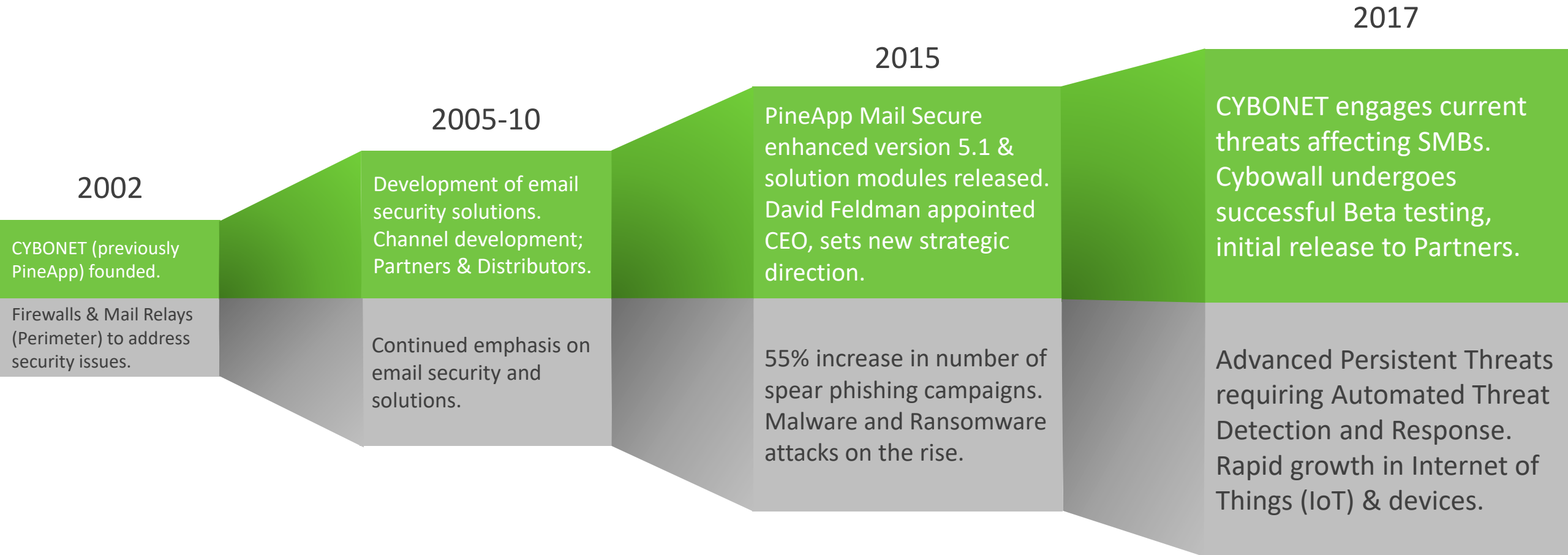


Cybowall Solution Overview

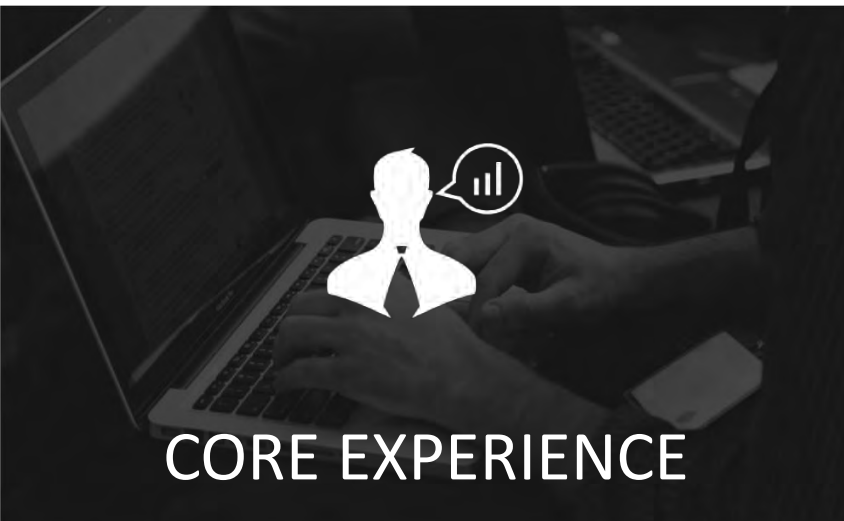


CYBONET OUR HISTORY



Our History reflects the Evolution of Cybersecurity

ABOUT CYBONET



- © 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

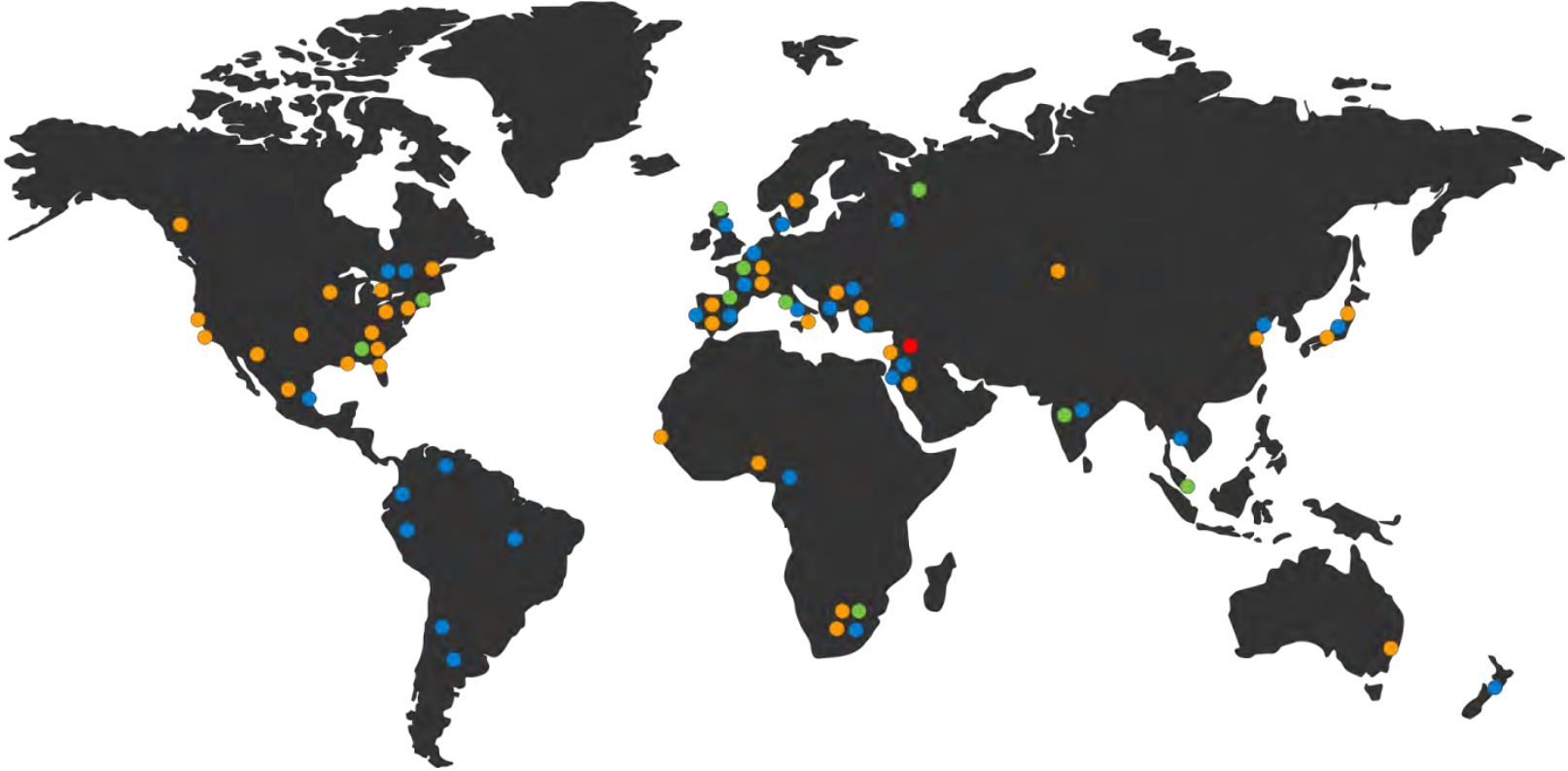


- © Cybowall:
 - Advanced Threat Detection
- © PineApp Mail Secure:
 - Advanced Messaging Solution
- © CyboCloud:
 - Cloud Messaging Solution
- © Outbound Spam Guard (OSG):
 - IP Blacklisting Prevention for Telecoms



- © 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

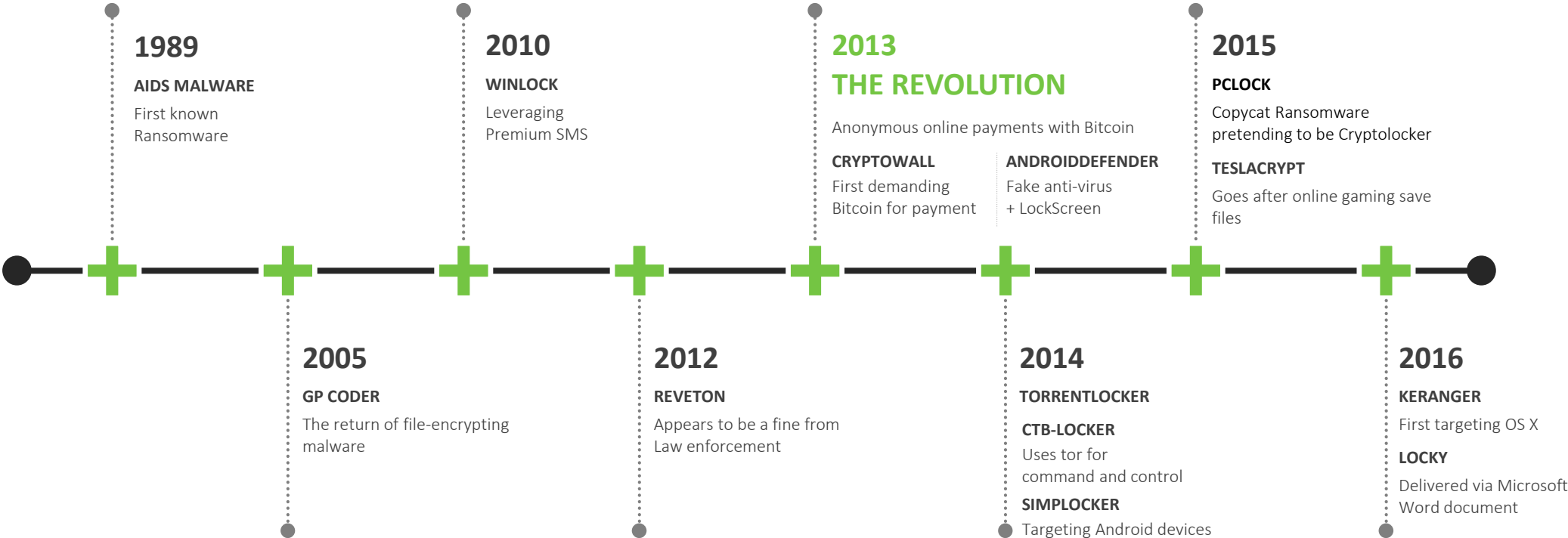
OUR LARGER INTERNATIONAL CLIENTS



SPAM PHISHING MALWARE RANSOMWARE

THE RISE OF RANSOMWARE

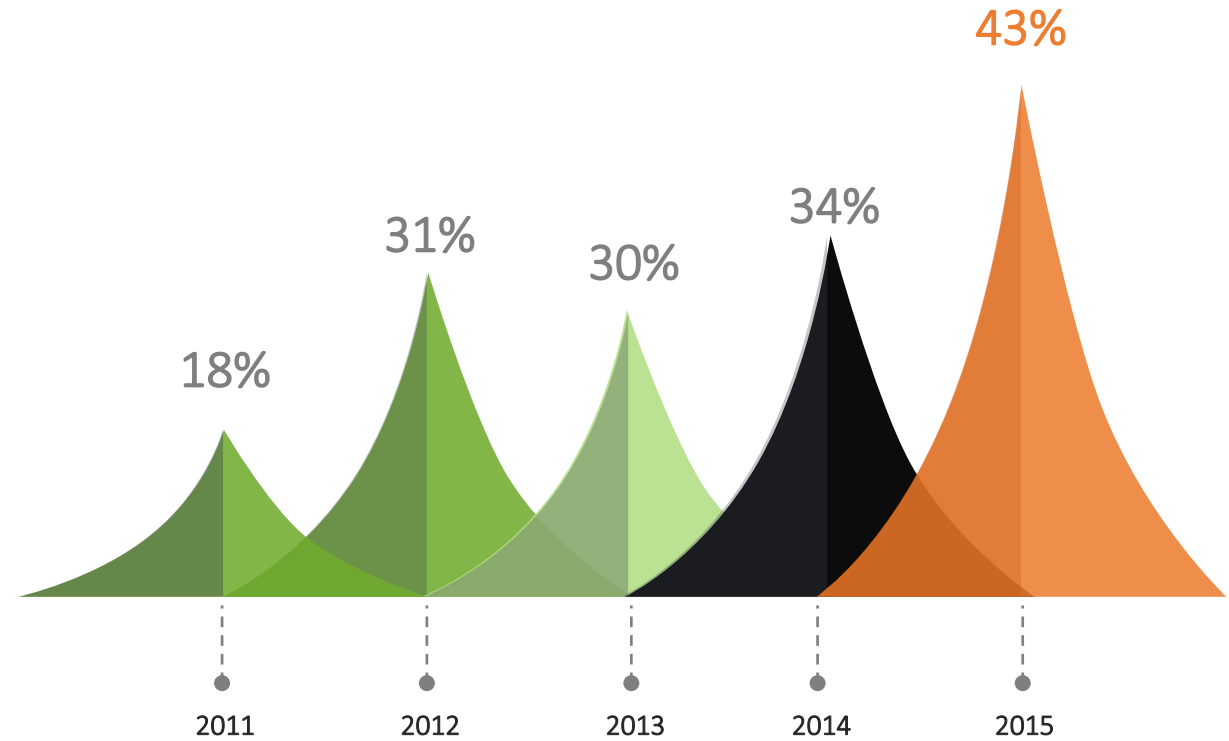
30 ACTIVE MALWARE FAMILIES



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

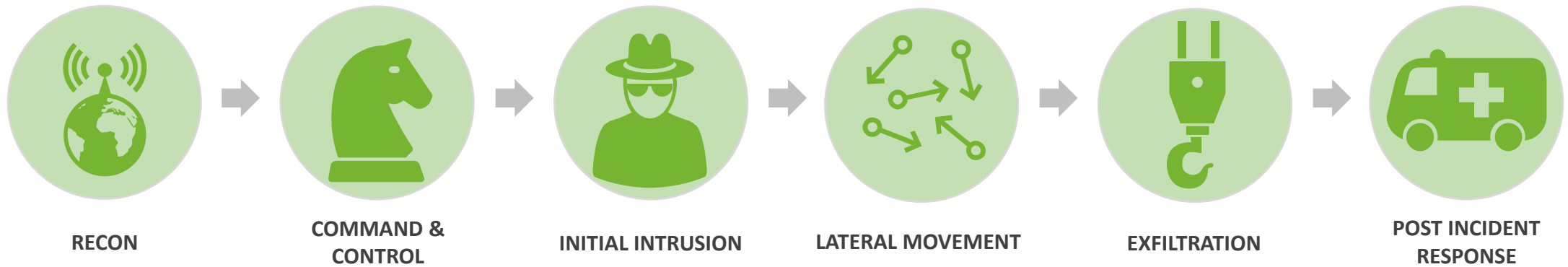
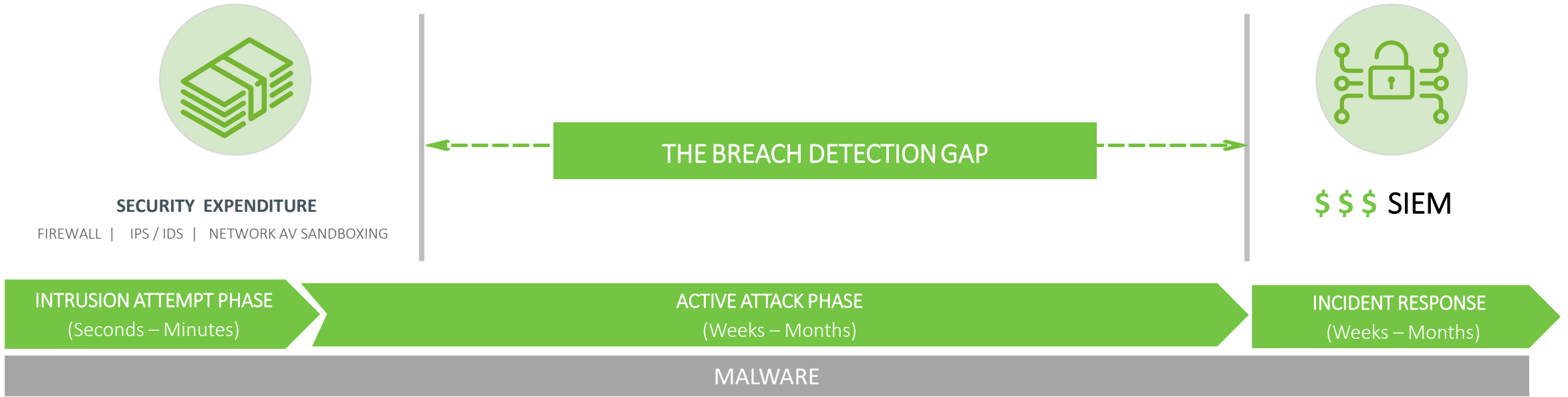
8 out of 10 SMBs don't have a basic cyber attack response plan



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



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

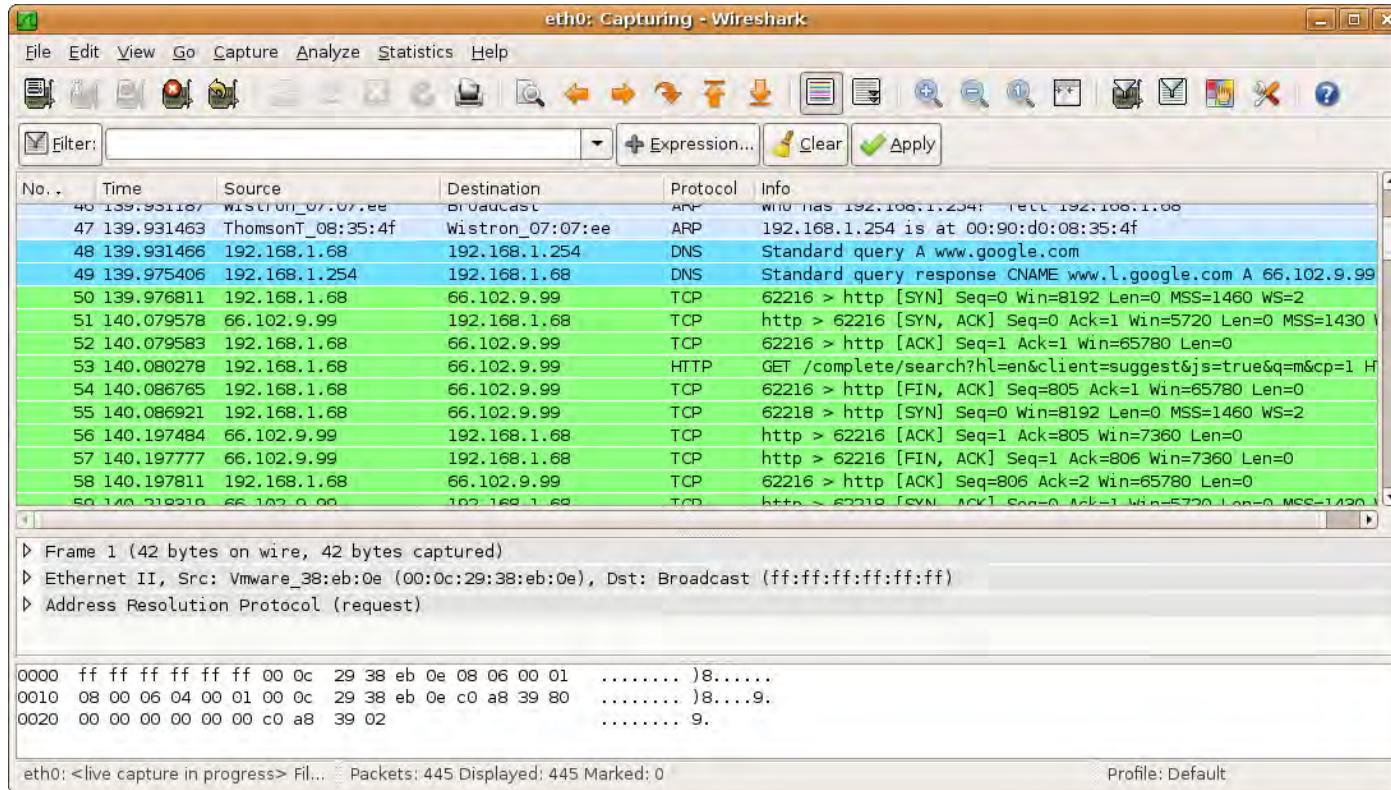


WHAT IS AN INTRUSION DETECTION SYSTEM (IDS)?

- 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)?

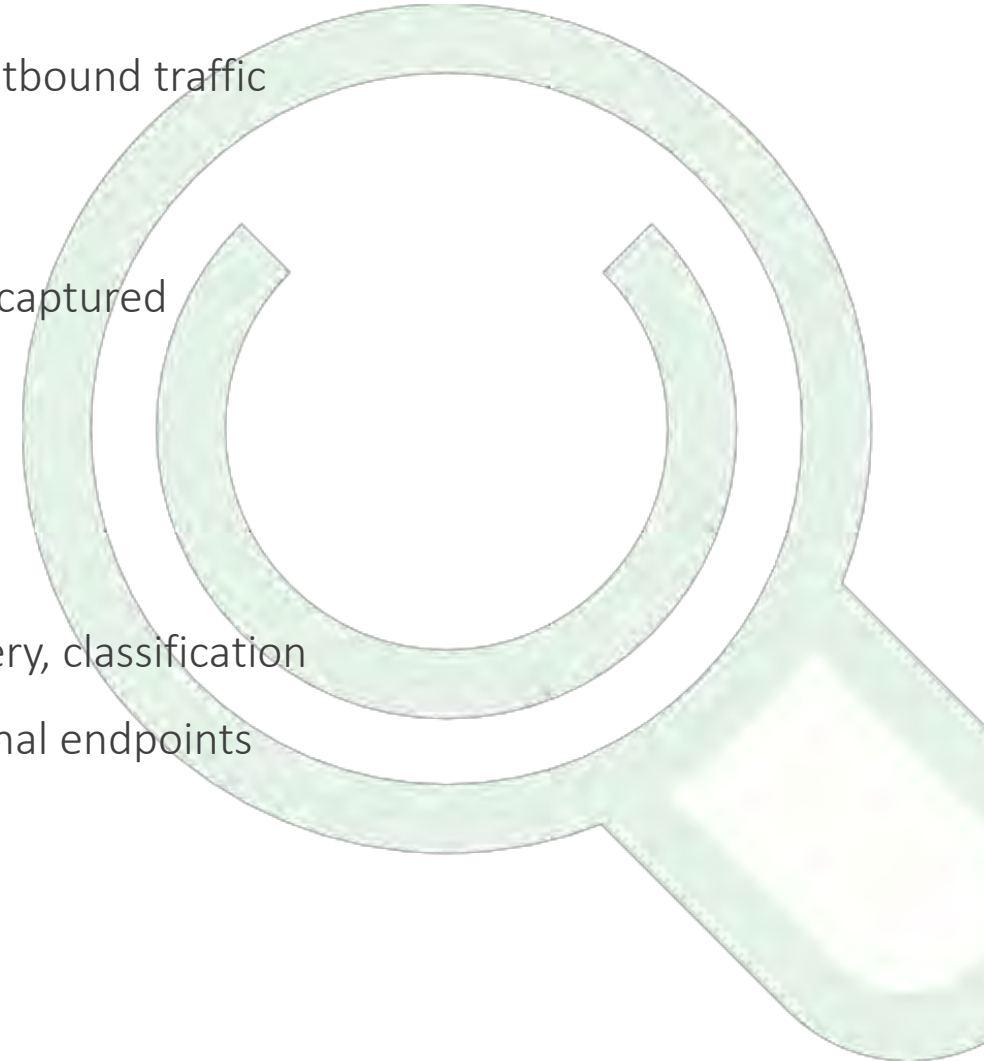


Classtype	Description
attempted-admin	Attempted Administrator Privilege Gain
attempted-user	Attempted User Privilege Gain
inappropriate-content	Inappropriate Content was Detected
policy-violation	Potential Corporate Privacy Violation
shellcode-detect	Executable code was detected
successful-admin	Successful 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



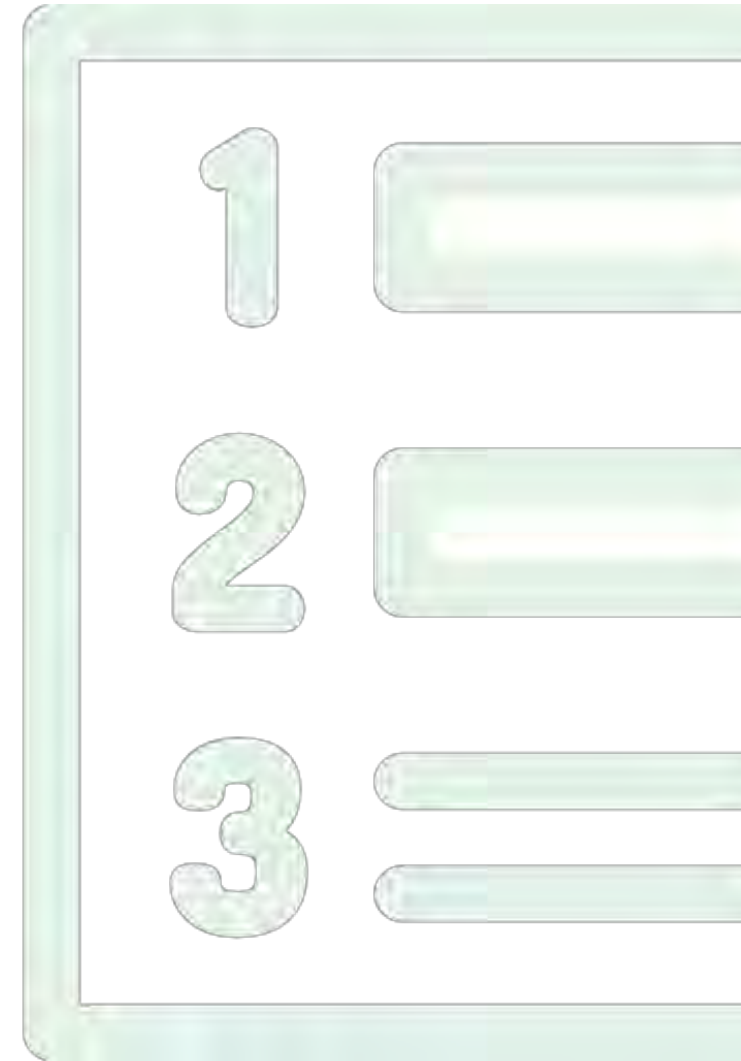
WHAT IS SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)?

- 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



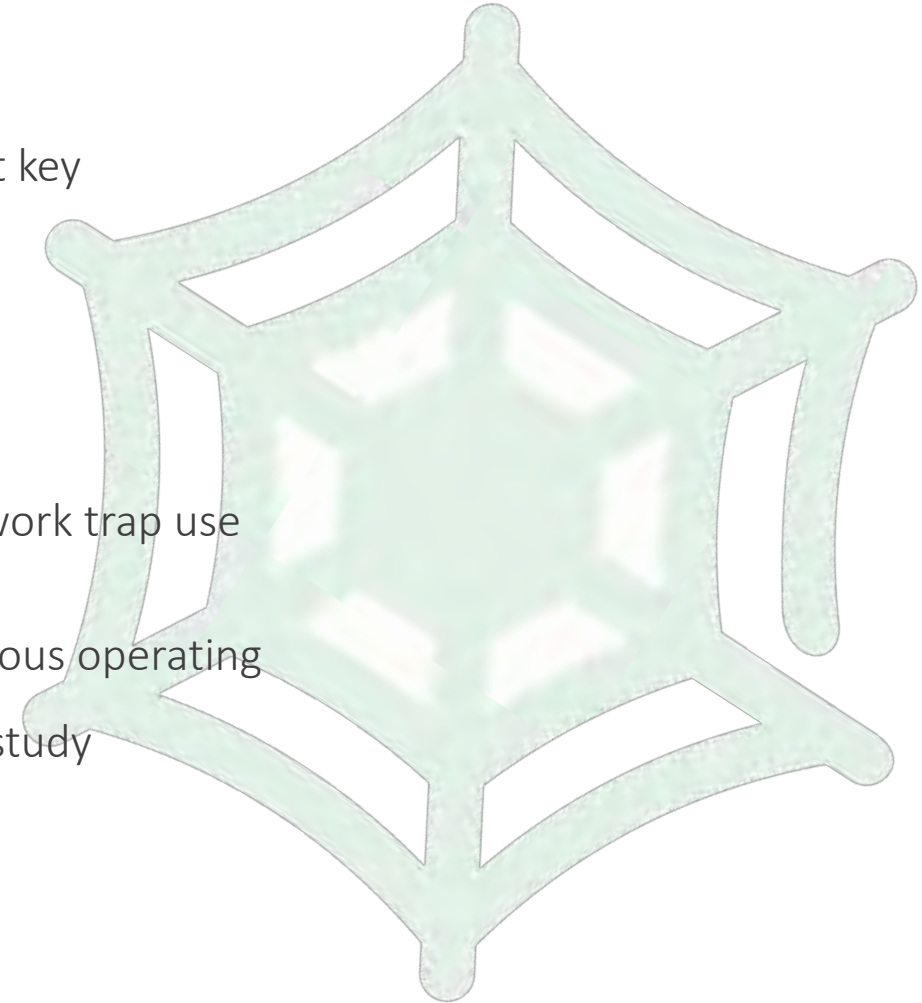
WHAT IS A NETWORK TRAP?

- 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



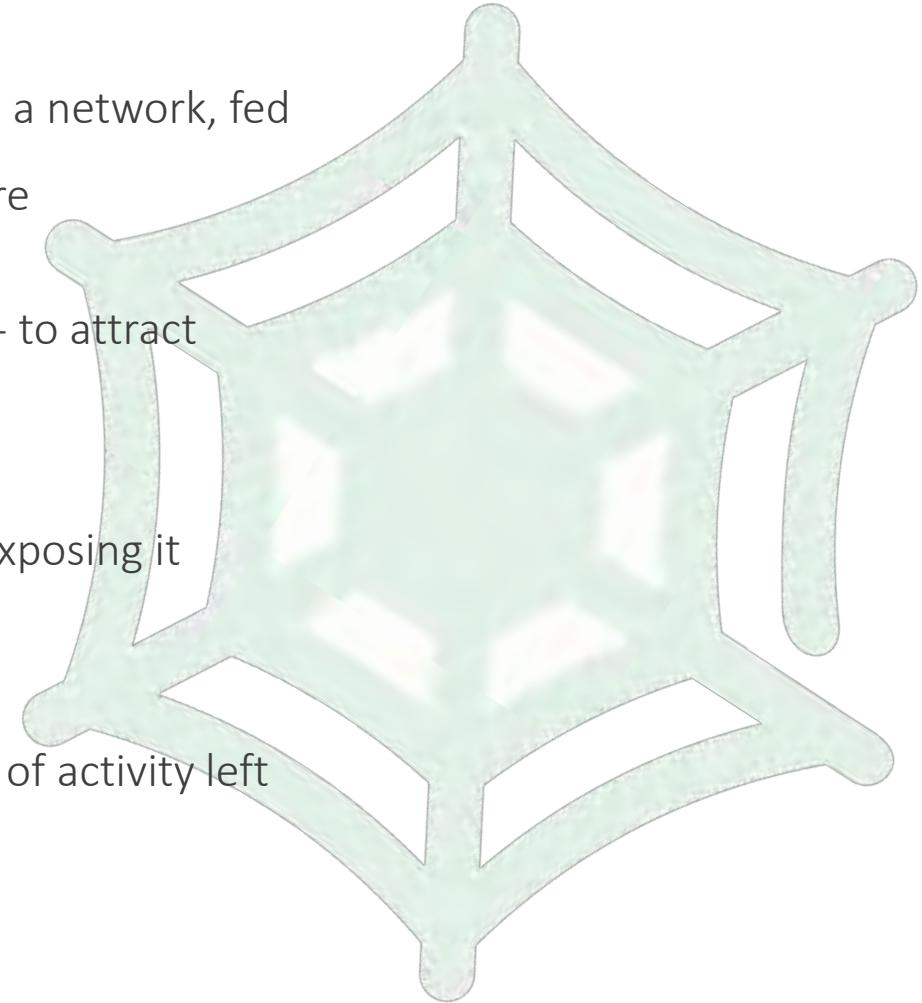
NETWORK TRAP FUNCTION

- 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



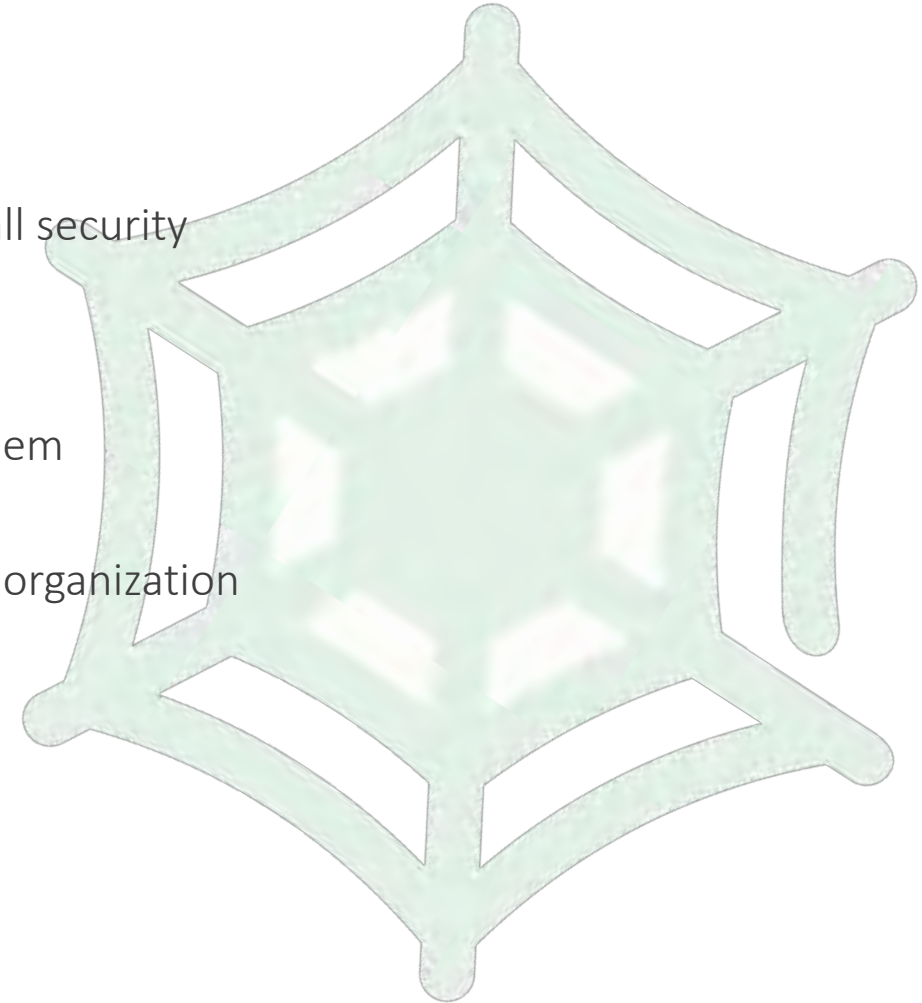
CYBOWALL NETWORK TRAP CAPABILITIES

- 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



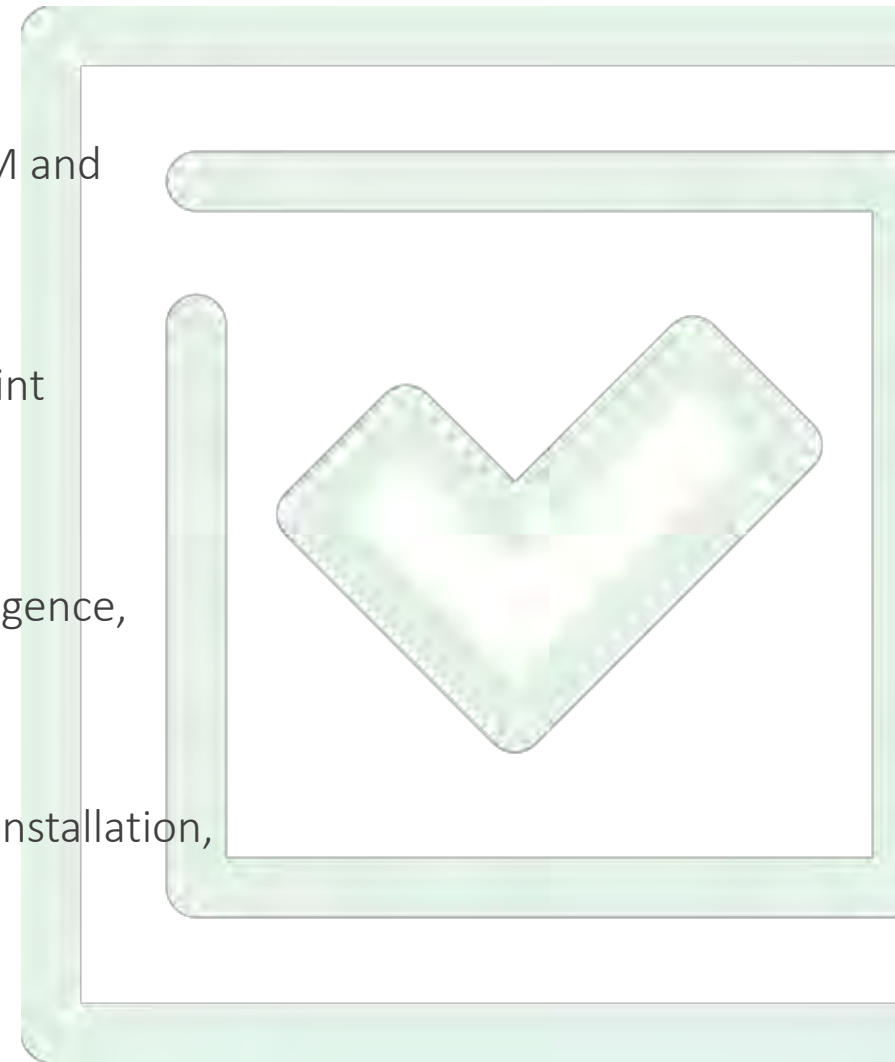
WHAT IS VULNERABILITY ASSESSMENT

- 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



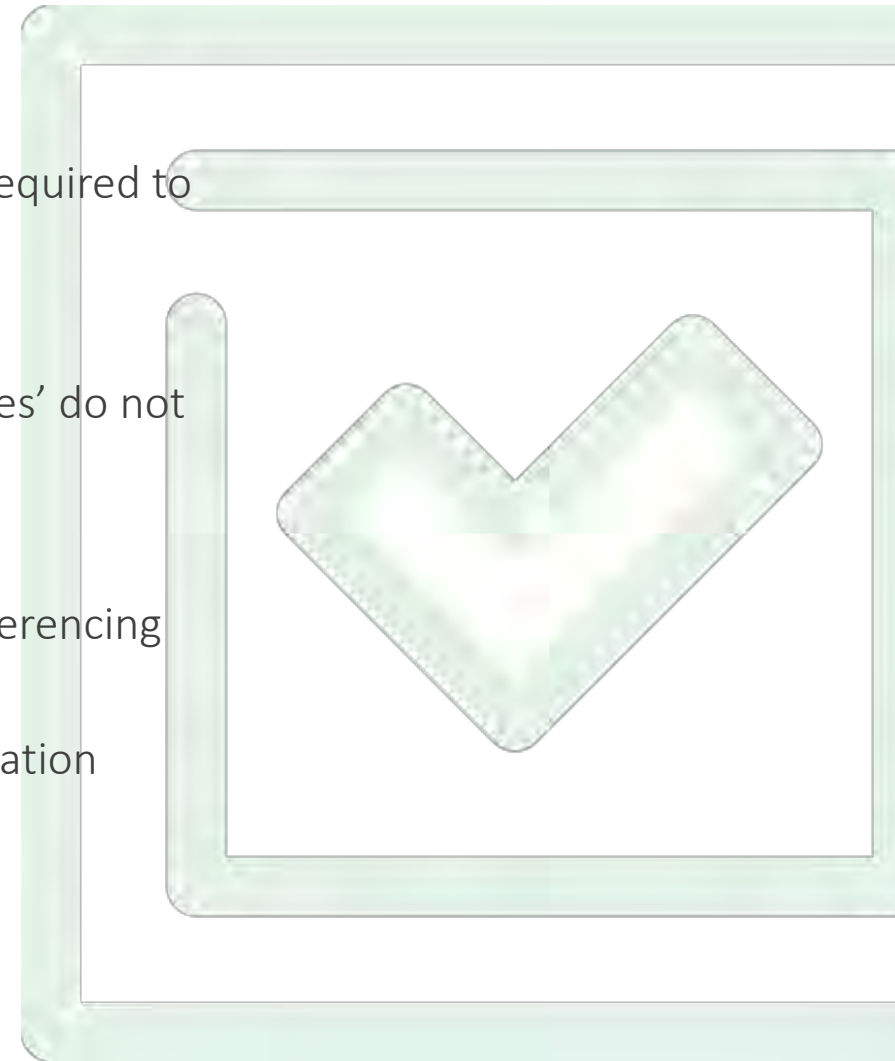
CYBOWALL VULNERABILITY ASSESSMENT CAPABILITIES

- 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



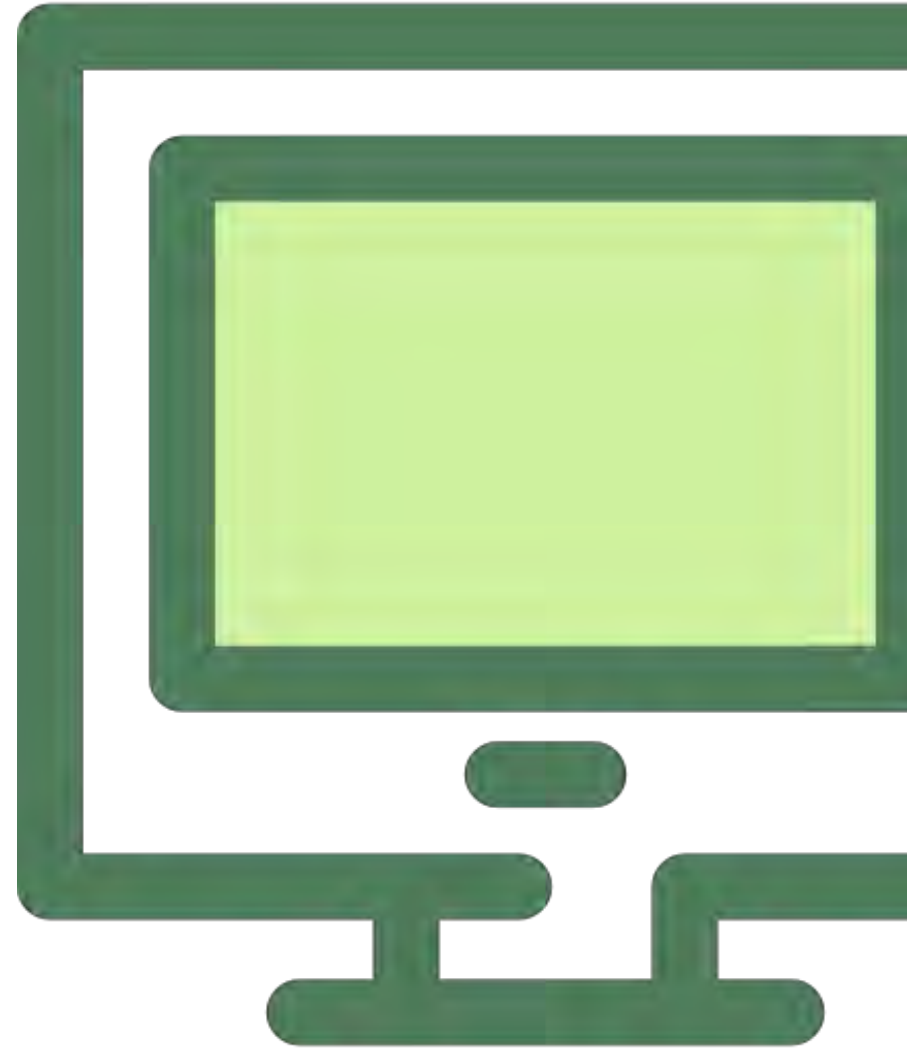
VULNERABILITY ASSESSMENT WHY IT'S NOT ENOUGH?

- 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



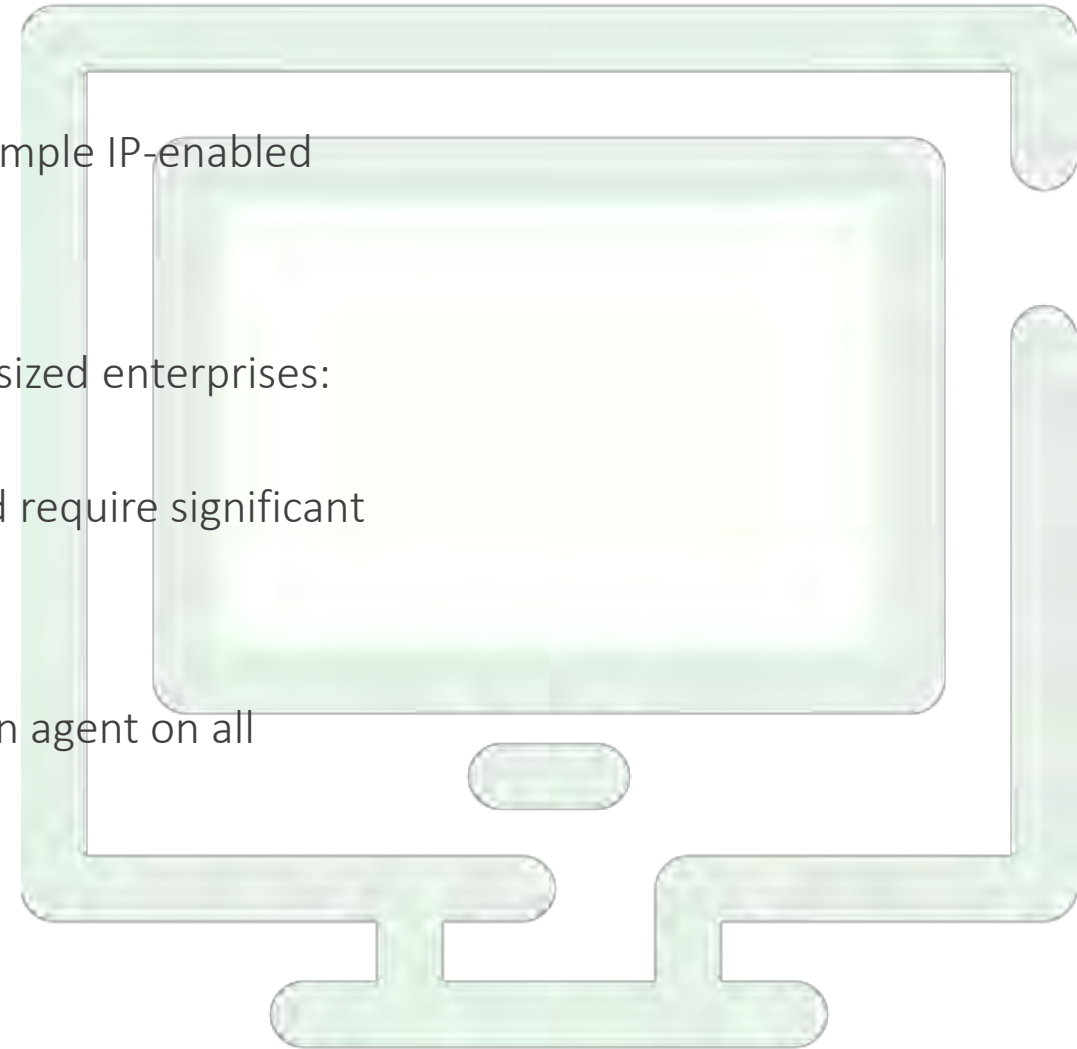
CYBOWALL EDR CAPABILITIES

- 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

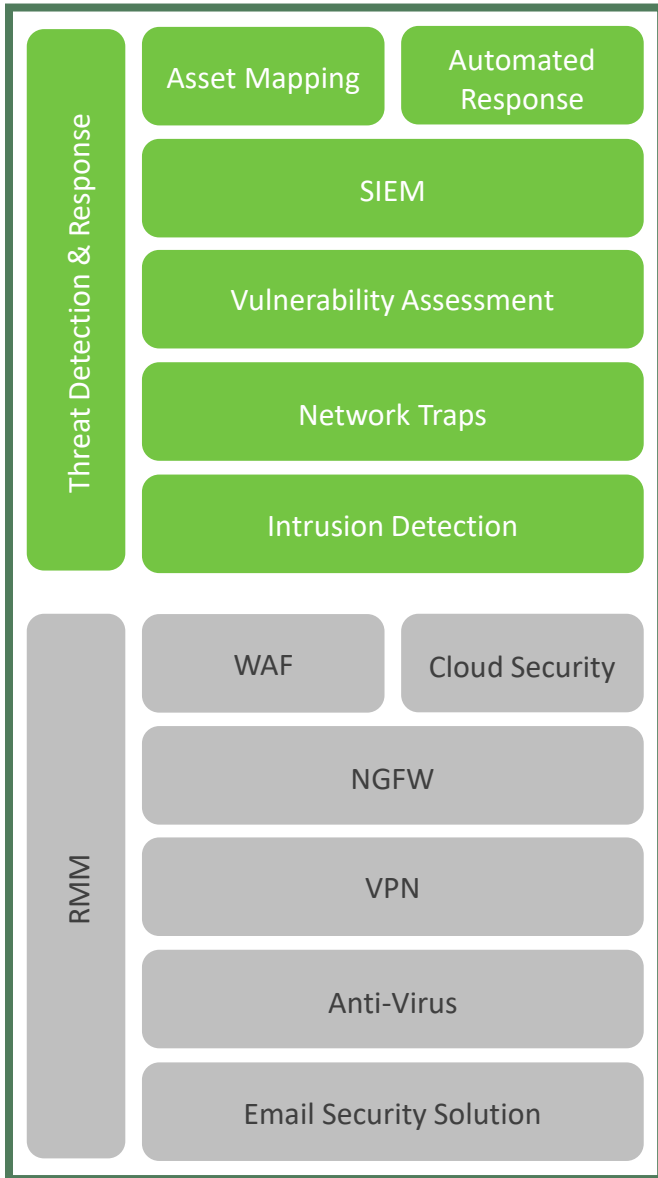


EDR WHY IT'S NOT ENOUGH?

- 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

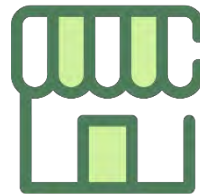


Typical Enterprise Security Stack



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

Typical SMB Security Stack

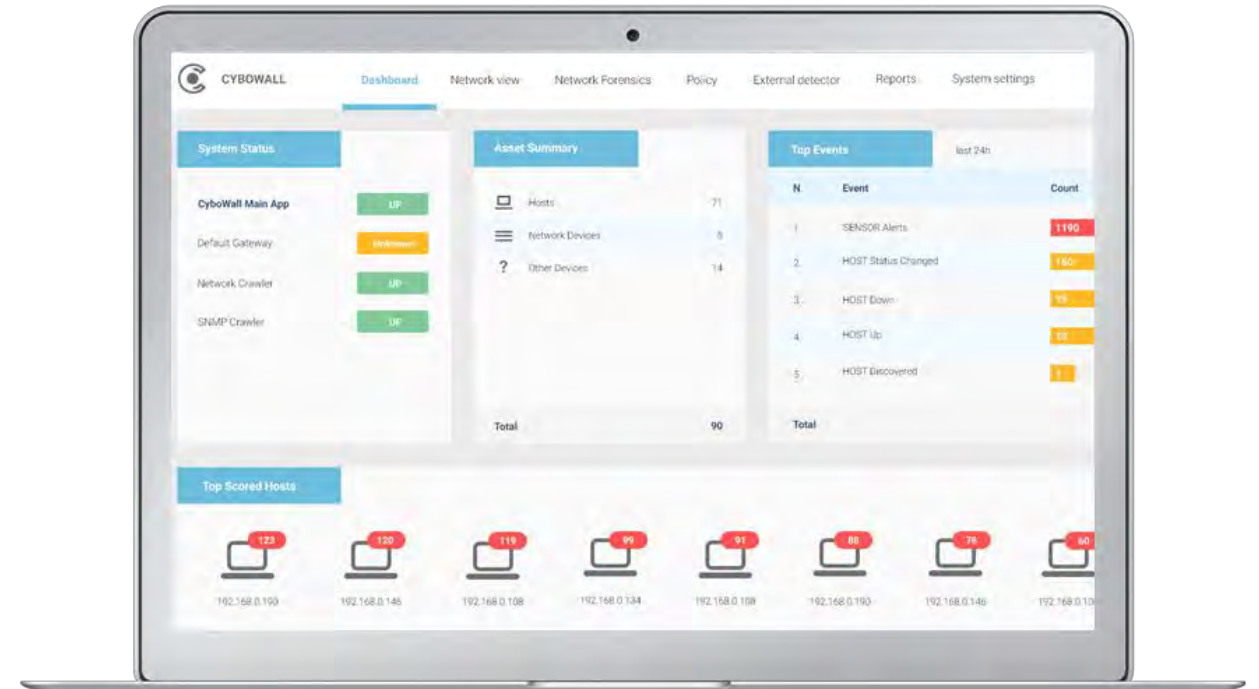


- Affordable for SMBs
- Can be managed with SMB resources

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



CYBOWALL SOLUTION BENEFITS



CYBOWALL OVERVIEW

1 Network Sensor

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

2 Network Traps

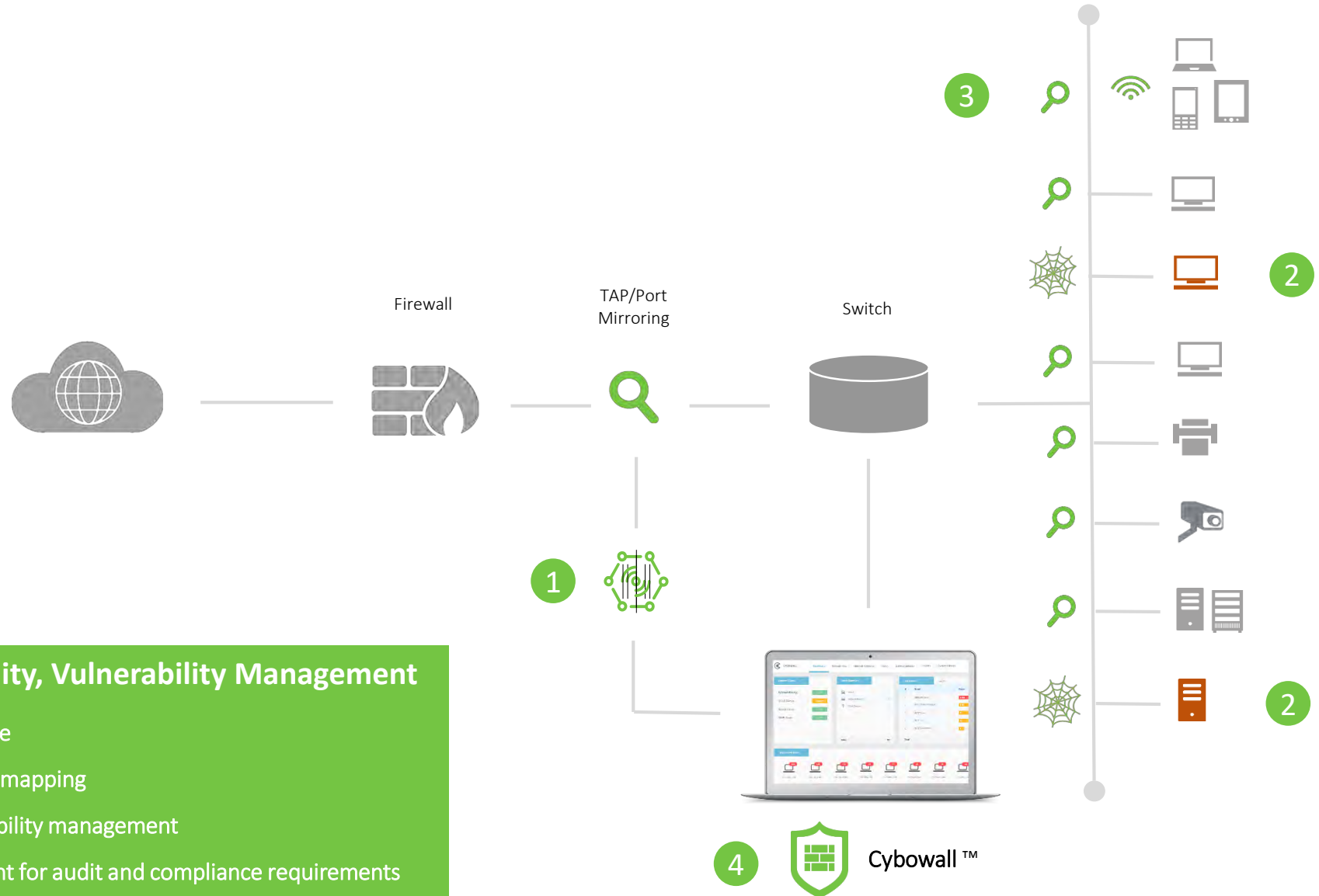
- Distributed deception grid
- Lateral movement

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

The dashboard provides a comprehensive overview of the network's security and performance. It is organized into several key sections:

- System status:** Displays the health of various components. The main app is UP, while Advanced IDS, Asset builder, and SNMP connector are in an Unknown state. Resource usage is shown as CPU (5%), Memory (70%), Bandwidth (15), and Disk size (1 Tb). Disk status is Normal.
- Asset summary:** Lists network assets such as General purpose (60), Broadband router (2), and Switch (2), with a total of 64 assets.
- Top events:** Shows the most frequent events in the last 24 hours, including WMI (16) and DNS malware (2), with a total of 18 events.
- Top scored hosts:** A message indicates that the network is secure and no scored hosts were found.
- Top hosts:** Lists the hosts with the most events, including EXCHANGE2010 (7), DESKTOP-WIN10 (4), VOTIROSrv (4), ADDC (2), and RNDWIN7PC (1).
- Threat GeoMap:** A world map showing the geographic distribution of threats.

The interface includes a navigation menu (Dashboard, Network View, Network Forensics, Policy, Reports, System settings) and user information (User: Admin, Host: [dropdown]). A notification at the bottom right states: "System configuration was modified. When you are ready to apply changes click here." with an "Apply changes" button.

CYBOWALL IDENTIFY VULNERABILITIES

The screenshot displays the CYBOWALL interface, specifically the Reports section. The top navigation bar includes 'Dashboard', 'Network View', 'Network Forensics', 'Policy', 'Reports', and 'System settings'. The user is logged in as 'Admin'.

The 'Reports' section features a grid of icons for various reports: Event timeline, Event description, Active hosts, Threat source, Open ports, Severity, Operating system, WMI events, DNS malware, Software, Vulnerabilities (highlighted), and Protection.

The 'Filters' section shows a time range of 'Last 24h', source and destination host dropdowns, a 'Switch to extended view' button, and a 'Records found' count of 492.

The 'Vulnerabilities' section contains a donut chart showing the distribution of vulnerabilities by severity: Low (yellow), Medium (light green), High (dark green), and Critical (bright green).

The 'Hosts' section displays a table with the following data:

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

A notification in the bottom right corner states: 'System configuration was modified. When you are ready to apply changes click here.' with a 'Apply changes' button.

Footer text: 'CYBOWALL © 2016-2017' and 'BUILD: 17.05.22.130520.9'.

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

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?