Cybowall Solution Overview

CYBONET

EVOLVING SECURITY CHALLENGES

EXAMPLES OF CYBER BREACHES INCLUDING CARD DATA

2013: Adobe Systems

- Hackers raided an Adobe back-up server on which they found and published a 3.8GB file containing 152 million usernames and poorly-encrypted passwords, plus customers' credit card numbers
- 38 million users affected in total
- Adobe paid an undisclosed amount to settle customer claims and faced US $1.2 million in legal fees
- Ordered to pay USD $1 million fine to North Carolina and 14 other US states and implement new policies and practices to prevent future similar breaches

2014: Home Depot

- US hardware retail giant robbed of the payment card details of 40 million customers
- Settled a class action consumer lawsuit agreeing to pay USD $13 million in cash compensation (up to $10,000 per customer affected), spend USD $6.5 million on ID theft protection and adopt a series of measures to tighten its security

SMBs

Small/Medium-sized businesses (SMBs) – targeted by about 60% of cyber attacks

- 43% of global attacks targeted SMBs with fewer than 250 staff (9% increase on previous year)
- Ranking of attack types: 1). General computer hack 2). Theft of credit card information
- Over USD $32,000 average loss for SMBs whose business bank accounts were hit
- 42% of SMBs took more than 3 days to resolve a cyber attack issue

SMB CYBER BREACH CASE STUDIES

Maine Indoor Karting, US

- Targeted by a phishing scam
- The owner, Rick Snow, received an email that appeared to be from his bank, asking him to log in with his account information
- Mr. Snow realized he had fallen victim to a phishing scam, closed his business account and opened a new account
- Hacked again 2 weeks later and the attackers stole over USD $37,000 to clear out his business bank account

MNH Platinum, UK

- Victim of a virus which encrypted over 12,000 files on its company network
- A ransom demand followed; the criminals would decrypt the company's files in exchange for more than GBP £3,000
- The company paid the ransom as the virus proved impossible to remove without the loss of crucial company data

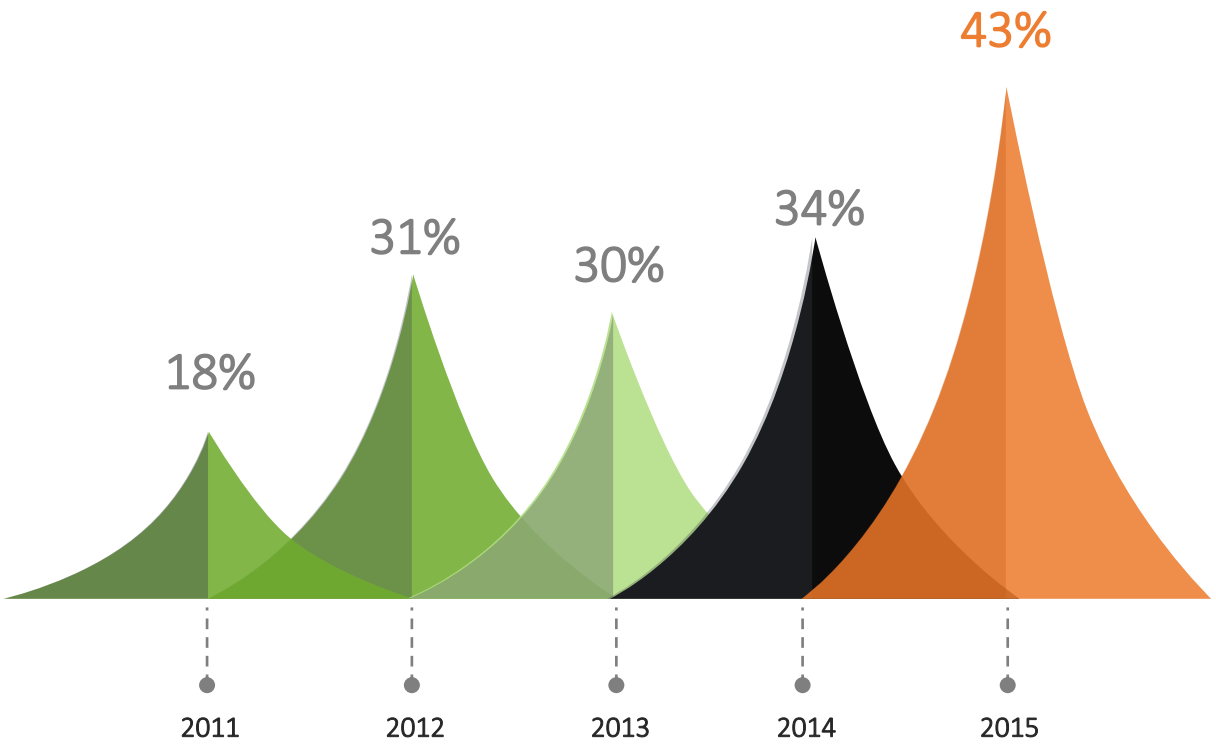
PCA Predict, UK

- Targeted by Russian hackers who sent out a spam email to 1.5 million people, claiming that GBP £120 had been charged to each person
- Customer service nightmare; company received overwhelming volume of calls and emails as people tried to get their money back
- As a technology company, PCA Predict was lucky that it could use its systems to respond quickly; recording a phone message explaining the issue and changing its homepage to a warning about the spam

SMB CYBER ATTACK STATISTICS

- Employee error and accidental email/internet exposure caused nearly 30% of all data breaches
- Ransomware attacks are on the rise and targeting not only employees but any devices connected to a company's hacked network
- 43% of information security attacks in 2015 targeted SMBs
- 60% of small businesses lose their business within 6 months of an attack

43% of Attacks target SMBs



Source: Symantec
More Charts: http://sbt.me/charts

SMB CYBERSECURITY CHALLENGES

RESOURCES & EXPERTISE

SMBs face the same threat with fewer resources and lack in-house expertise

RECOVERY FROM A CYBER ATTACK

33% of SMBs took 3 days to recover from an attack, and 60% of SMBs lose their business within 6 months of an attack

COST OF DATA BREACH

Recovery from a SMB data breach can cost between USD $36,000 - $50,000

GLOBAL ATTACK TARGET

43% of global attacks targeted SMBs with fewer than 250 staff (9% increase on previous year)

SPEAR PHISHING CAMPAIGNS

55% increase from previous year in number of spear phishing campaigns targeting all businesses

CYBER ATTACK RESPONSE PLAN

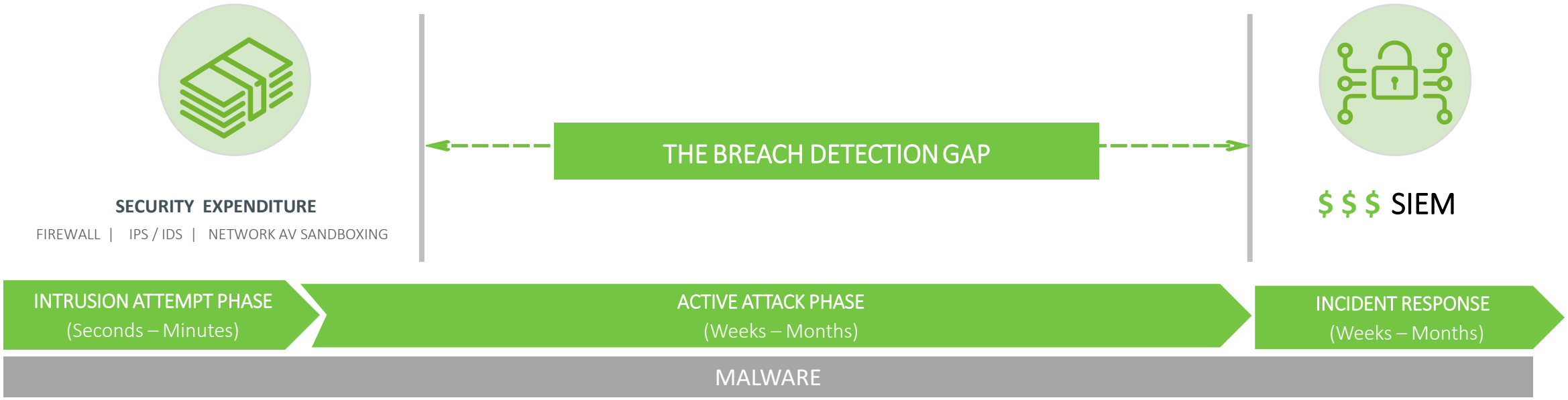
8 out of 10 SMBs don’t have a basic cyber attack response plan

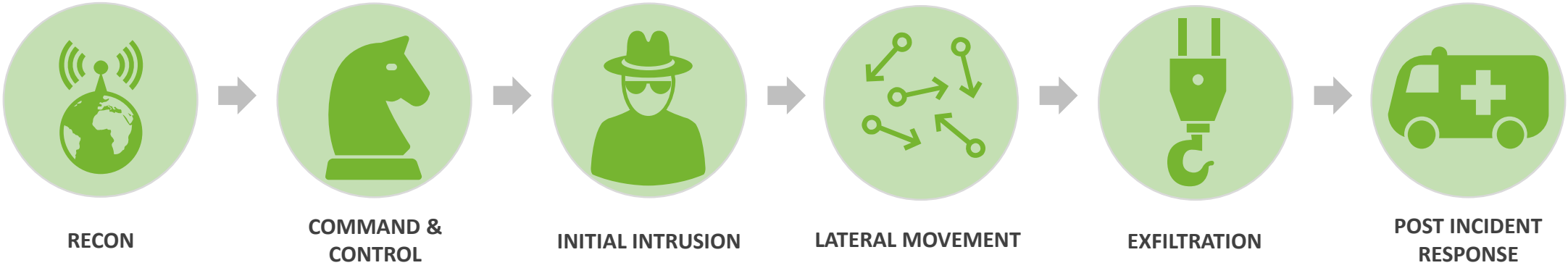
CYBONET

SMB BUYER PROFILE

- Organizations with USD $1–15 million annual revenue are looking for a comprehensive yet affordable security solution
- On average only around 8% of a SMB's budget goes towards the business' security
- Many enterprise solutions require an investment of at least $200,000
- Small and medium sized organizations will often not have a SOC or CISO; most enterprise solutions demand a dedicated analyst interpreting threats

THE BREACH DETECTION GAP

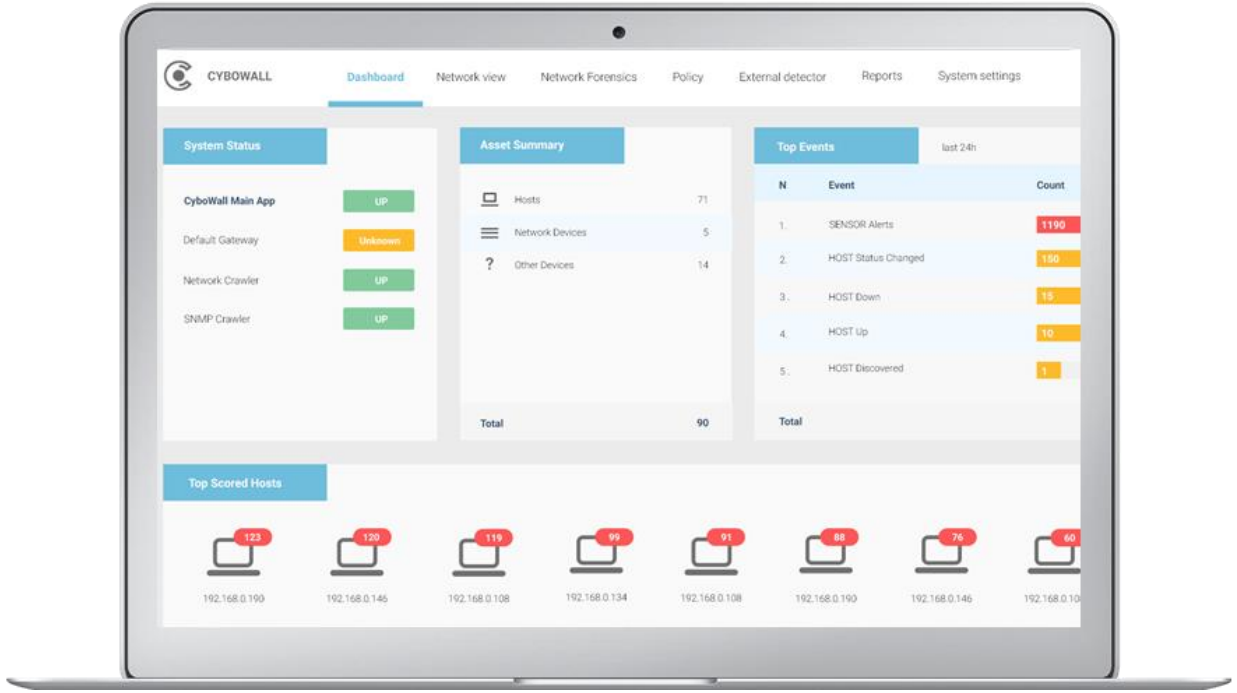




CYBONET INTRODUCES CYBOWALL

Multi-Vector Threat Detection and Response for Small and Medium Sized Organizations

- Quickly detect potential vulnerabilities and active breaches
- Automatically respond to threats as they are discovered
- Manage and report on compliance (GDPR, PCI-DSS, ISO etc.)
- Record and analyze all events and incidents within the network for further investigation



CYBOWALL SOLUTION BENEFITS

Detect Lateral Movement

to trap attackers that have already breached perimeter defenses

Identify Vulnerabilities

for patch deployment prioritization

Automated Response

based on configurable policies without System Administrator/ CISO/SOC intervention

Stop Endpoint Tampering and Malware

by leveraging network and endpoint detection

Map Network Assets

to increase visibility with a comprehensive endpoint map

Meet Compliance Requirements

for PCI-DSS, HIPAA, HITECH, GDPR, ISO etc.

CYBONET

CYBOWALL OVERVIEW

1 Network Sensor

- Network visibility
- Port mirroring/TAP
- IDS at the network level
- Inbound & outbound traffic

2 Network Traps

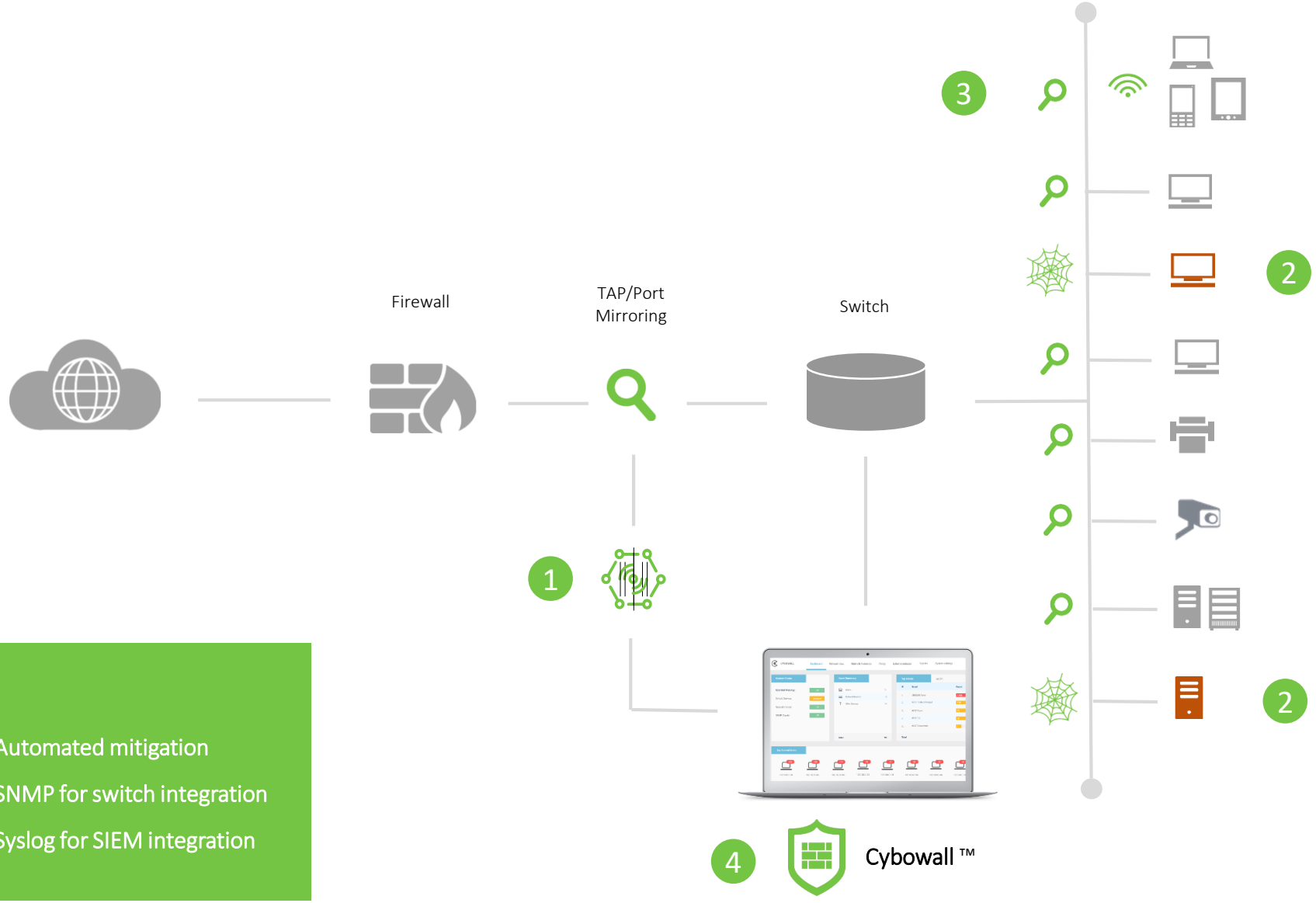
- Distributed deception grid
- Lateral movement

3 Agentless Endpoint Scan

- Asset mapping & port profiles
- Leverage WMI for registry & process investigation
- Correlate forensic data with IOC

4 Policy, Response and Integration

- Send alerts
- Quarantine
- Shutdown port
- End process or application (WMI)
- Automated mitigation
- SNMP for switch integration
- Syslog for SIEM integration



CYBOWALL SOLUTION FEATURES

Asset Mapping

Continuously updated list of all endpoints, including port profiles and activities

Intrusion Detection

Full inbound and outbound network traffic visibility without causing interference

SIEM

Log management, event management, event correlation and reporting to help identify policy violations and enable response procedures

Network Traps

Enable insight into lateral movement between endpoints and detect threats originating within the network by serving as a trip wire for active attacks

Vulnerability Assessment

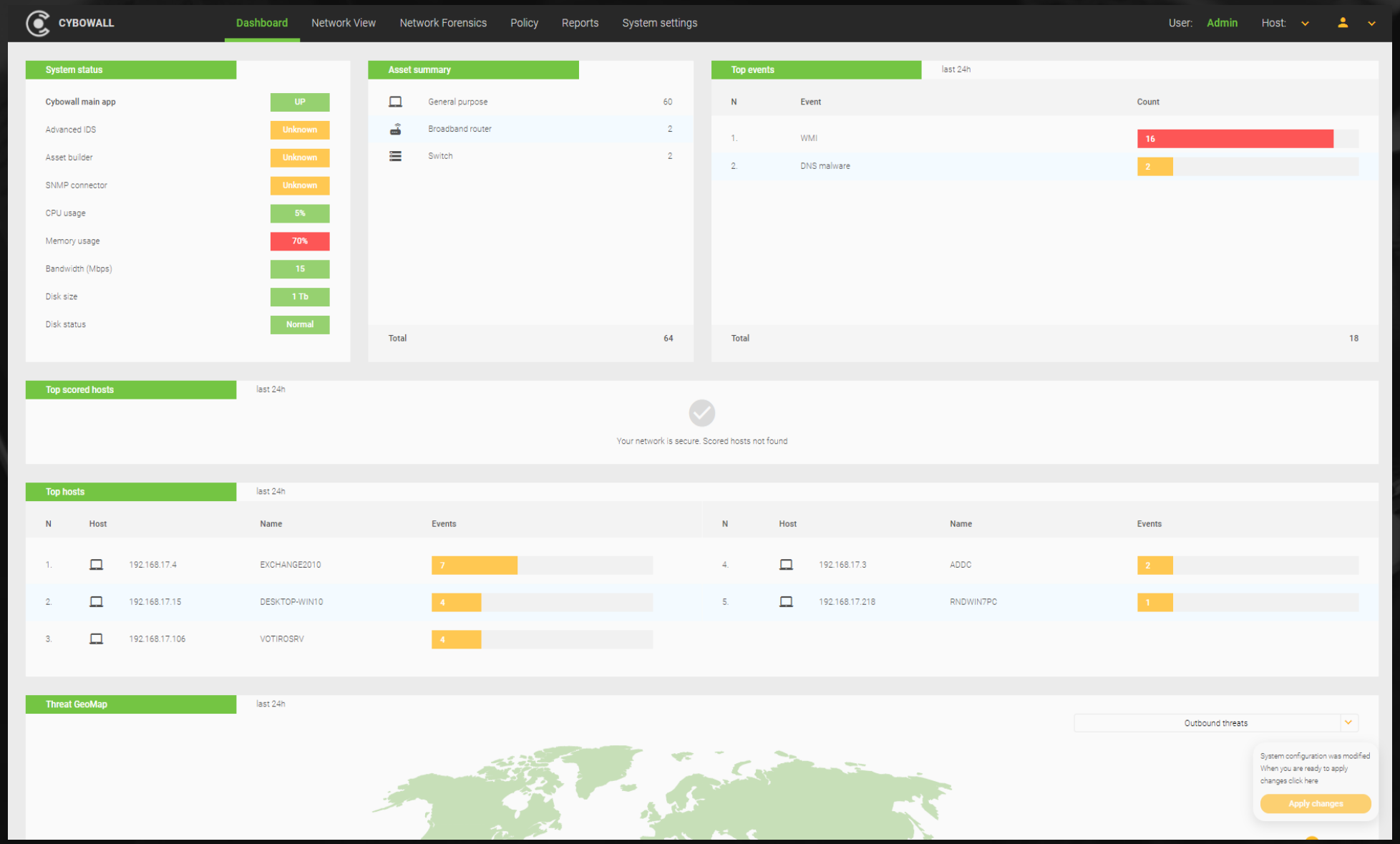
Monitor business assets and identify vulnerable systems inside the network, including risk level, for patch deployment prioritization

Automated Response

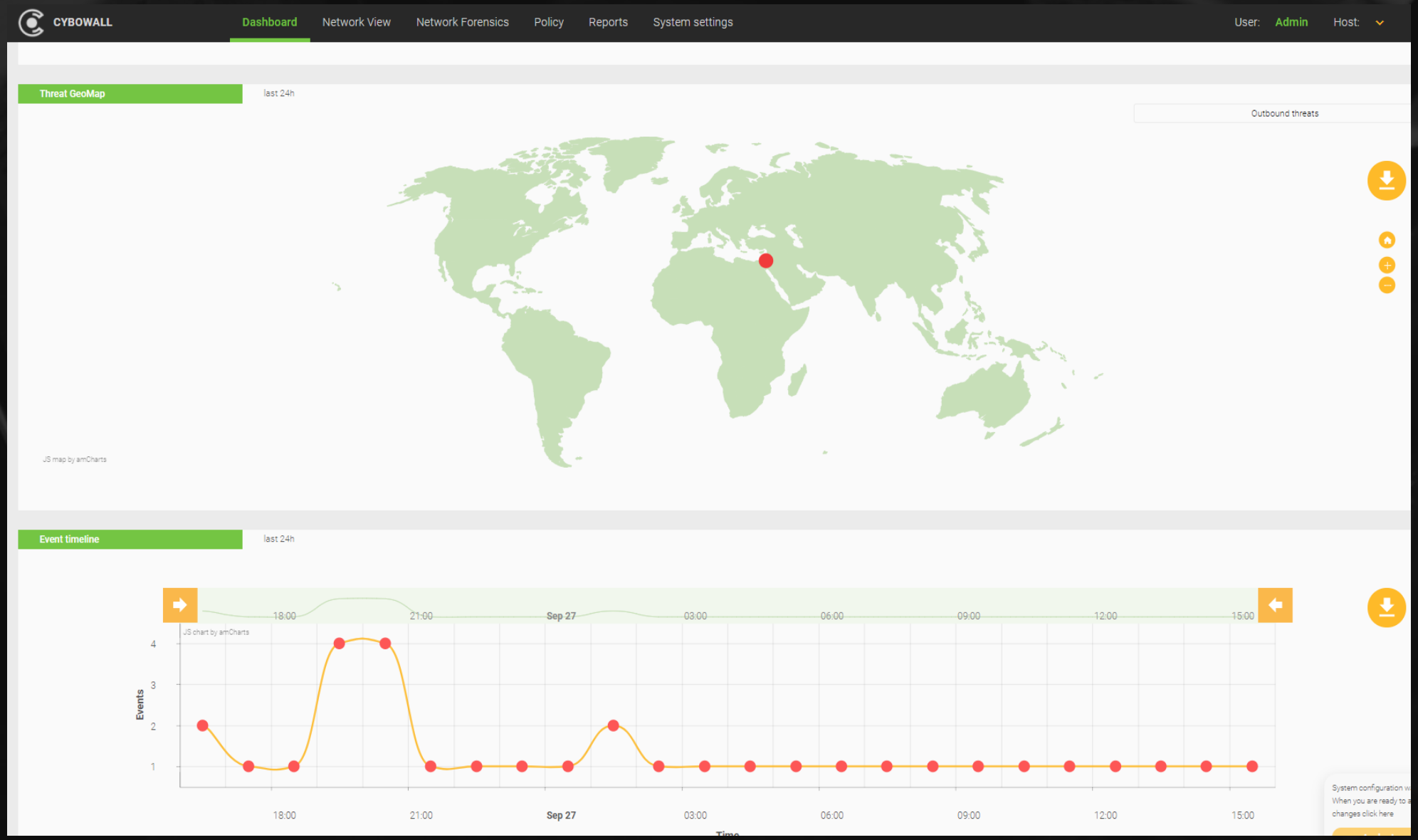
Policy-based responses initiated according to assigned activity/risk factor scores, enabling containment of real time attacks

CYBONET

CYBOWALL INTUITIVE MONITORING WITHOUT A CISO/SOC



CYBOWALL INTUITIVE MONITORING WITHOUT A CISO/SOC



CYBOWALL STOP ENDPOINT TAMPERING & MALWARE

Filter

2017-06-20 - 2017-07-19

Source host

Source port

Destination host

Destination port

Engines:

Sensor × DNS malware alert ×

Severity Severity

Protocol All

Flow All

P2P

Return to SIMPLE View

Records found: 85

Network Forensics

Date&Time	Source Host	Port	Flow	Destination Host	Port	Protocol	Engine	Severity	Description	
2017-07-18 09:33:50.944	10.200.108.7	26237	↑	95.211.223.2 Netherlands	6881	UDP	Sensor	High	A Network Trojan was detected ET CNC Shadowserver Reported CnC Server IP group 46	Details

Network Forensics

Date&Time	Source Host	Port	Flow	Destination Host	Port	Protocol	Engine	Severity	Description	
2017-07-19 11:31:13.132	192.168.248.108	56536	↑	88.245.1.89 Turkey (Izmir)	63456	UDP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent DHT ping request	Details
2017-07-19 10:30:56.022	192.168.248.108	56536	↑	41.177.127.196 South Africa (Cape Town)	47705	UDP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent DHT ping request	Details
2017-07-19 10:20:27.428	192.168.248.108	56536	↑	94.242.219.107 Luxembourg	35075	UDP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent DHT ping request	Details
2017-07-19 10:00:00.329	192.168.248.108	56536	↑	185.36.211.196 Spain (Lorqui)	20706	UDP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent DHT ping request	Details
2017-07-19 09:52:25.173	192.168.248.108	56536	↑	95.186.46.38 Saudi Arabia (Jeddah)	1828	UDP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent DHT ping request	Details
2017-07-19 09:47:00.092	192.168.248.108	56536	↑	190.24.59.225 Colombia (Bogotá)	41016	UDP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent DHT ping request	Details
2017-07-19 09:38:10.021	192.168.248.108	56536	↑	178.141.130.225 Russia (Kirov)	14730	UDP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent DHT ping request	Details
2017-07-19 09:27:59.459	192.168.248.108	56536	↑	213.136.79.7 Germany	6881	UDP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent DHT ping request	Details
2017-07-19 09:04:19.074	192.168.248.108	56536	↑	131.213.35.95 Japan (Tokyo)	6889	UDP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent DHT ping request	Details
2017-07-19 00:37:19.958	192.168.248.192	58989	↑	41.188.108.105 Mauritania	64006	TCP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent peer sync	Details
2017-07-19 00:35:16.832	192.168.248.192	58911	↑	176.58.153.94 Greece (Athens)	28970	TCP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent peer sync	Details
2017-07-19 00:35:16.746	192.168.248.192	58798	↑	111.100.30.20 Japan (Kamirenjaku)	60725	TCP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent peer sync	Details
2017-07-19 00:35:16.730	192.168.248.192	58725	↑	87.203.111.97 Greece (Athens)	24959	TCP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent peer sync	Details
2017-07-19 00:35:16.620	192.168.248.192	58768	↑	197.0.143.203 Tunisia	42610	TCP	Sensor	High	Potential Corporate Privacy Violation ET P2P BitTorrent peer sync	Details

CYBOWALL STOP ENDPOINT TAMPERING & MALWARE

Network Forensics

Date&Time	Source Host	Port	Flow	Destination Host	Port	Protocol	Engine	Severity	Description	
2017-06-22 08:06:59.240	192.168.19.3	63450	↑	8.8.8.8	53		DNS malware alert	CnC	www.joyhafakot.co.il	Details
2017-06-22 08:06:59.240	192.168.19.3	63450	↑	8.8.8.8	53		DNS malware alert	CnC	www.joyhafakot.co.il	Details
2017-06-22 08:06:59.240	192.168.17.210	52402	↔	192.168.19.3	53		DNS malware alert	CnC	www.joyhafakot.co.il	Details
2017-06-22 07:31:06.773	192.168.19.2	58585	↑	8.8.8.8	53		DNS malware alert	CnC	www.joyhafakot.co.il	Details
2017-06-22 07:31:06.773	192.168.19.2	58585	↑	8.8.8.8	53		DNS malware alert	CnC	www.joyhafakot.co.il	Details

virustotal

URL: http://www.joyhafakot.co.il/

Detection ratio: 3 / 65

Analysis date: 2017-06-22 09:33:19 UTC (0 minutes ago)

0 0

Analysis | Additional information | Comments | Votes

URL Scanner	Result
Sophos	Malicious site
Fortinet	Malware site
Kaspersky	Malware site
Quttera	Suspicious site
ADMINUSLabs	Clean site
AegisLab WebGuard	Clean site
AlienVault	Clean site
Antiy-AVL	Clean site
Avira (no cloud)	Clean site

SiteCheck Results | Website Details | Blacklist Status

Warning: Your Website Has Been Blacklisted!

Website: www.joyhafakot.co.il

Status: Site Potentially Harmful. Immediate Action is Required.

Web Trust: Blacklisted (10 Blacklists Checked): Indicates that a major security company (such as Google, McAfee, Norton, etc) is blocking access to your website for security reasons. Please see our recommendation below to fix this issue and restore your traffic.

Scan	Result	Severity	Recommendation
Website Blacklisting	Detected	Critical	CLEAN UP Clean Up & Remove Blacklisting
Site Likely Compromised	Detected	Critical	CLEAN UP Clean Up & Remove Blacklisting
Website Firewall	Not Found	Medium Risk	PATCH AND PROTECT With Sucuri Firewall
Outdated Software	Detected	Medium Risk	PATCH AND PROTECT With Sucuri Firewall

Clean Up your Site Now — CLEAN UP MY SITE

(More Information)

Your site appears to be hacked. Hacked sites can lose nearly 95% of your traffic in as little as 24 to 48 hours if not fixed immediately – losing your organic rankings and being blocked by Google, Bing and many other blacklists. Hacked sites can also expose your customers and readers private and financial information, and turn your site into a host for dangerous malware and illicit material, creating massive liability. Secure your site now with Sucuri.

https://www.virustotal.com/en/url/9a63c7030728eccc8ff24abe0084d67033f8846b56dc2edfdcaf4330bc2da125/analysis/1498123999/

https://sitecheck.sucuri.net/results/www.joyhafakot.co.il

CYBOWALL MAP NETWORK ASSETS

CYBOWALL | Dashboard | Network View | Network Forensics | Policy | Reports | System settings | User: Admin | Host:

Filter

Up | Down | Host | Network | Switch to extended view | Records found 69

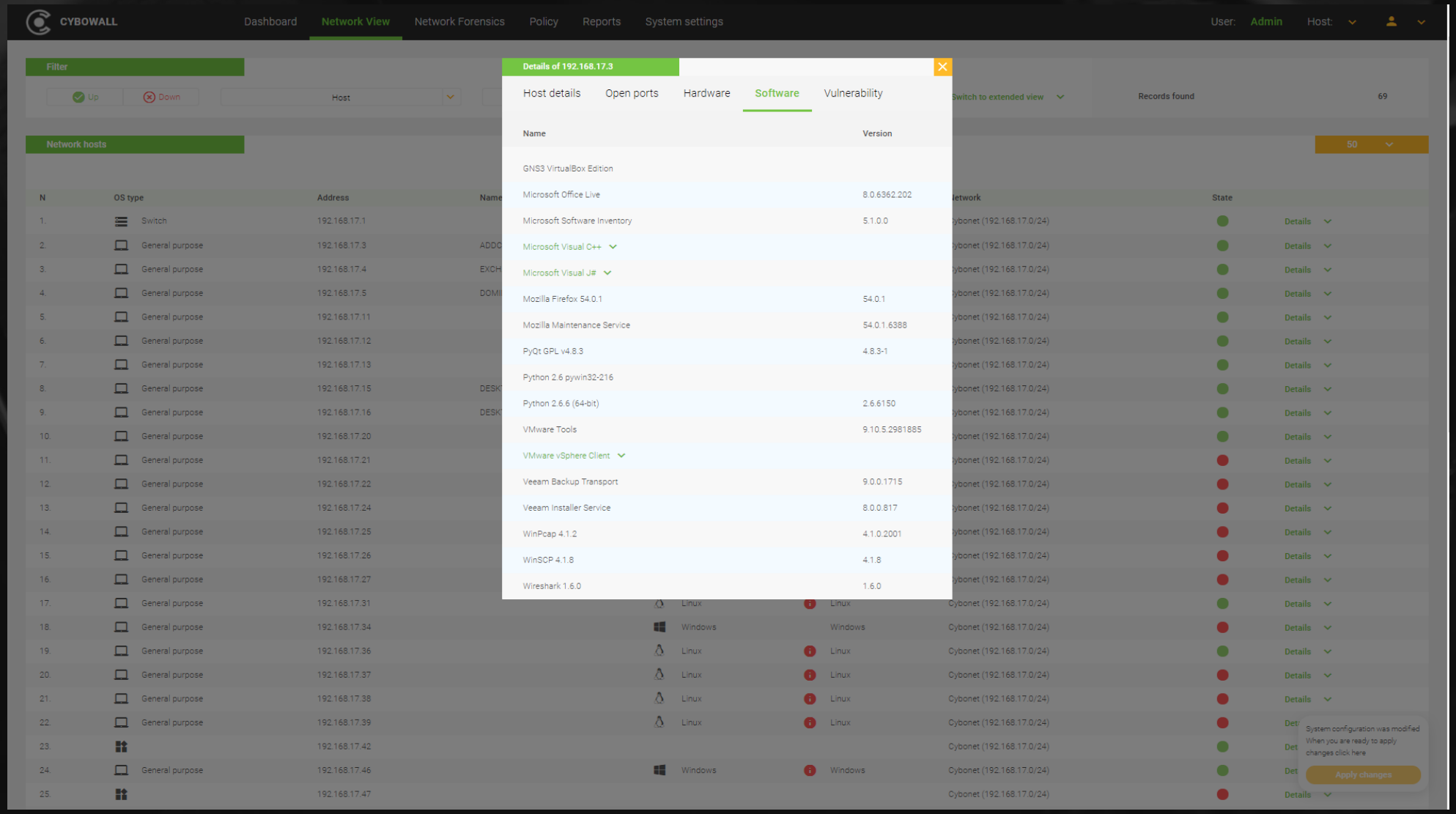
Network hosts

1 2 | 50

N	OS type	Address	Name	OS family	Port profile	Network	State	
1.	Switch	192.168.17.1		Comware		Cybonet (192.168.17.0/24)		Details
2.	General purpose	192.168.17.3	ADDC	Windows	Windows	Cybonet (192.168.17.0/24)		Details
3.	General purpose	192.168.17.4	EXCHANGE2010	Windows	Windows	Cybonet (192.168.17.0/24)		Details
4.	General purpose	192.168.17.5	DOMINOSRV	Windows	Windows	Cybonet (192.168.17.0/24)		Details
5.	General purpose	192.168.17.11		Linux	Linux	Cybonet (192.168.17.0/24)		Details
6.	General purpose	192.168.17.12		Linux	Linux	Cybonet (192.168.17.0/24)		Details
7.	General purpose	192.168.17.13		Linux	Linux	Cybonet (192.168.17.0/24)		Details
8.	General purpose	192.168.17.15	DESKTOP-WIN10	Windows	Windows	Cybonet (192.168.17.0/24)		Details
9.	General purpose	192.168.17.16	DESKTOP-WIN8	Windows	Windows	Cybonet (192.168.17.0/24)		Details
10.	General purpose	192.168.17.20		Linux	Linux	Cybonet (192.168.17.0/24)		Details
11.	General purpose	192.168.17.21		Linux	Linux	Cybonet (192.168.17.0/24)		Details
12.	General purpose	192.168.17.22		Linux	Linux	Cybonet (192.168.17.0/24)		Details
13.	General purpose	192.168.17.24		Linux	Linux	Cybonet (192.168.17.0/24)		Details
14.	General purpose	192.168.17.25		Linux	Linux	Cybonet (192.168.17.0/24)		Details
15.	General purpose	192.168.17.26		Linux	Linux	Cybonet (192.168.17.0/24)		Details
16.	General purpose	192.168.17.27		Linux	Linux	Cybonet (192.168.17.0/24)		Details
17.	General purpose	192.168.17.31		Linux	Linux	Cybonet (192.168.17.0/24)		Details
18.	General purpose	192.168.17.34		Windows	Windows	Cybonet (192.168.17.0/24)		Details
19.	General purpose	192.168.17.36		Linux	Linux	Cybonet (192.168.17.0/24)		Details
20.	General purpose	192.168.17.37		Linux	Linux	Cybonet (192.168.17.0/24)		Details
21.	General purpose	192.168.17.38		Linux	Linux	Cybonet (192.168.17.0/24)		Details
22.	General purpose	192.168.17.39		Linux	Linux	Cybonet (192.168.17.0/24)		Det
23.		192.168.17.42				Cybonet (192.168.17.0/24)		Det
24.	General purpose	192.168.17.46		Windows	Windows	Cybonet (192.168.17.0/24)		Det
25.		192.168.17.47				Cybonet (192.168.17.0/24)		Details

System configuration was modified
When you are ready to apply changes click here
Apply changes
0

CYBOWALL MAP NETWORK ASSETS



CYBOWALL IDENTIFY VULNERABILITIES

CYBOWALL | Dashboard | Network View | Network Forensics | Policy | Reports | System settings | User: Admin | Host:

Details of 192.168.17.106

Host details | Open ports | Hardware | Software | Vulnerability

Common Vulnerabilities and Exposures

Application	Details	Top score
Cisco WebEx Meetings	CVE-2017-3823	9.3

Description: An issue was discovered in the Cisco WebEx Extension before 1.0.7 on Google Chrome, the ActiveTouch General Plugin Container before 106 on Mozilla Firefox, the GpcContainer Class ActiveX control plugin before 10031.6.2017.0126 on Internet Explorer, and the Download Manager ActiveX control plugin before 2.1.0.10 on Internet Explorer. A vulnerability in these Cisco WebEx browser extensions could allow an unauthenticated, remote attacker to execute arbitrary code with the privileges of the affected browser on an affected system. This vulnerability affects the browser extensions for Cisco WebEx Meetings Server and Cisco WebEx Centers (Meeting Center, Event Center, Training Center, and Support Center) when they are running on Microsoft Windows. The vulnerability is a design defect in an application programing interface (API) response parser within the extension. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.

Links:

http://www.securityfocus.com/bid/95737

https://0patch.blogspot.com/2017/01/micropatching-remote-code-execution-in.html

https://bugs.chromium.org/p/project-zero/issues/detail?id=1096

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170124-webex

CWE: CWE-119

Cvssv3:

Attack vector: NETWORK

Attack complexity: LOW

Privileges required: NONE

User interaction: REQUIRED

Confidentiality: HIGH

Integrity: HIGH

Availability: HIGH

Cvssv2:

Attack vector: NETWORK

Attack complexity: MEDIUM

Confidentiality: COMPLETE

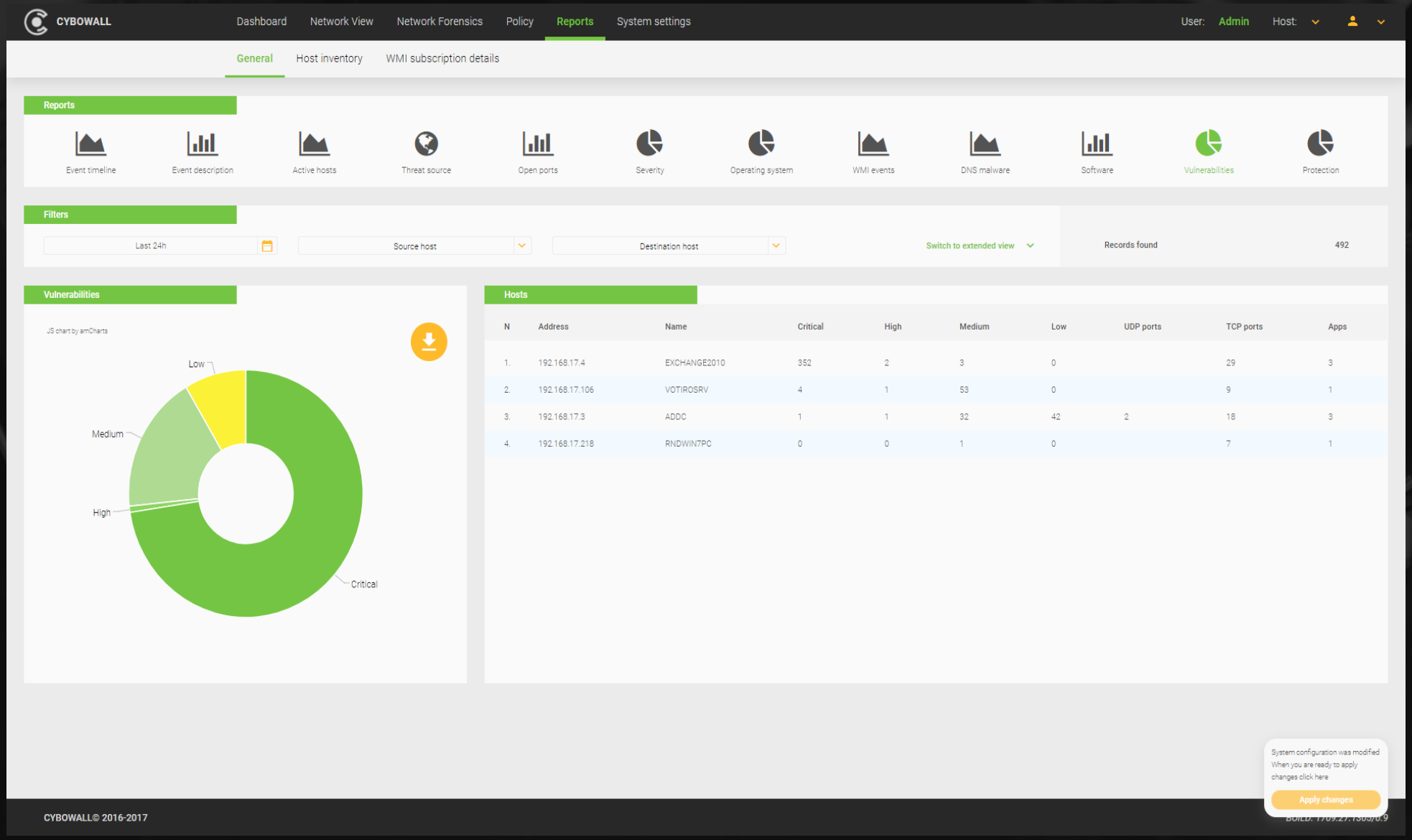
Integrity: COMPLETE

Availability: COMPLETE

System configuration was modif
When you are ready to apply changes click here

Apply changes

CYBOWALL IDENTIFY VULNERABILITIES



CYBONET

R&D Center

Matam, Building 23,

P.O.B. 15102

Haifa 3190501 Israel

+972 (4) 821-2321

info@cybonet.com

www.cybonet.com

CASE STUDY TARGET BREACH

Background

At the end of 2013, attackers breached the US chain retailer's point-of-sale system and stole data, including names and all the information required to manufacture counterfeit credit cards.

Facts and Figures

- 40 million credit card / debit card records stolen
- 70 million data files stolen
- 98 million total unique customers affected

Outcomes

Firings of Target executives including the CEO, President and Chairman.

Target settled class action lawsuits for approximately USD $50 million.

ANATOMY OF THE TARGET BREACH