheduling capability to keep you covered

Web-based review and tagging

Securely wipe non-compliant data
EnCase forensic capabilities will investigate how the malware compromised the endpoint(s).

What was the delivery mechanism (e.g., USB drive, web page, email, etc.).

What activity occurred before the compromise, during and after.

What type of data was possibly exposed or compromised.

Have we identified all of the compromised systems?
What About A Different Approach?
Challenges With Today’s Current Approach

- “Rule” based security is limited
- Knowledge of what to look for is required
- Endpoint visibility is lacking
- Historical trends are not considered
- Correlation of endpoint data points is overlooked or missing
- Time required to manually audit system configurations
- Overall, too much data to analyze
Not constrained by signatures, indicators, behaviors, or heuristics

Looking across all endpoints and servers, where threats ultimately hide

Providing multi-dimensional analysis of unstructured endpoint data

Exposing gaps in security posture
Allowing quick visualization of undetected risks or threats

- Exposing suspicious patterns, commonalities and anomalies
- Spotting unusual changes over time

Interactive interface allowing on-the-fly adjustments so you can zero in on the threat
Introducing EnCase Analytics

- Security insights via complete endpoint visibility
- Comprehensive view into security risks and threats
- Quickly derive insights from visual representations of data
- Expose unknown threats through statistical analysis of endpoint data
EnCase Analytics: Process Variant Anomalies

Process Names

- Process Name
- Current Count of Unique Hashes

- ntdsntdll.exe
- 3.000
- ntdkmdk.exe
- 1.789
- rundrv.exe
- 1.789
- conhost.exe
- 1.789
- aksfridge.sys
- 1.565
- dllhost.exe
- 1.500
- eps.sys
- 1.434
- updater.exe
- 1.434
- arnsvc.exe
- 1.414
- opui.exe
- 1.414
- Imagent.exe
- 1.414
- vnmat.exe
- 1.403
- vmnetdhcp.exe
- 1.403
- vms.exe
- 1.403
- acord32.exe
- 1.231
- nvidia.msi
- 1.228
- nvidia.sys
- 1.228
- nvdsync.exe
- 1.228
- googleupdate.exe
- 1.095
- lvuv64.sys
- 1.095
EnCase Analytics: Account Trends Over Time

Count of Machines by Account Name

Count of Machines

Apr 24  Apr 25  Apr 26  Apr 27  Apr 28  Apr 29  Apr 30  May 1

Date of Scan [2013]

admin-na-Meira.shellenbarger
Guidance Software, Inc. Overview

- World Leader in Computer Forensics, eDiscovery and Incident Response
  - Company Founded in 1997
  - Publicly Traded Company on NASDAQ (ticker symbol = GUID) Since 2006
  - 40,000 EnCase Customers World Wide
  - Over 1,500 EnCase Enterprise Customers
    - More than 65% of the Fortune 100
    - More than 40% of the Fortune 500
  - 300+ EnCase eDiscovery Customers, 200+ EnCase Cybersecurity Customers
  - 50,000 people trained on EnCase
Thank You

Mel Pless, Sr. Director, Solutions Consulting, Guidance Software
mel.pless@encase.com