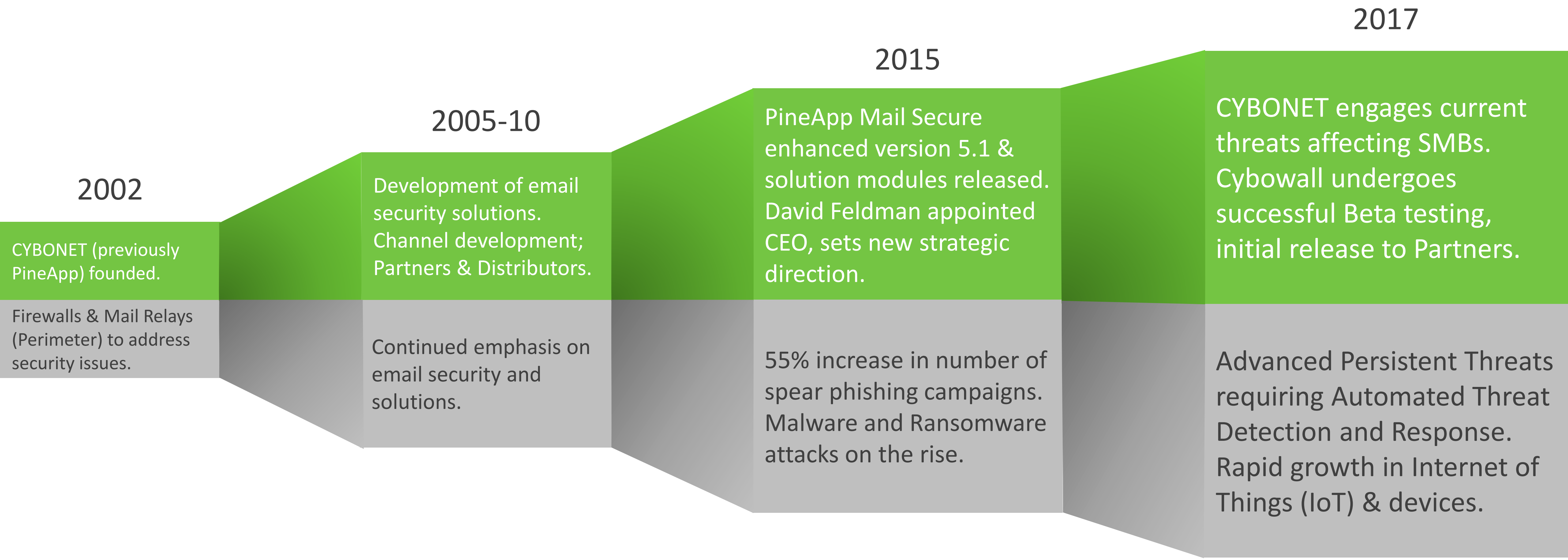
Cybowall Solution Overview

CYBONET

CYBONET OUR HISTORY



2002

CYBONET (previously PineApp) founded.

Firewalls & Mail Relays (Perimeter) to address security issues.

2005-10

Development of email security solutions. Channel development; Partners & Distributors.

Continued emphasis on email security and solutions.

2015

PineApp Mail Secure enhanced version 5.1 & solution modules released. David Feldman appointed CEO, sets new strategic direction.

55% increase in number of spear phishing campaigns. Malware and Ransomware attacks on the rise.

2017

CYBONET engages current threats affecting SMBs. Cybowall undergoes successful Beta testing, initial release to Partners.

Advanced Persistent Threats requiring Automated Threat Detection and Response. Rapid growth in Internet of Things (IoT) & devices.

Our History reflects the Evolution of Cybersecurity

ABOUT CYBONET

CORE EXPERIENCE

PRODUCT LINES

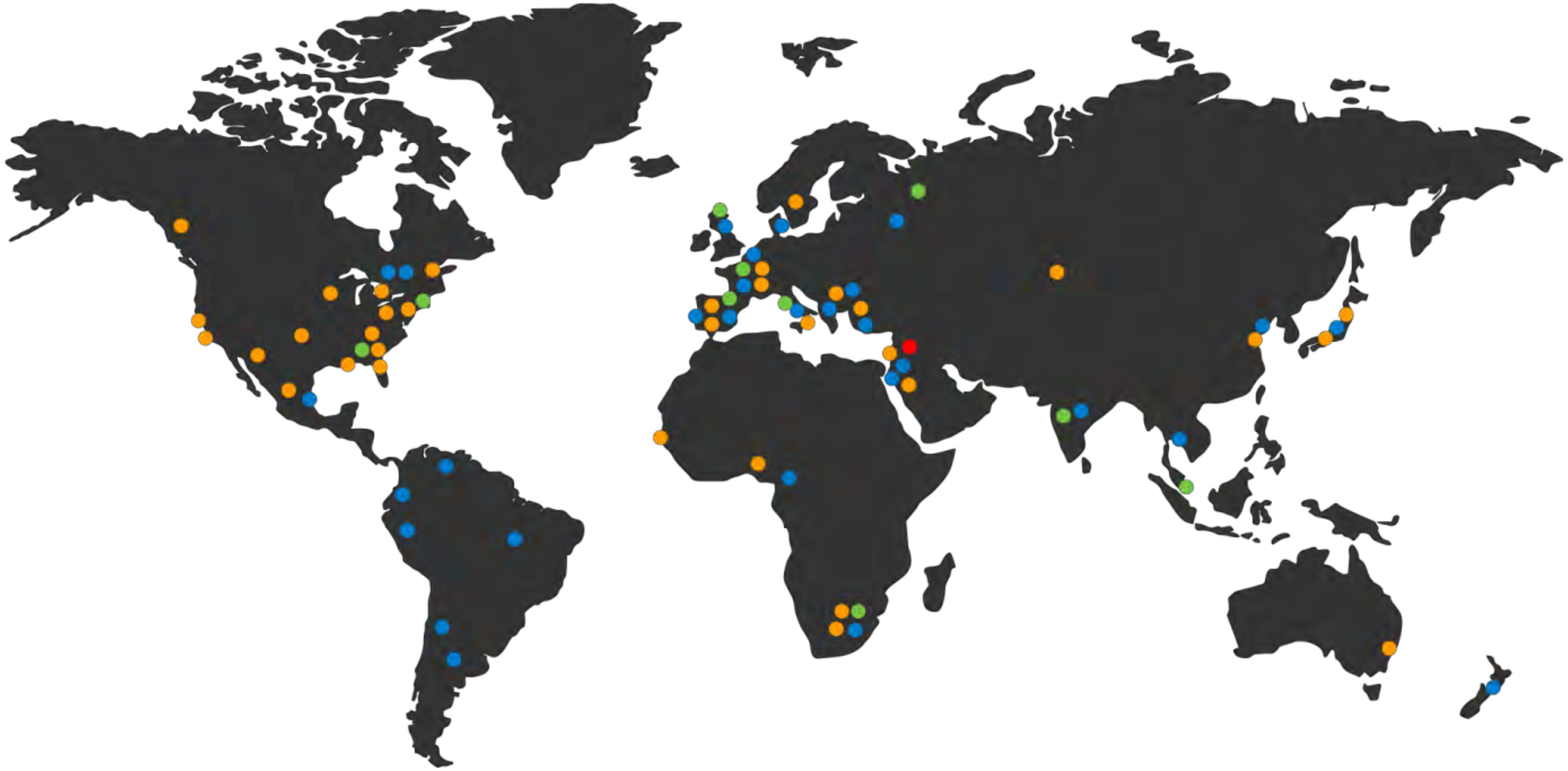
FACTS & FIGURES

- Leading product company servicing multiple vertical markets
- Deploy and manage large scale enterprise cloud platforms
- Managed services, enterprise software, SaaS
- Telco installation worldwide
- Innovator and leader in anti-botnet activity

- Cybowall:
  - Advanced Threat Detection
- PineApp Mail Secure:
  - Advanced Messaging Solution
- CyboCloud:
  - Cloud Messaging Solution
- Outbound Spam Guard (OSG):
  - IP Blacklisting Prevention for Telecoms

- HQ & R&D in Israel
- Privately owned
- Global company with partners in North America, Europe, CIS & Far East
- Wide installation base in over 60 countries

CYBONET GLOBAL PRESENCE



● Headquarters ● Office ● Distribution ● Reseller

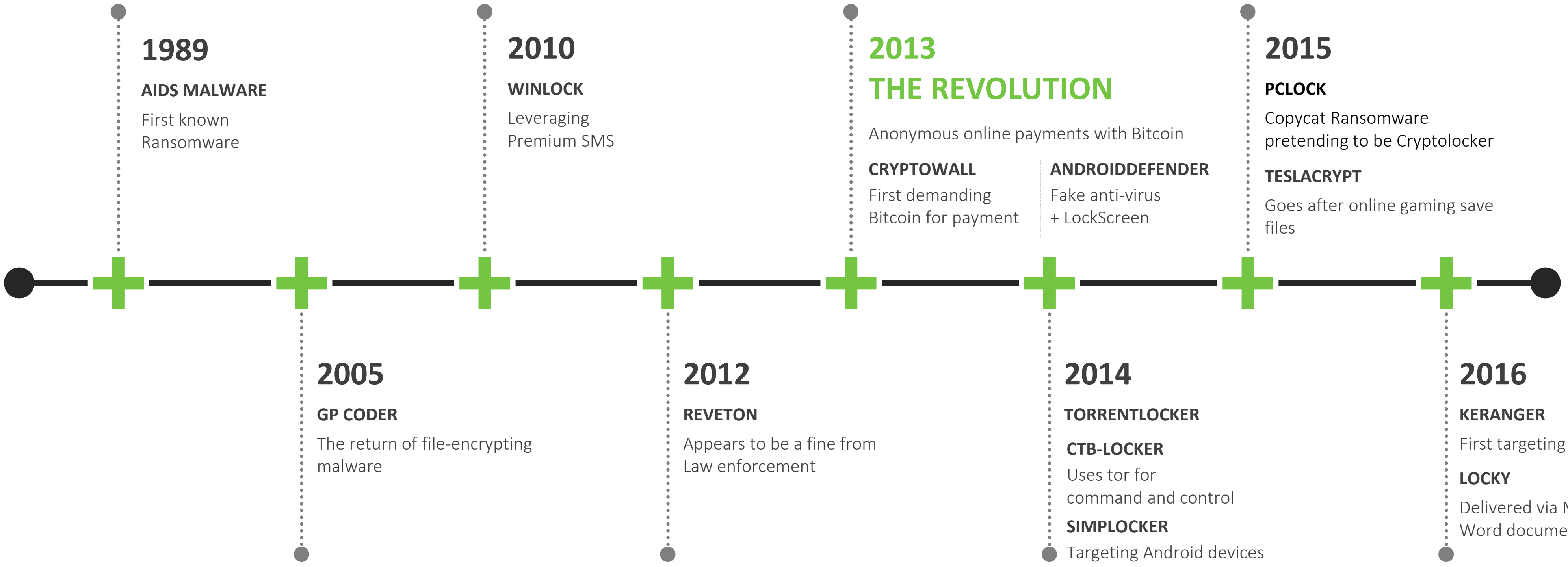
OUR LARGER INTERNATIONAL CLIENTS

Транснефть
Федеральное дорожное агентство
LFP
I'm lovin' it
The Knesset
JAVERIANA
ВОЛГАЭНЕРГОСБЫТ
ФЕДЕРАЛЬНАЯ ТАМОЖЕННАЯ СЛУЖБА
nucentric
GENESI SERVICE
FINGER LAKES Technologies Group, Inc.
TRIMAX
columbus
ipNX
Telma
it æ
First Technology
GAZPROM
SUBARU
alicorp
alvarion
Navantia
ups
OAK
Альфа-Банк
MIND
VEGA
БАНК СОВЕТСКИЙ
Ministério da Economia e da Inovação
DATA SHEPHERD
NEVIS COMPUTERS
N-Defender
VIETTEL
iConnecT.zm
more than just internet!
MTN
ISOCEL telecom
CipherWave
Cyber-NET
Ministry of Education
Нефтиса
Formação Vocacional
HITACHI Inspire the Next
ELES
GESTAMP
Банк Балтика
Банк Москвы
TOYOTA
LANKA BELL
net4 reach beyond
Data Secure Solutions Securing IT Networks
APJII
CtrlS
prodware a global partner
SWAZILAND POSTS & TELECOMMUNICATIONS CORPORATION
isenr
СБСистем
ИНГОССТРАХ Ingosstrakh
MRV
АЛЬТА-БАНК
БАНК ЗЕНИТ
ASI SOLUTIONS
BEAM TELECOM
Make the right connection
pegasus
...and networking comes closer
TOT
INFRASAT
mailsecurer
Moratelindo
Балтийский Банк
Europcar
Pubblicità

SPAM PHISHING MALWARE RANSOMWARE

THE RISE OF RANSOMWARE

30 ACTIVE MALWARE FAMILIES



1989

AIDS MALWARE

First known Ransomware

2005

GP CODER

The return of file-encrypting malware

2010

WINLOCK

Leveraging Premium SMS

2012

REVETON

Appears to be a fine from Law enforcement

2013 THE REVOLUTION

Anonymous online payments with Bitcoin

CRYPTOWALL

First demanding Bitcoin for payment

ANDROIDDEFENDER

Fake anti-virus + LockScreen

2014

TORRENTLOCKER

CTB-LOCKER

Uses tor for command and control

SIMPLOCKER

Targeting Android devices

2015

PCLOCK

Copycat Ransomware pretending to be Cryptolocker

TESLACRYPT

Goes after online gaming save files

2016

KERANGER

First targeting OS X

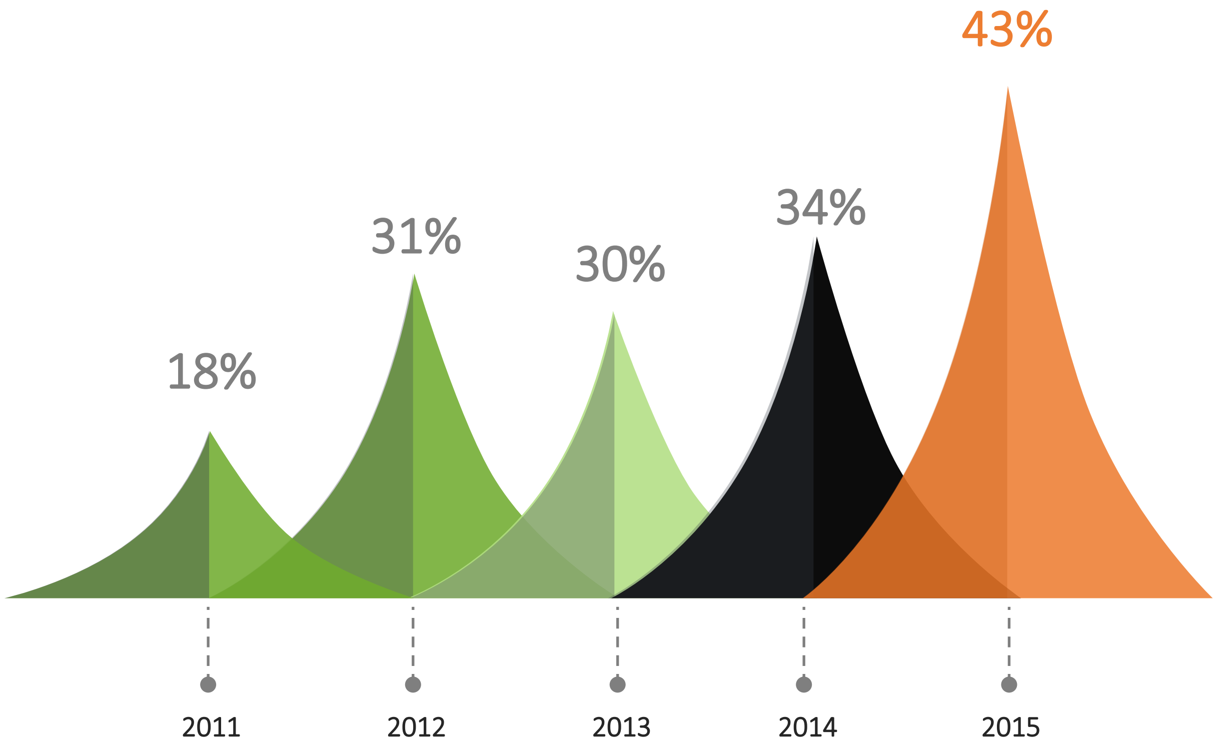
LOCKY

Delivered via Microsoft Word document

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
© 2016, Small Business Trends, LLC

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

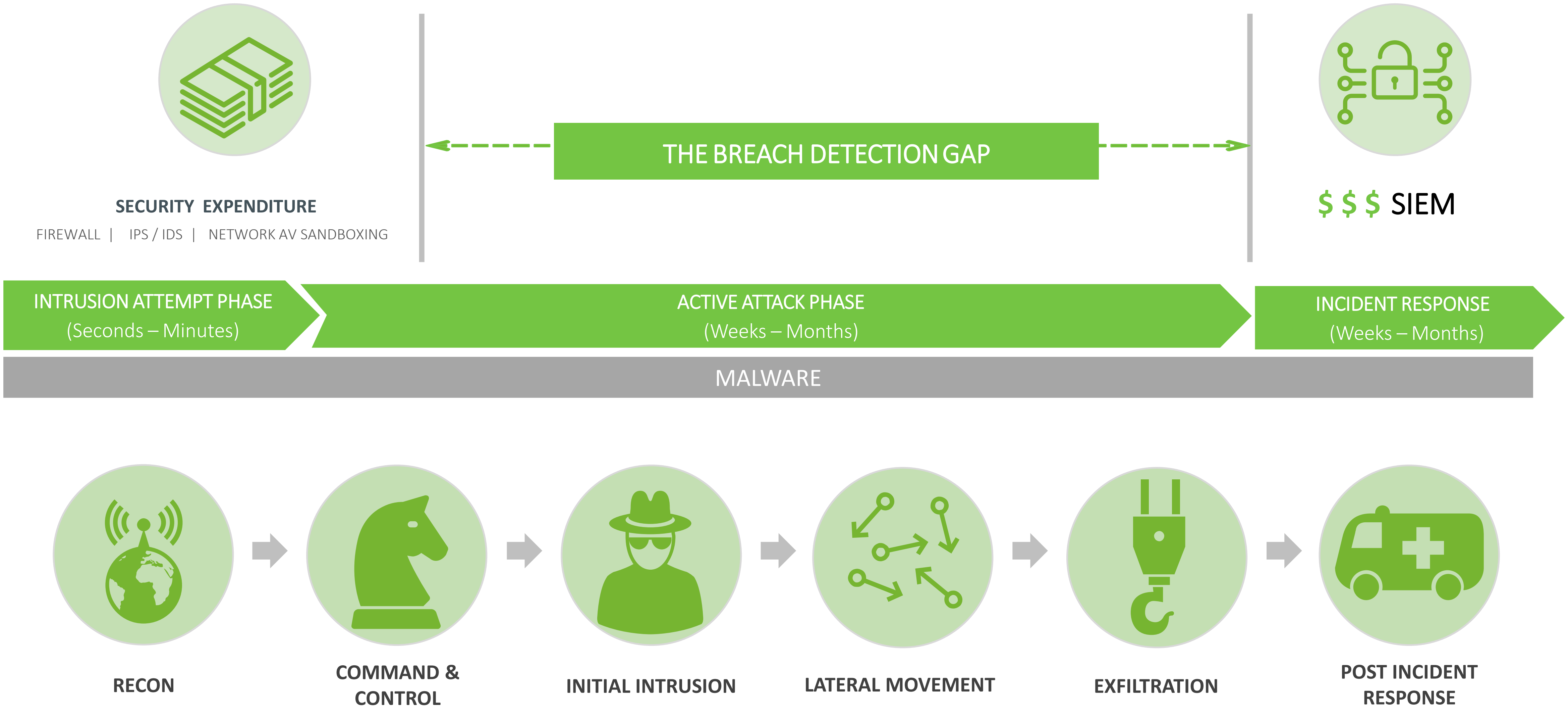
CYBER ATTACK RESPONSE PLAN

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

SMB BUYER PROFILE

- Organizations with limited security resources are looking for a comprehensive yet affordable security solution
- On average only around 6-8% 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



SECURITY EXPENDITURE

FIREWALL | IPS / IDS | NETWORK AV SANDBOXING

THE BREACH DETECTION GAP

$ $ $ SIEM

INTRUSION ATTEMPT PHASE (Seconds – Minutes)

ACTIVE ATTACK PHASE (Weeks – Months)

INCIDENT RESPONSE (Weeks – Months)

MALWARE

RECON

COMMAND & CONTROL

INITIAL INTRUSION

LATERAL MOVEMENT

EXFILTRATION

POST INCIDENT RESPONSE

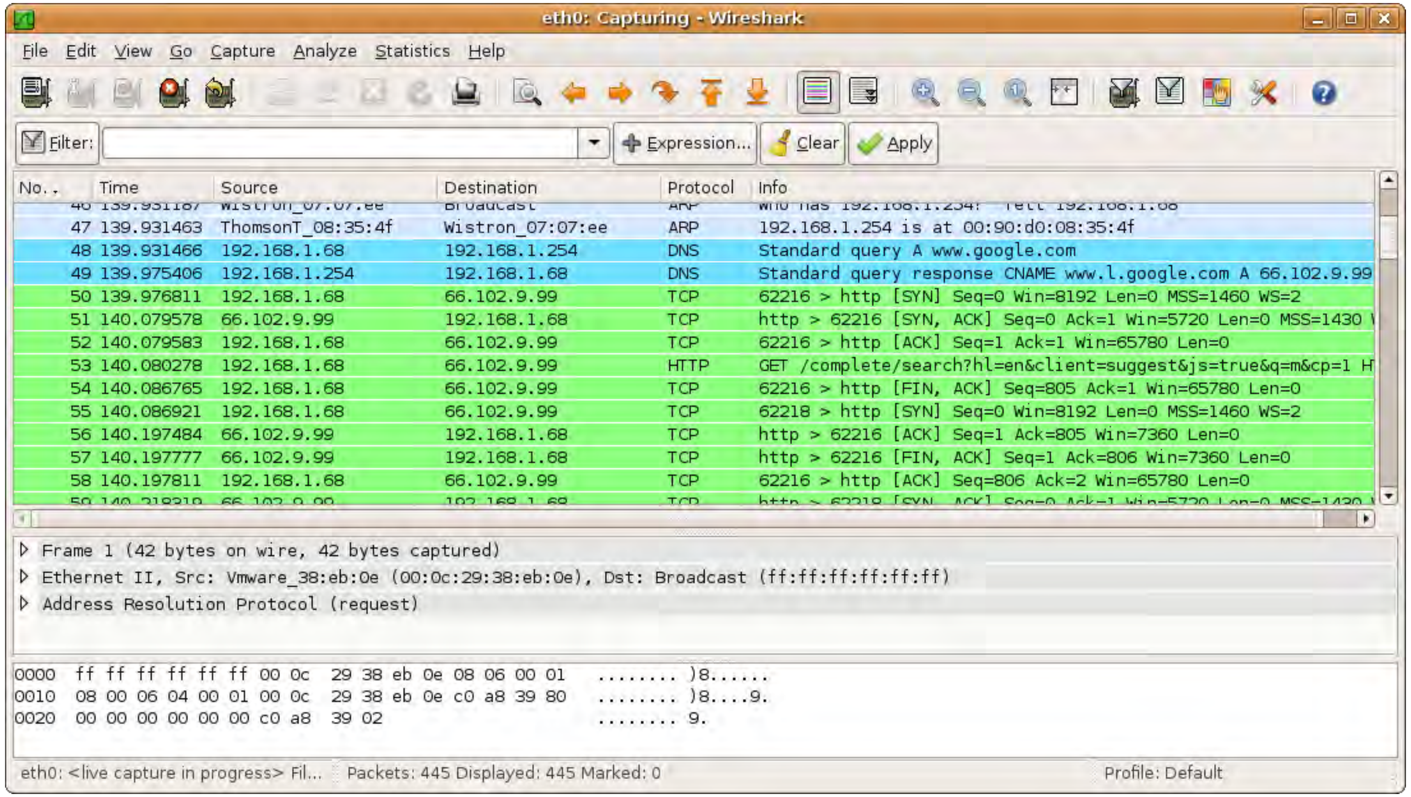
WHAT IS AN INTRUSION?

- Somebody attempting to break into or misuse your system
- The word ‘misuse’ can reflect something as severe as stealing confidential data or something more minor, for example, misusing your email system for spam
- Any set of actions that attempt to compromise the integrity, confidentiality or availability of resources
- In the context of information systems, intrusion refers to any unauthorized access, unauthorized attempts to access or damage resources, or malicious use of information resources

WHAT IS AN INTRUSION DETECTION SYSTEM (IDS)?

- A system that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack
- Designed to detect security breaches and aid in mitigating damage caused by hacking
- Capable of recognizing typical attack patterns, analyzing abnormal activity patterns and tracking user policy violations
- Purpose of IDS; spot suspicious activity within the system and sound an alarm. Can be configured to trigger an alarm for abnormal activity, not only an intrusion
- Can alert an administrator to a security breach, policy violation or other compromise

WHAT IS AN INTRUSION DETECTION SYSTEM (IDS)?

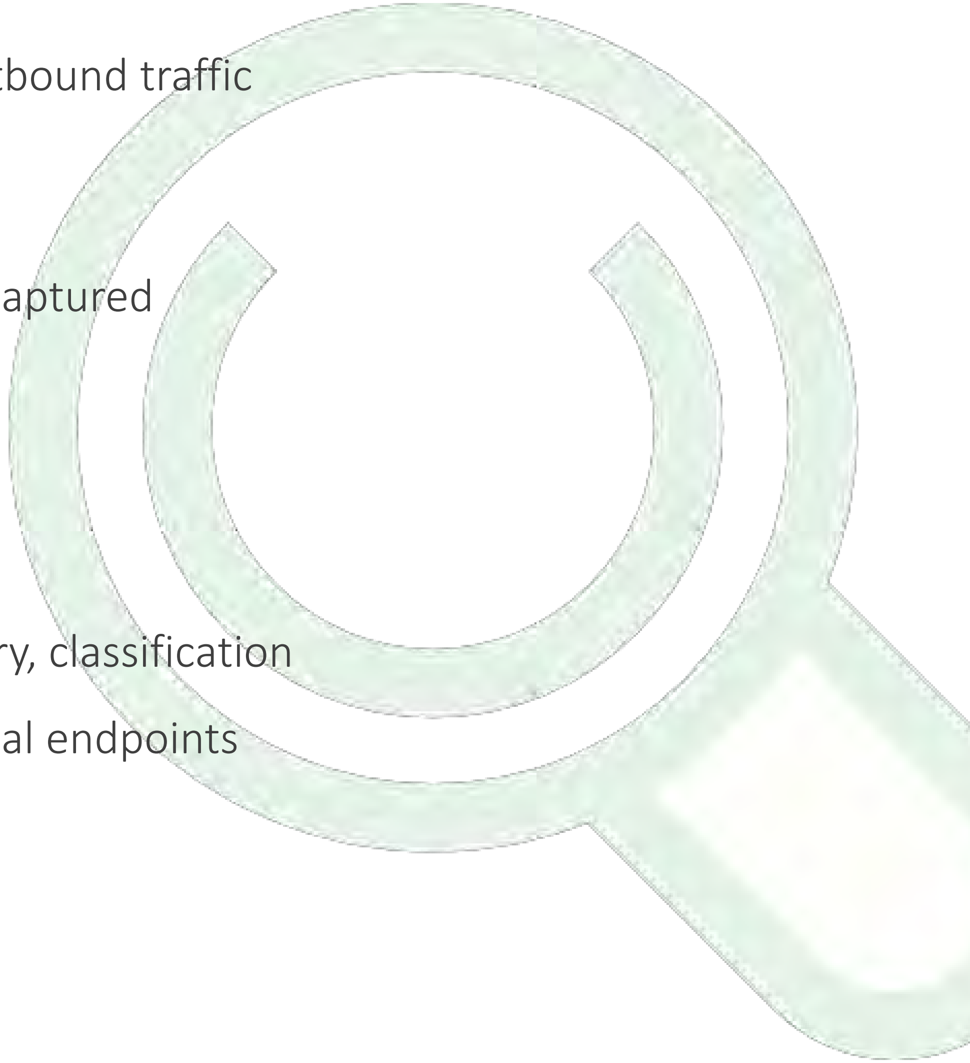

eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source             Destination        Protocol  Info
  46 139.931187  Wistron_07:07:ee   Broadcast          ARP       Who has 192.168.1.254?  Tell 192.168.1.68
  47 139.931463  ThomsonT_08:35:4f  Wistron_07:07:ee   ARP       192.168.1.254 is at 00:90:d0:08:35:4f
  48 139.931466  192.168.1.68       192.168.1.254      DNS       Standard query A www.google.com
  49 139.975406  192.168.1.254      192.168.1.68       DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
  50 139.976811  192.168.1.68       66.102.9.99        TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  51 140.079578  66.102.9.99        192.168.1.68       TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 \
  52 140.079583  192.168.1.68       66.102.9.99        TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
  53 140.080278  192.168.1.68       66.102.9.99        HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
  54 140.086765  192.168.1.68       66.102.9.99        TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
  55 140.086921  192.168.1.68       66.102.9.99        TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
  56 140.197484  66.102.9.99        192.168.1.68       TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
  57 140.197777  66.102.9.99        192.168.1.68       TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
  58 140.197811  192.168.1.68       66.102.9.99        TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
  59 140.218319  66.102.9.99        192.168.1.68       TCP       http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 \

▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.

eth0: <live capture in progress> Fil...   Packets: 445 Displayed: 445 Marked: 0          Profile: Default
```

Classtype	Description
attempted-admin	Attempted Administrator Privilege Gain
attempted-user	Attempted User Privilege Gain
inappropriate-content	Inappropriate Content was Detected
policy-violation	Potential Corporate Privacy Violation
shellcode-detect	Executable code was detected
successful-admin	Successful Administrator Privilege Gain
successful-user	Successful User Privilege Gain
trojan-activity	A Network Trojan was detected
unsuccessful-user	Unsuccessful User Privilege Gain
web-application-attack	Web Application Attack
attempted-dos	Attempted Denial of Service
attempted-recon	Attempted Information Leak
bad-unknown	Potentially Bad Traffic
default-login-attempt	Attempt to login by a default username and password
denial-of-service	Detection of a Denial of Service Attack
misc-attack	Misc Attack
non-standard-protocol	Detection of a non-standard protocol or event
rpc-portmap-decode	Decode of an RPC Query
successful-dos	Denial of Service
successful-recon-largescale	Large Scale Information Leak
successful-recon-limited	Information Leak
suspicious-filename-detect	A suspicious filename was detected
suspicious-login	An attempted login using a suspicious username was detected
system-call-detect	A system call was detected
unusual-client-port-connection	A client was using an unusual port
web-application-activity	Access to a potentially vulnerable web application

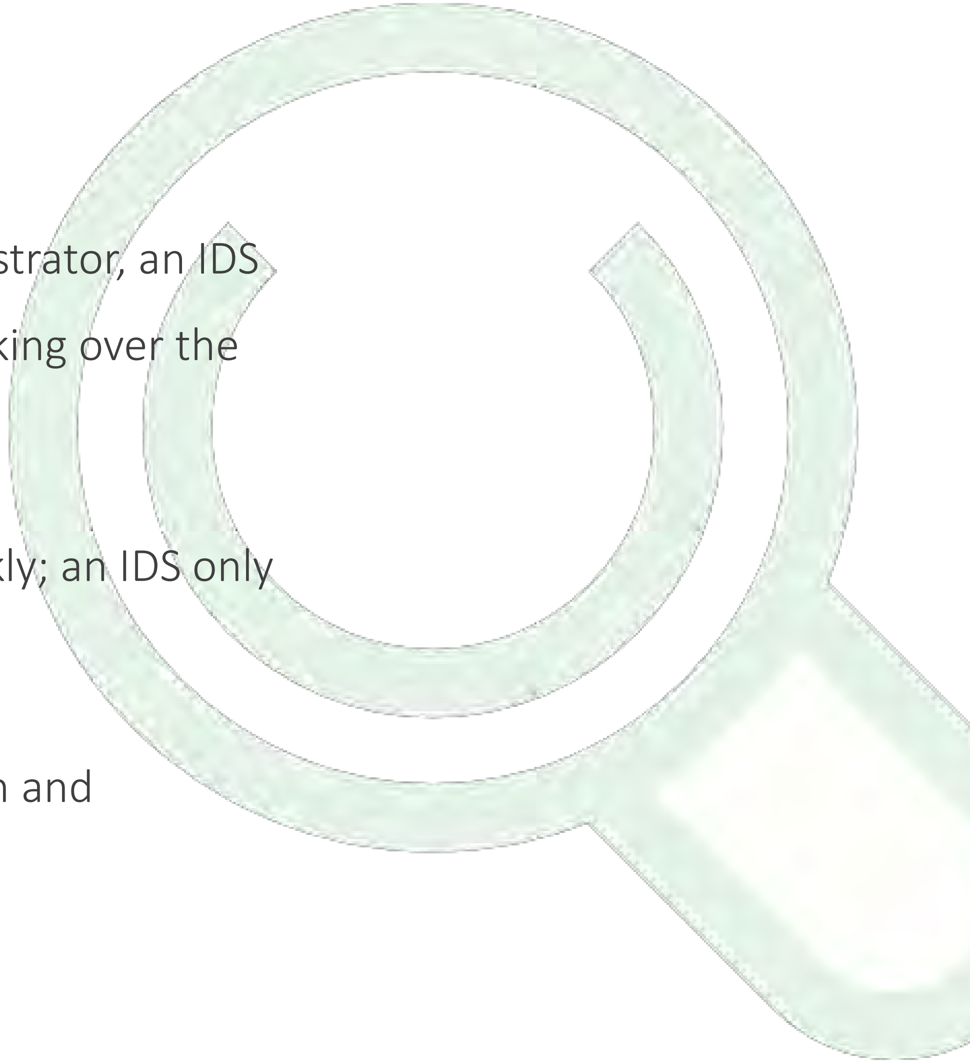
IDS classifications

CYBOWALL IDS CAPABILITIES



- Network Sensor TAP/Port Mirroring takes a copy of all inbound and outbound traffic for full visibility
- Abnormal/suspicious user or service activity is identified by analyzing captured network traffic
- Employs the Suricata Open Source IDS monitoring engine
- Uses Endpoint Fingerprinting and File Fingerprinting to enable discovery, classification and monitoring of data and connected devices, including non-traditional endpoints
- No interference in the organization’s operations
- Does not reveal traffic monitoring to potentially malicious sources

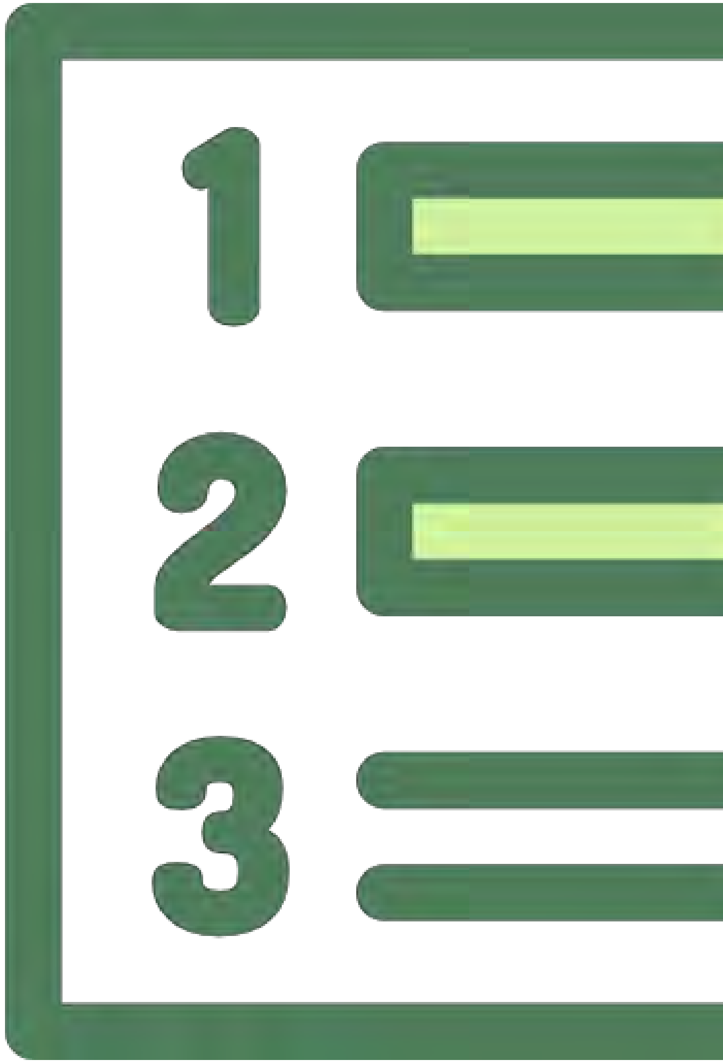
IDS WHY IT’S NOT ENOUGH?



- IDS is a listen-only device; passive – monitors and notifies
- Although traffic is monitored and results can be reported to an administrator, an IDS cannot automatically take action to prevent a detected exploit from taking over the system
- Once a network is breached, vulnerabilities can be exploited very quickly; an IDS only cannot provide adequate response/mitigation
- An IDS can be prone to ‘false positives’; requires effective configuration and interpretation

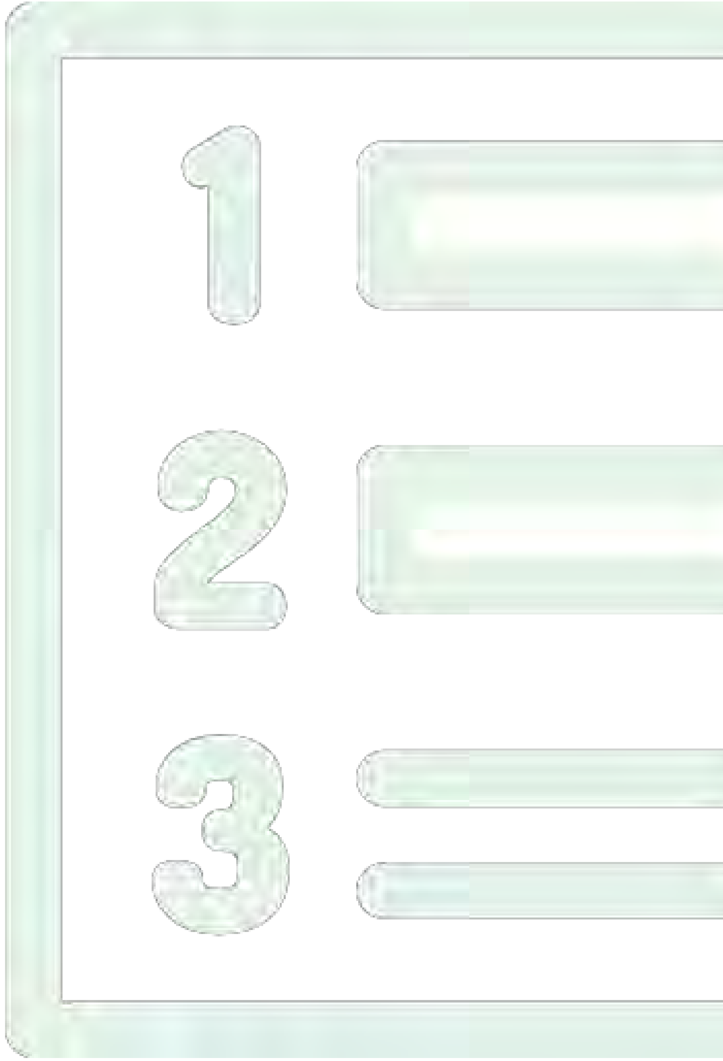
WHAT IS SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)?

- An approach to security management that seeks to provide a holistic view of an organization’s IT security
- Combines SIM (Security Information Management) and SEM (Security Event Management) into a single security management system
- Data analyzed from a single point of view to make it easier to spot trends and see patterns
- Correlate and analyze security event data from across the network in real-time
- Features; data aggregation, correlation, alerts, dashboards, compliance, retention, forensic analysis



CYBOWALL SIEM CAPABILITIES

- Combines output from multi-vector solution; Network Sensor, Network Traps, Agentless Endpoint Scan
- Correlates and analyzes events across disparate sources within the network
- Dashboard; intuitive interface to optimize monitoring and breach detection
- Offers simple, configurable, policy-based mitigation and response
- Includes; event correlation, alerts, incident response and reporting



SIEM WHY IT’S NOT ENOUGH?

- Complex to set up and manage, including data collection, normalization, correlation
- SIEM takes long to deploy; critical questions cannot be answered until correlation rules fine-tuned
- Report data is often not actionable, hard to understand and contains too much ‘noise’
- Analytical capabilities can be limited and cumbersome for the current threat landscape; insufficiently agile and responsive to counter Advance Persistent Threats
- SIEM requires considerable investment; cost of the solution, cost of hiring and training security specialists/consultants for data analysis and operation

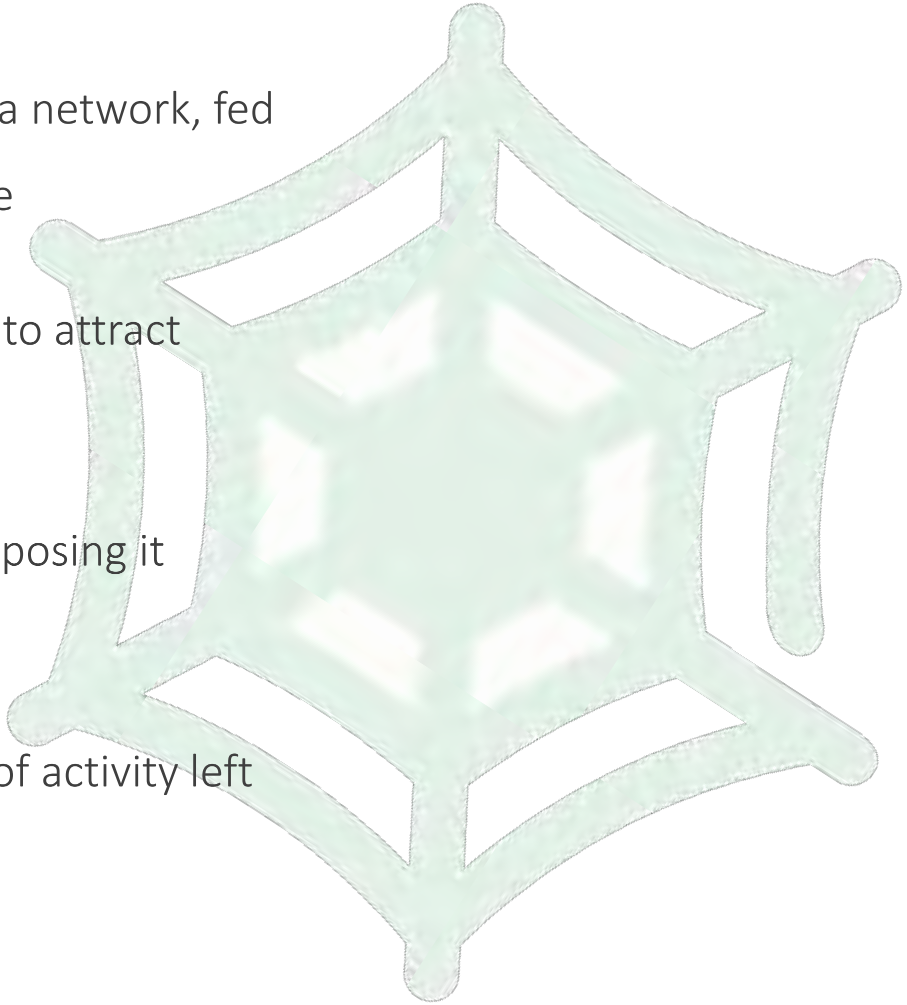
WHAT IS A NETWORK TRAP?

- Sometimes referred to as ‘honeypots’ or ‘honey traps’
- An intrusion detection technique used to study hacker movement and improve system defenses against future attacks
- Decoy endpoints distributed throughout the network that effectively lie dormant; ‘looking’ like a viable endpoint within the network
- A security resource whose value lies in being probed, attacked, or compromised
- Provides indications of intrusion if triggered/interacted with

NETWORK TRAP FUNCTION

- Divert the attention of the attacker from the real network, in a way that key information resources are not compromised
- Build attacker profiles in order to identify preferred attack methods
- Allows in-depth examination of unwelcome users during and after network trap use
- Identify new vulnerabilities and risks - including viruses/worms - to various operating systems, environments and programs and provide material for further study

NETWORK TRAP CONFIGURATION

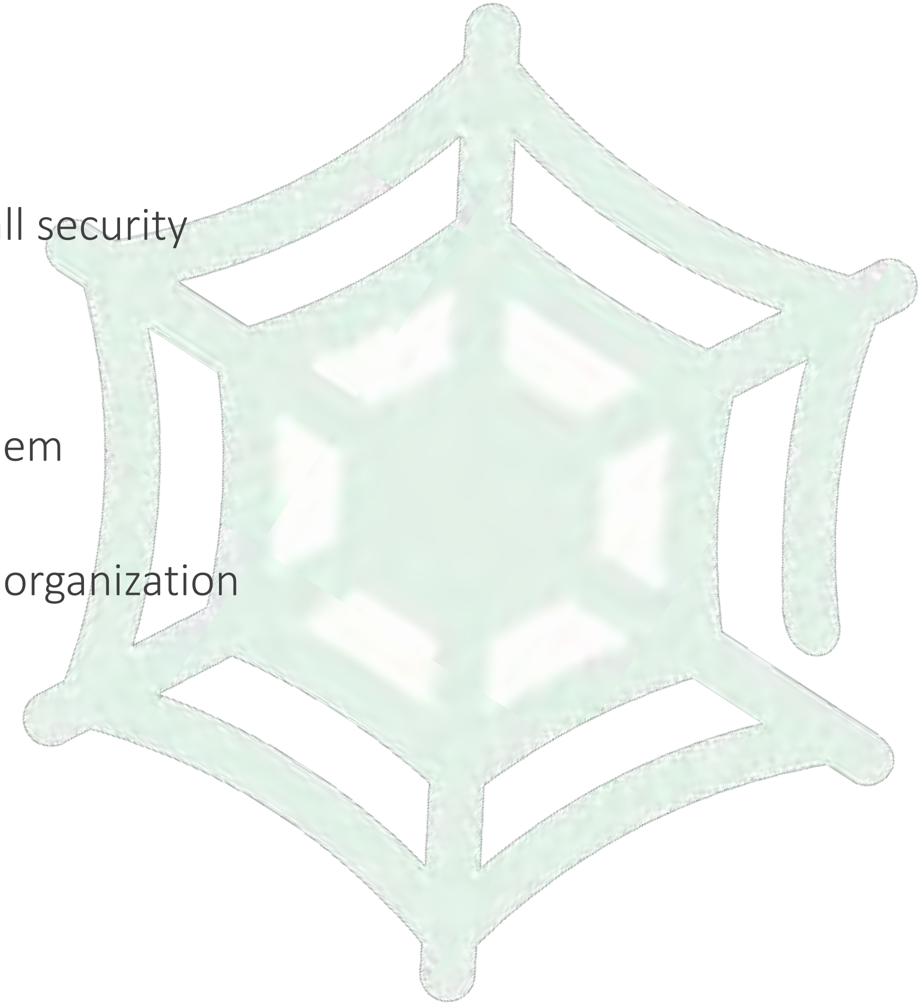


- Fake information server/ virtual machine strategically positioned within a network, fed with false information made unrecognizable as files of a classified nature
- Set up to look just like a regular system - including files and directories - to attract attackers to connect to it so that their actions can be studied
- Configured in a way that is difficult, but not impossible, to break into; exposing it deliberately to an attacker in search of an attractive target
- Loaded with monitoring and tracking tools so that every step and trace of activity left by an attacker can be captured in detail and recorded in a log

CYBOWALL NETWORK TRAP CAPABILITIES

- Enables insight into lateral movement between endpoints and can detect threats originating within the network
- Distributed deception grid slows down and stops automated attacks, such as worms or autorooters, which randomly scan the network to identify vulnerable systems
- Deters human attacks by sidetracking the attacker; leading them to devote attention to activities that cause neither harm nor loss
- Buys time for Cybowall to initiate an automated response

NETWORK TRAP WHY IT'S NOT ENOUGH?



- Does not replace security mechanisms; works with and enhances overall security architecture
- Narrow field of view; network traps only see activity directed against them
- An attacker who identifies a network trap can avoid it and infiltrate the organization

WHAT IS VULNERABILITY ASSESSMENT

- Also known as Vulnerability Analysis
- A process that defines, identifies and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure
- A search for weaknesses and exposures in order to apply a patch or fix to prevent a compromise
- Find weak spots in critical assets/endpoints and take corrective action before they can be exploited
- Obtain a prioritized list of vulnerabilities for remediation

CYBOWALL VULNERABILITY ASSESSMENT CAPABILITIES

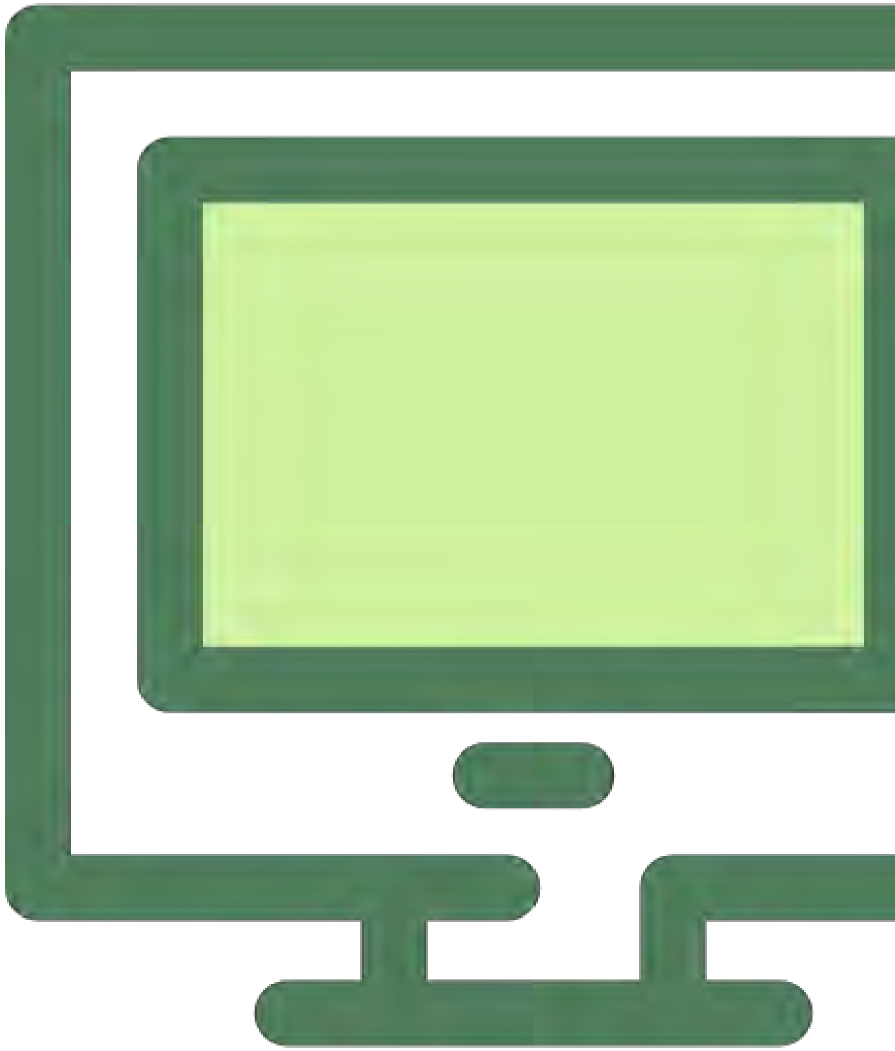
- Integrated solution encompassing asset mapping, intrusion detection, SIEM and vulnerability assessment with a single pane of glass view
- Continuously scans your network systems and devices to detect and pinpoint vulnerabilities as they arise
- Collects detailed forensic data and correlates it with the latest threat intelligence, including known Indicators of Compromise (IOC)
- Flags vulnerabilities such as; out-of-date software, unauthorized software installation, configuration errors, insecure endpoint devices

VULNERABILITY ASSESSMENT WHY IT’S NOT ENOUGH?

- In isolation, vulnerability assessment may not provide all the information required to efficiently prioritize response and mitigation actions
- Accurate testing is key and ensuring that ‘false negatives’ and ‘false positives’ do not undermine analysis
- Assessment results are dependent on the quality of data used for cross referencing
- Remediation actions, such as patch deployment, require timely implementation

WHAT IS ENDPOINT DETECTION & RESPONSE (EDR)?

- Category of tools and solutions that focus on detecting, investigating, and mitigating suspicious activities and issues on hosts and endpoints
- Gartner EDR solution capabilities:
  - Detect security incidents; monitor endpoint activities, objects and policy violations, or validate externally fed Indicators of Compromise (IOC)
  - Contain incident at the endpoint; remotely control network traffic / process execution
  - Investigate security incidents; capture history to determine technical changes and business effect
  - Remediate endpoints to pre-infection state; remove malicious files, roll-back and repair changes



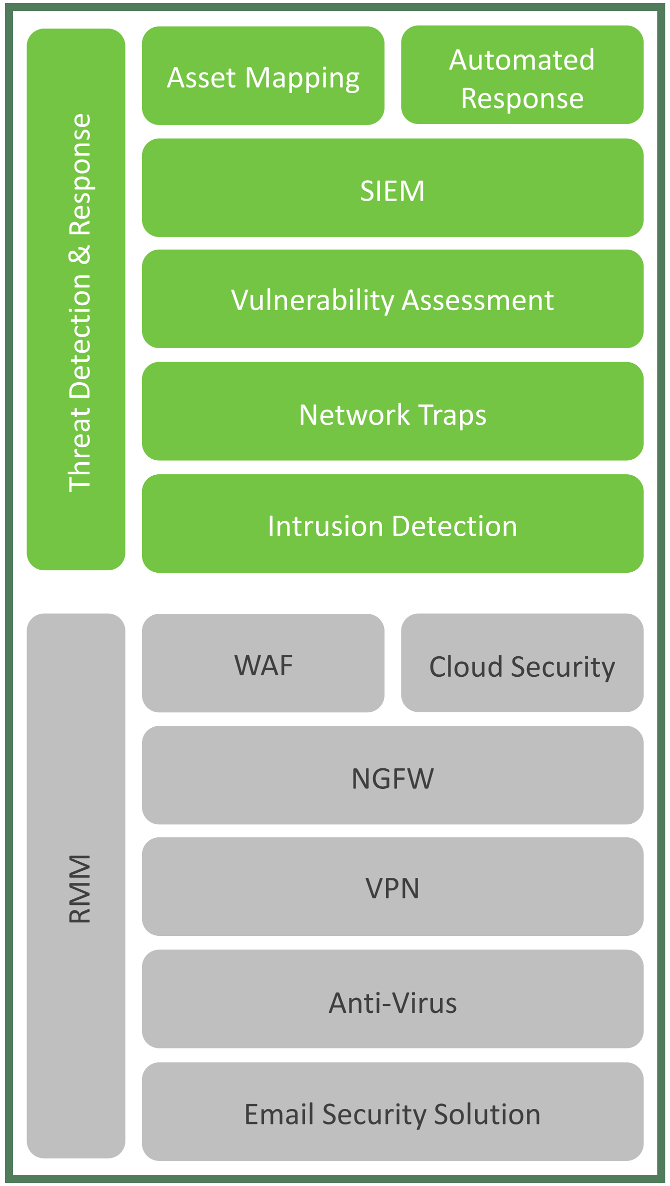
CYBOWALL EDR CAPABILITIES

- Full coverage of endpoints; desktops, laptops, servers, routers, smartphones, tablets, wired/wireless LANs, printers, IoT devices - cameras, healthcare, manufacturing, POS etc.
- Agentless: continually engages endpoints, without need for agent installation and maintenance
- Network Asset Mapping; create and manage updated list of all endpoints including port profiles and activity
- Remote management of endpoints via WMI capabilities
- Automated, policy-based remediation; email alerts, walled VLAN, shutdown port, end process or application

EDR WHY IT’S NOT ENOUGH?

- Non-traditional endpoints cannot have an agent installed, for example IP-enabled door locks
- EDR solutions perhaps ‘too much’, particularly for small and mid-sized enterprises:
  - Premium, best-of-breed solutions can be very expensive and require significant IT security staffing support
  - ‘Agent fatigue’; cost and time of installing and maintaining an agent on all endpoints

CYBONET MARKET OPPORTUNITY FOR A SINGLE SMB SOLUTION



Threat Detection & Response

Asset Mapping

Automated Response

SIEM

Vulnerability Assessment

Network Traps

Intrusion Detection

RMM

WAF

Cloud Security

NGFW

VPN

Anti-Virus

Email Security Solution

Typical Enterprise Security Stack

- Expensive
- Requires oversight by dedicated Analyst / CISO / SOC

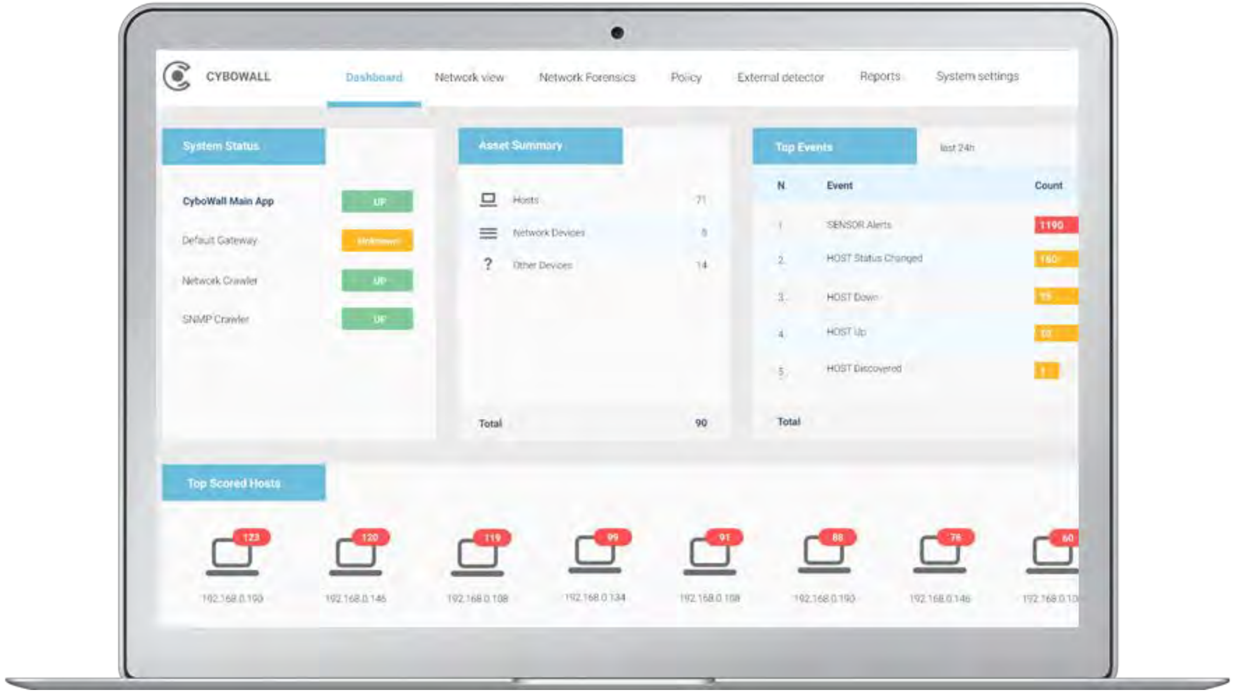
Typical SMB Security Stack

- Affordable for SMBs
- Can be managed with SMB resources

CYBONET INTRODUCES CYBOWALL

Breach Detection, Network Visibility and Vulnerability Management 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



System Status

CyboWall Main App	UP
Default Gateway	Unknown
Network Crawler	UP
SNMP Crawler	UP

Asset Summary

Hosts	71
Network Devices	5
Other Devices	14
Total	90

Top Events last 24h

N	Event	Count
1	SENSOR Alerts	1190
2	HOST Status Changed	150
3	HOST Down	[illegible]
4	HOST Up	[illegible]
5	HOST Discovered	1
Total		

Top Scored Hosts

123	192.168.0.190
120	192.168.0.146
119	192.168.0.108
99	192.168.0.134
91	192.168.0.108
88	192.168.0.190
76	192.168.0.146
60	192.168.0.10

CYBOWALL SOLUTION BENEFITS

Stop Endpoint Tampering and Malware

by leveraging network and endpoint detection

Detect Lateral Movement

to trap attackers that have already breached perimeter defenses

Map Network Assets

to increase visibility with a comprehensive endpoint map

Identify Vulnerabilities

for patch deployment prioritization

Meet Compliance Requirements

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

Automated Response

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

CYBOWALL OVERVIEW

1 Network Sensor

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

2 Network Traps

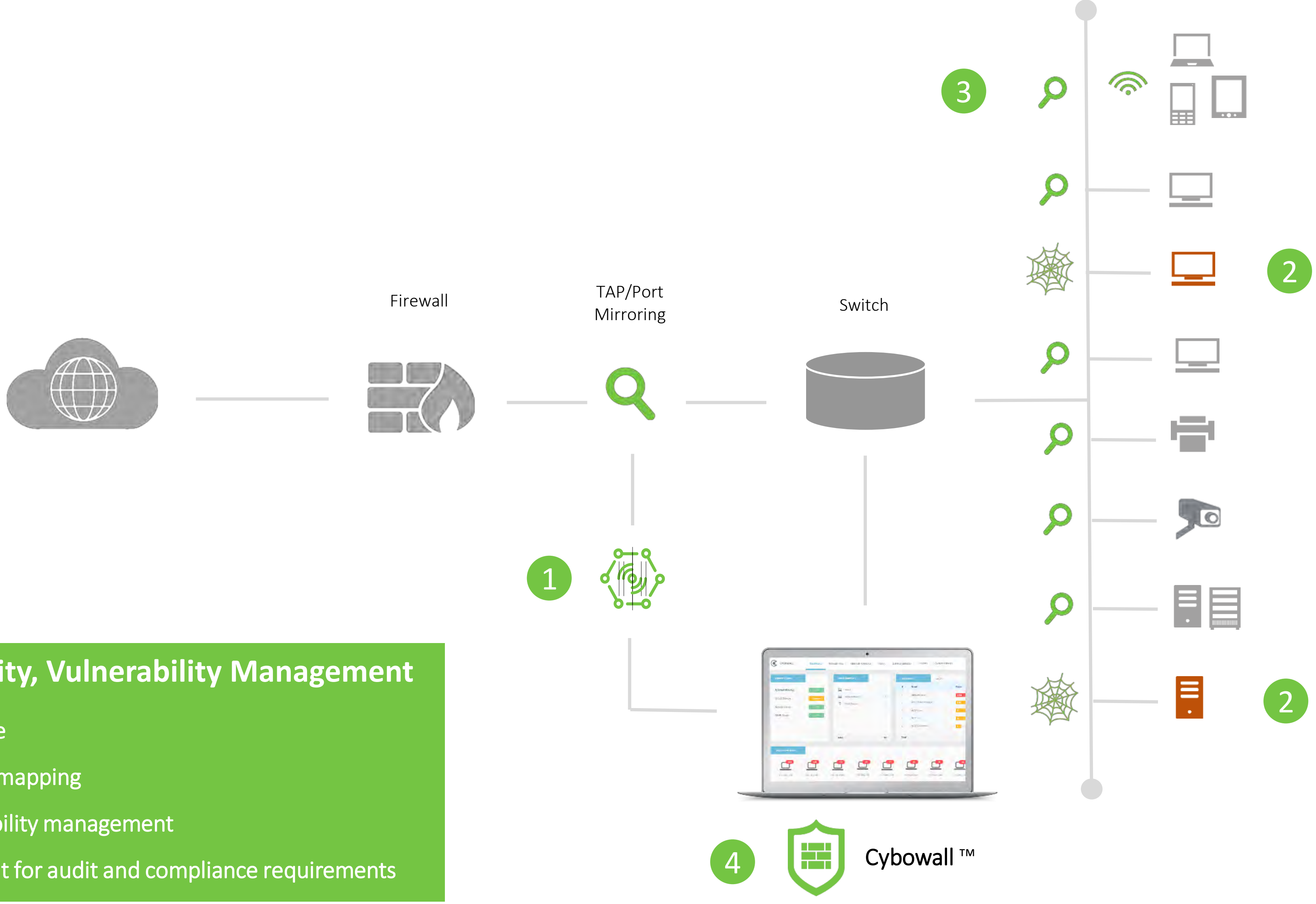
- Distributed deception grid
- Lateral movement

3 Agentless Endpoint Scan

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

4 Breach Detection, Network Visibility, Vulnerability Management

- Identify endpoint tampering and malware
- Full network visibility and dynamic asset mapping
- OS, application and service level vulnerability management
- Integrated reporting and log management for audit and compliance requirements



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

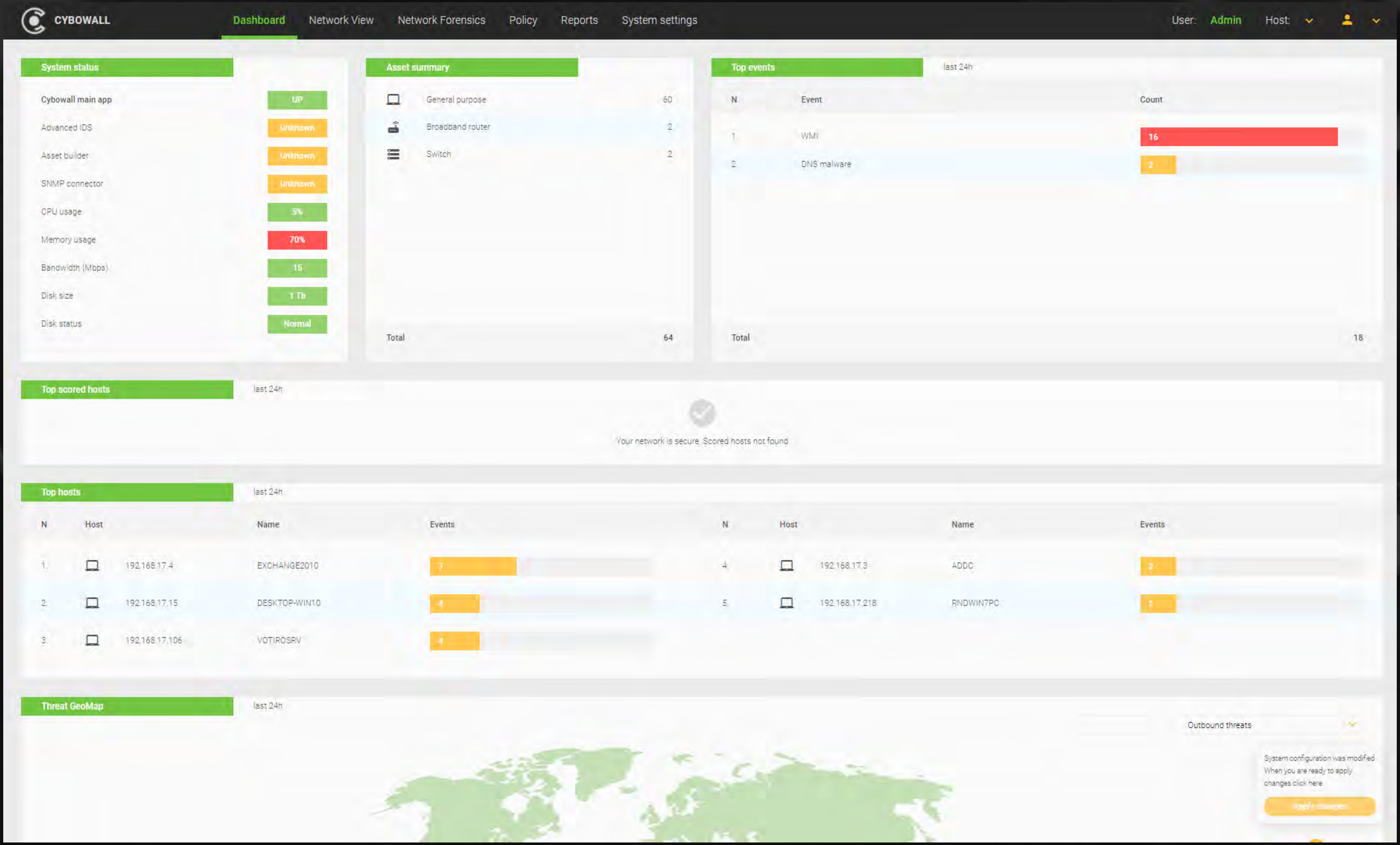
Vulnerability Assessment

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

Automated Response

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

CYBOWALL INTUITIVE MONITORING WITHOUT A CISO/SOC



System status

Cybowall main app	UP
Advanced IDS	Unknown
Asset builder	Unknown
SNMP connector	Unknown
CPU usage	5%
Memory usage	70%
Bandwidth (Mbps)	15
Disk size	1 Tb
Disk status	Normal

Asset summary

General purpose	60
Broadband router	2
Switch	2
Total	64

Top events last 24h

N	Event	Count
1.	WMI	16
2.	DNS malware	2
Total		18

Top scored hosts last 24h

Your network is secure. Scored hosts not found

Top hosts last 24h

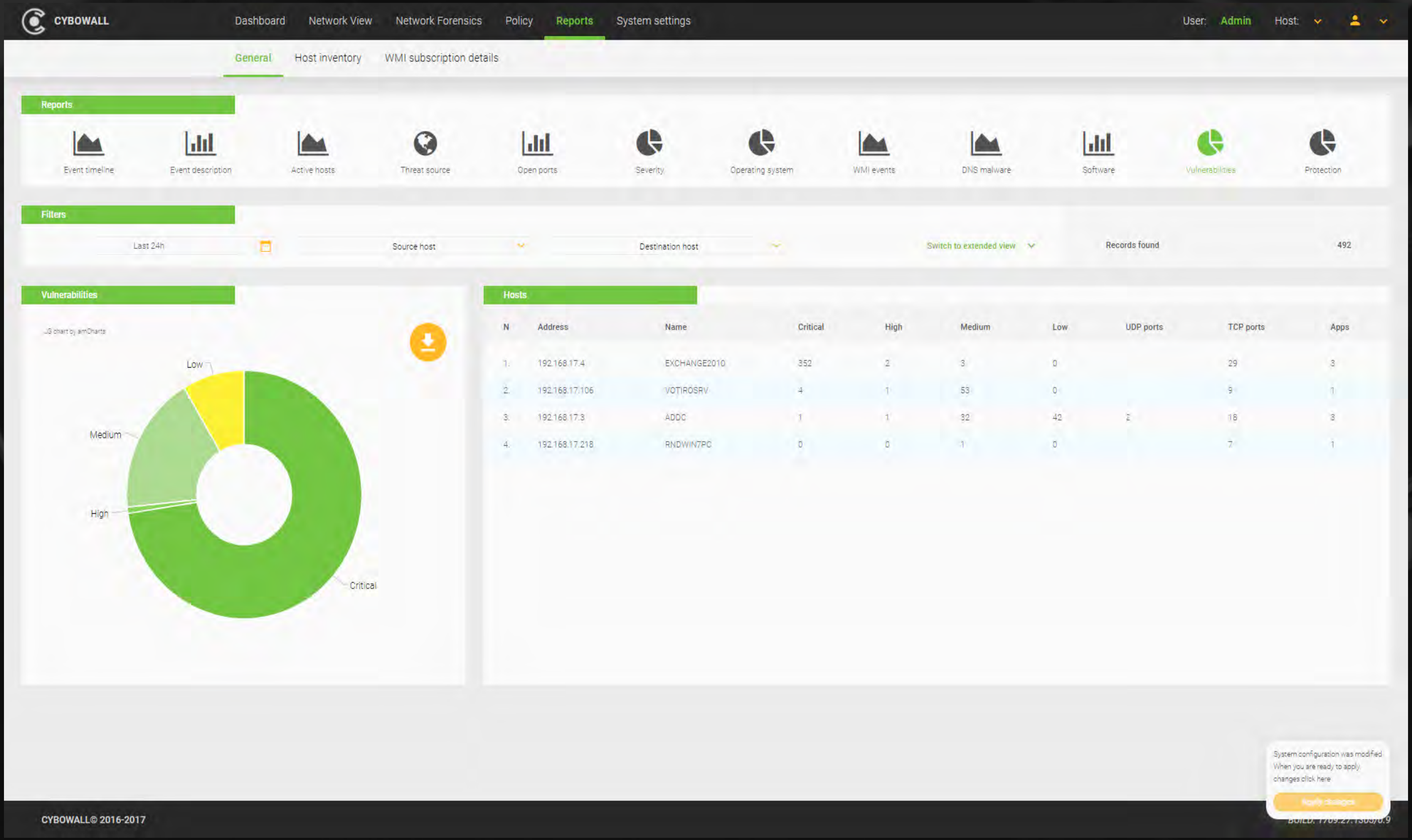
N	Host	Name	Events
1.	192.168.17.4	EXCHANGE2010	7
2.	192.168.17.15	DESKTOP-WIN10	4
3.	192.168.17.106	VOTIROSRV	4
4.	192.168.17.3	ADDC	2
5.	192.168.17.218	RNDWIN7PC	1

Threat GeoMap last 24h

Outbound threats

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

CYBOWALL IDENTIFY VULNERABILITIES



Last 24h | Source host | Destination host | Switch to extended view

Records found 492

N	Address	Name	Critical	High	Medium	Low	UDP ports	TCP ports	Apps
1.	192.168.17.4	EXCHANGE2010	352	2	3	0		29	3
2.	192.168.17.106	VOTIROSRV	4	1	53	0		9	1
3.	192.168.17.3	ADDC	1	1	32	42	2	18	3
4.	192.168.17.218	RNDWIN7PC	0	0	1	0		7	1

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

CYBOWALL© 2016-2017

BUILD: 1709.27.1305/0.9

CYBOWALL PRICING AND LICENSING

SYSTEM LICENSE

One time system license fee for initial Cybowall installation

ENDPOINT PRICING

Priced per endpoint with standard cost for all endpoint types including workstations, servers etc.

SOLUTION SUPPORT

Working hours support is included within endpoint price

RENEWAL

Renewal fee based on number of endpoints with support

CYBOWALL PRICING (EUR)

	Tier 1 # of Endpoints	Tier 2 # of Endpoints	Tier 3 # of Endpoints	Tier 4 # of Endpoints	Tier 5 # of Endpoints	Tier 6 # of Endpoints
	100	101 - 250	251 - 500	501 - 750	751 - 1000	1001+
System License	€ 4,217	€ 4,217	€ 4,217	€ 4,217	€ 4,217	€ 4,217
Per Endpoint Per Year 1Y + Support	€ 59	€ 50	€ 38	€ 34	€ 30	€ 17
Per Endpoint - 1Y Renewal + Support	€ 59	€ 50	€ 38	€ 34	€ 30	€ 17
Per Endpoint - 2Y Renewal + Support	€ 100	€ 85	€ 65	€ 58	€ 51	€ 29
Per Endpoint - 3Y Renewal + Support	€ 133	€ 113	€ 86	€ 77	€ 68	€ 38

GETTING STARTED QUESTIONS

- **Estimated total number of endpoints?**
  Includes printers, servers, workstations etc. Estimates are more than sufficient
- **Total number of networks?**
  Please include all VLANS etc.
- **Make and model of core switch?**
  Please include as much detail as possible
- **Access and/or ability to enable port mirroring?**
- **Percentage of workstations and servers that run a Microsoft OS?**
  Estimates are more than sufficient
- **Do you have access and/or the ability to manage WMI access?**