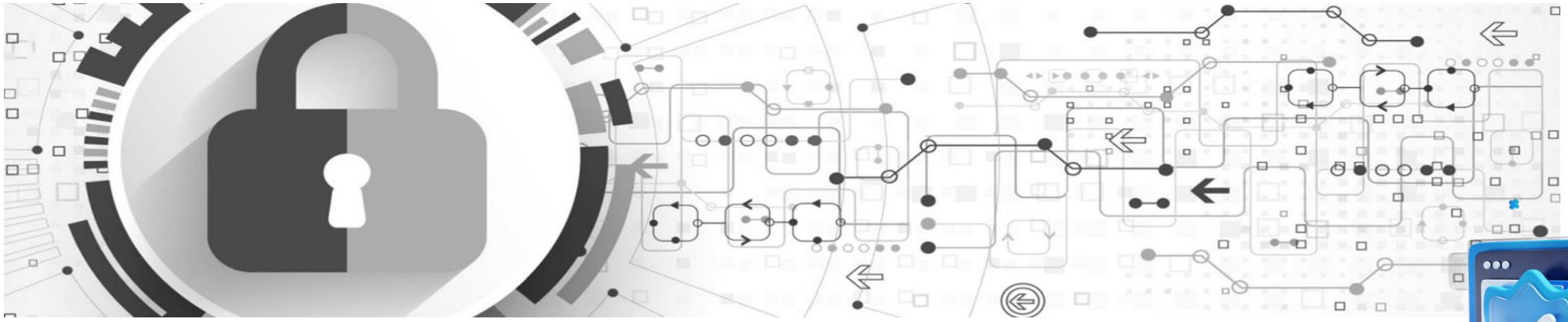
Application Data Security

https://www.deltadatamandiri.com

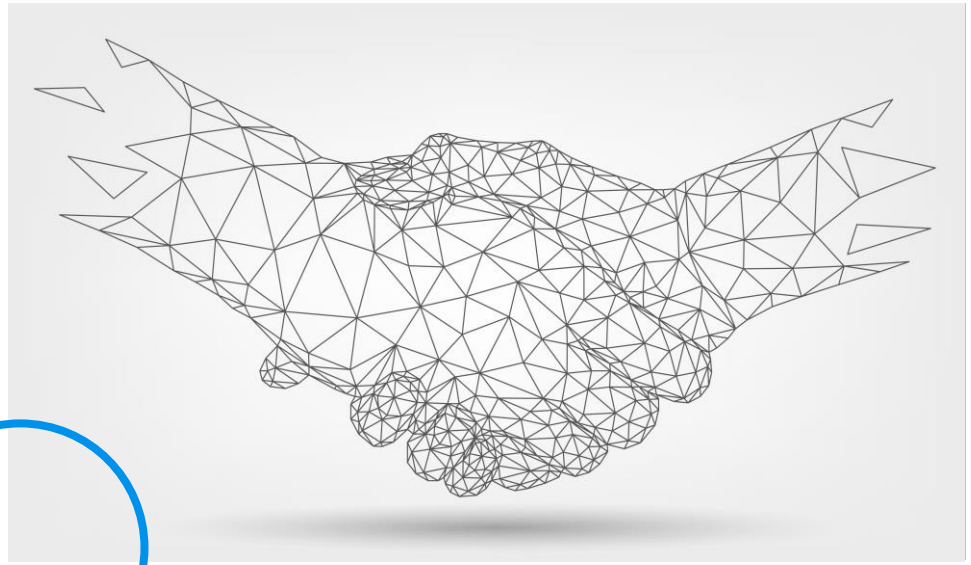


# UNIFIED AND SIMPLIFIED YOUR CSIRT

Active Extended Network Detection And Response (Active XDR) to protect enterprise network and endpoints

deltadata mandiri

Explore →



# Who We Are ?

### About Deltadata Mandiri

Deltadata is the fastest enterprise digital transformation implementation partner, consulting, and service company that provides effective digital transformation leveraging latest advanced technologies and extraordinary talents to help client enabling digital transformation FAST and SECURED.

### About Fidelis Cyber Security

Fidelis Cybersecurity is the industry innovator in Active XDR enabling proactive cyber defense and defense-in-depth. We help safeguard your data, assets, and services – no matter where they are on your networks.

# Risk We Are Facing

### Individual

Photo
Credit card details
Bank account details
Personal Identifiable information
Social media accounts
Primary email
Bitcoin wallet
Browser history
Secret files
Password information
Financial records

### Organization

Intellectual property
Source code repository
Spreadsheets
Office documents
Business process
Designs
Customer database
Confidential data

### Service

Cloud native
API gateway
External Vendor
File sharing
Devops

### Application

Broken access control
Cryptographic Failures
Injection vulnerabilities
Security Misconfiguration
Vulnerable and Outdated Components
Software and Data Integrity Failures
Server-side Request Forgery
Broken Object Level Authorization

# After Investments made on Cybersecurity Infrastructure

**Ever wondered why your Security Infrastructure only gives you alerts and logs but not what exactly happens**

On-Prem, Cloud and Hybrid

## WEB STACK

| | |
|---|---|
| Symantec, DIGITAL GUARDIAN, FORCEPOINT | Content Analysis and DLP |
| FireEye | Sandboxing |
| FireEye, Symantec, McAfee | Advanced Malware Detection |
| zscaler, cisco, McAfee, Symantec, FORCEPOINT | Secure Web Gateway |
| Symantec, McAfee | Web Proxy |

## NETWORK STACK

| | |
|---|---|
| TANIUM, NMAP, solarwinds, armis | Asset Classification |
| Symantec, FORCEPOINT, McAfee, DIGITAL GUARDIAN | Content Analysis & DLP |
| cisco | Sandboxing |
| paloalto networks, cisco, TREND MICRO, McAfee, Symantec | Advanced Malware Detection |
| f5, A10, Symantec | TLS Decryption |
| Check Point, paloalto networks, FORTINET, JUNIPER | Firewalls / IPS |

## INTERGRATION STACK

SIEM

SOAR

## E-MAIL STACK

| | |
|---|---|
| Content Analysis and DLP | Symantec, DIGITAL GUARDIAN, FORCEPOINT |
| Sandboxing | FireEye |
| Advanced Malware Detection | FireEye, Symantec, McAfee |
| Secure E-mail Gateway | cisco, Microsoft, proofpoint. |
| Exchange | Microsoft |

## ENDPOINT STACK

| | |
|---|---|
| Endpoint Protection Platform | Symantec, CROWDSTRIKE, McAfee, Microsoft, SentinelOne, CYLANCE |
| System / Vulnerability Management | TANIUM, Microsoft, ivanti, Symantec, Kaseya, McAfee |
| Endpoint Detection and Response | CARBON BLACK, Microsoft, FireEye, DIGITAL GUARDIAN, ENDGAME., cybereason |
| Endpoint Forensics | GUIDANCE SOFTWARE, nuix, X-Ways |
| Endpoint DLP | FORCEPOINT, McAfee, Symantec, DIGITAL GUARDIAN |
| Firewall / IDS | Microsoft, McAfee, Symantec |

**ARE WE REALLY SAFE ???**

**How much budget we should spend?**

## Threat-Intelligence

System information that information from a range of sources about current or potential attacks against an organization

## Analytic and machine learning

With machine learning, cybersecurity systems can analyze patterns and learn from them to help prevent similar attacks and respond to changing behavior.

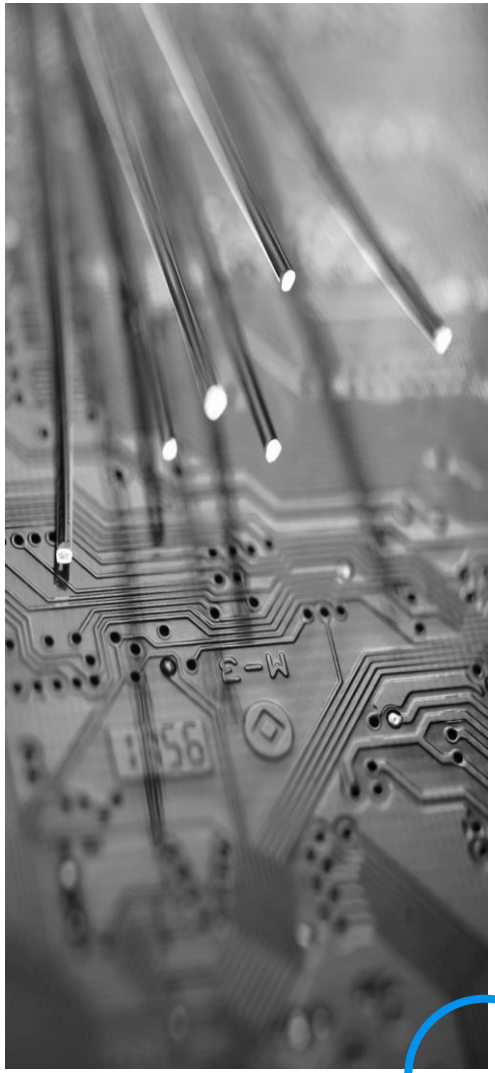
## SIEM

Software that  combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.

## File analysis tools

A system  operating a safe and isolated environment decoupled from the surrounding infrastructure and used  to test code and analyze malware

**Additional Solution Needed**



Find Out More

# Will that be Enough ?

**Protecting Network east west and north south network ?**

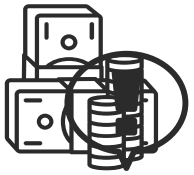
# It is more than who interact with whom

But What, When, Where, How, Why ?

Decode content level

Extract metadata

Asset identification



Assess the risks

Malicious script

Hacker deception

# That's Why Fidelis Elevate

**Fidelis Endpoint**

Safeguard devices on and off network with unmatched investigations, forensics and response

**Fidelis Network**

Detect and respond faster to threats anywhere on the network including email

**Fidelis Deception**

Reshape the attack surface and lure, detect, and defend earlier in the attack lifecycle

## Endpoint

Monitor, detect , respond, protect, any endpoints and correlate with Fidelis Network and Fidelis Insight for unmatched investigations, and forensics

## Network

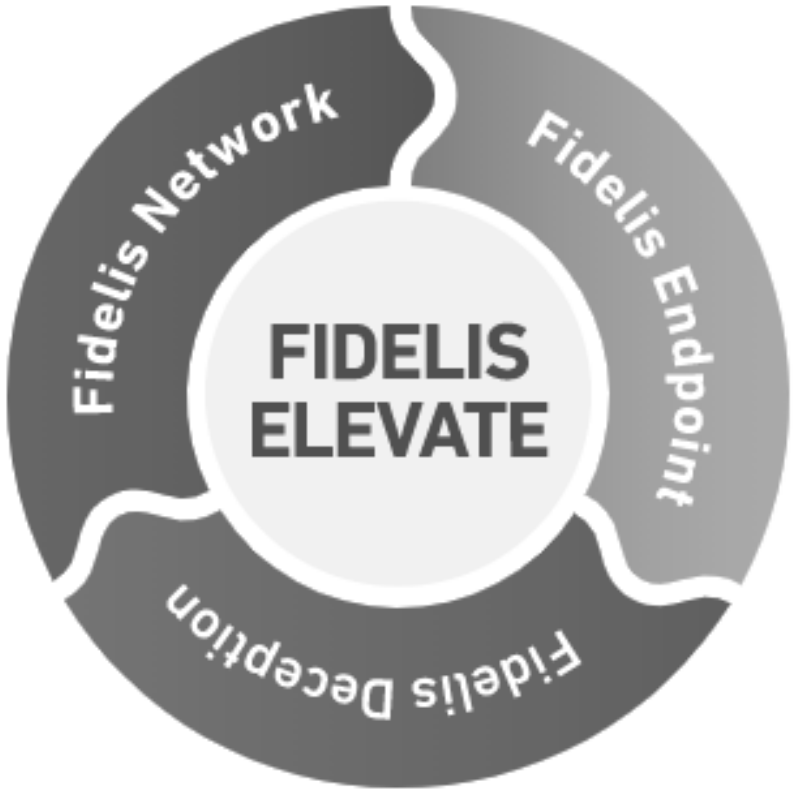
Identify assets, complete terrain mapping and risk analysis that eliminates blind spots and closes security gaps on network Deep network visibility into embedded content, including encrypted traffic, inbound and outbound, across all ports and protocols.

## Deception

Lure and distract adversaries with an authentic deception layer, including decoys, breadcrumbs, and traps that prevent attackers from discovering key assets

# Why Fidelis Elevate?

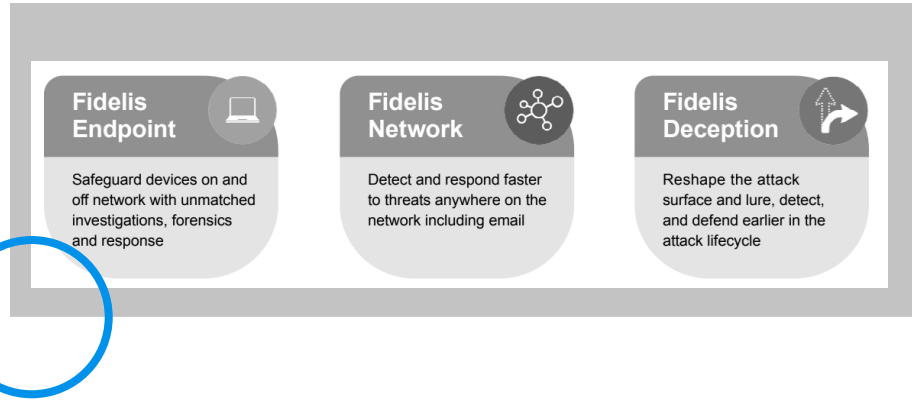
- SIEM →
- Threat-Intel →
- Sandbox →
- Analytics & ML →
- Endpoint →
- Honeypot →



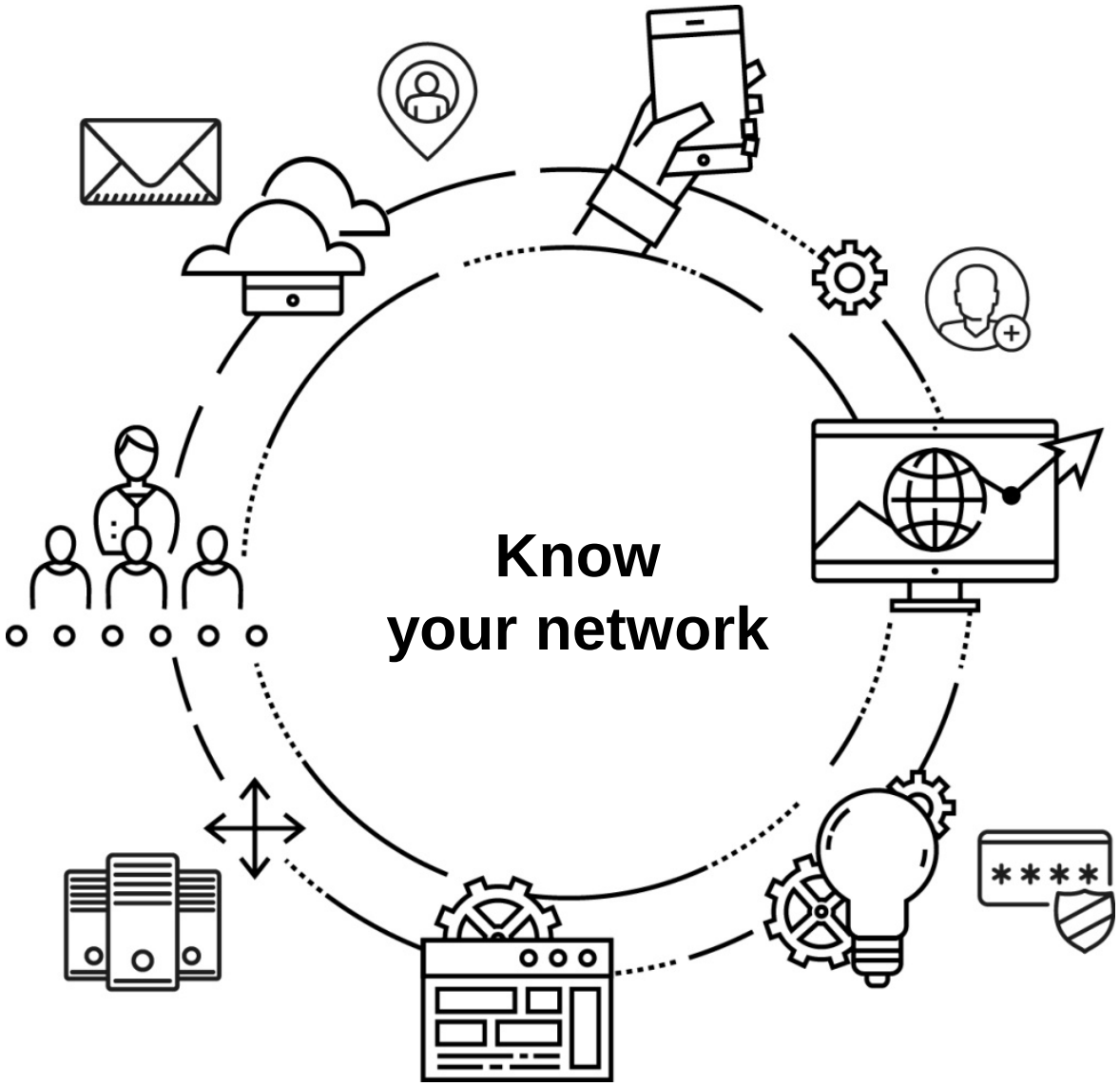

**All-In-One Active XDR for your cyber defense**

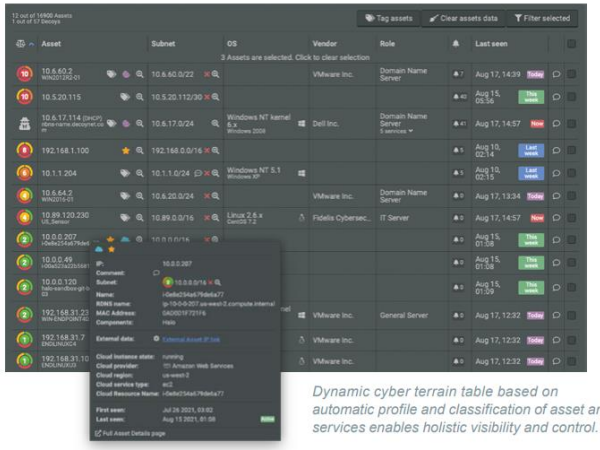
Explore →

# What Fidelis Elevate does after you install?




- Know your network asset in the network
- Automatically classify and identify endpoint assets
- Deploy Decoy and bradcumb

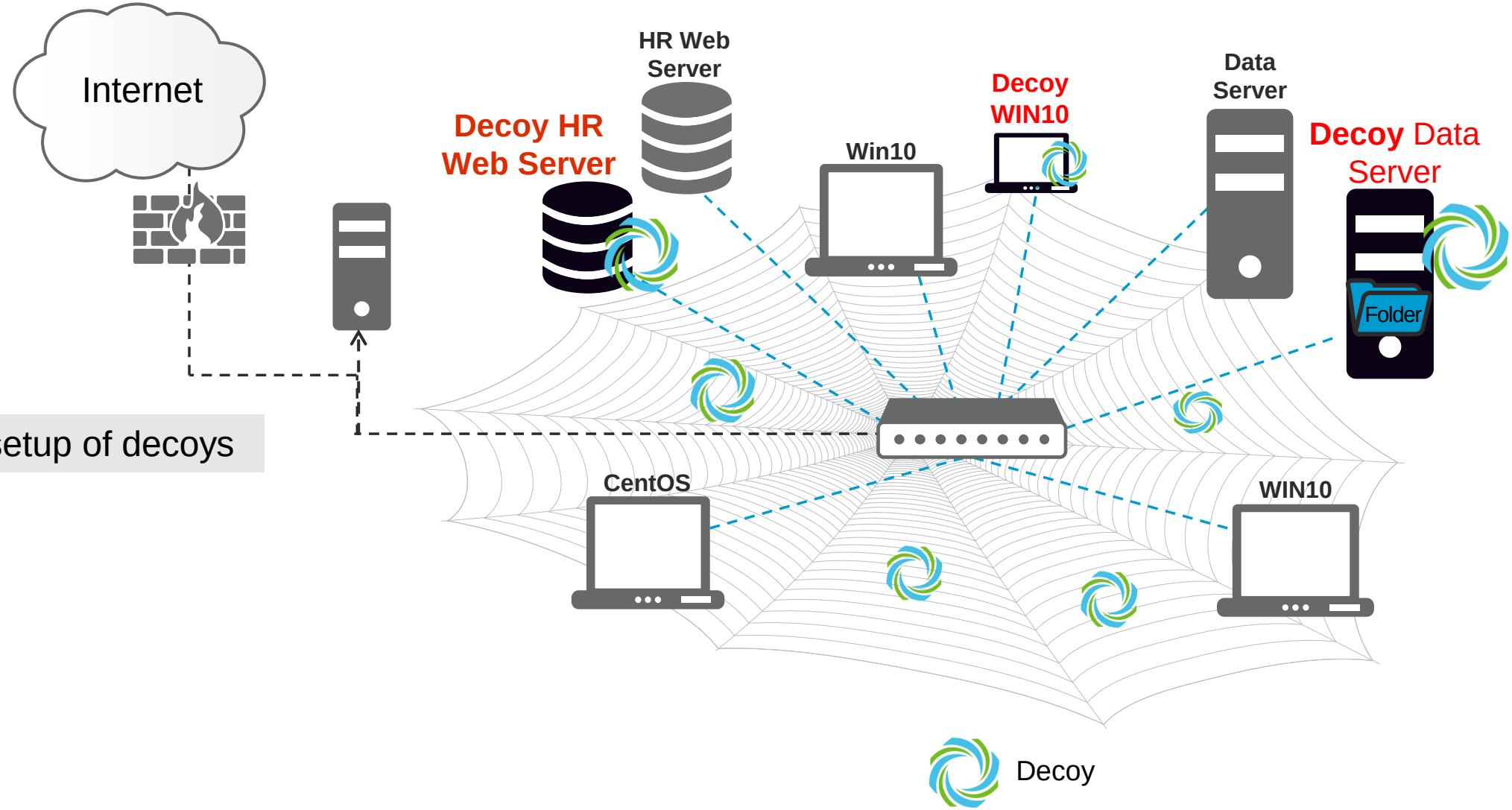


*Dynamic cyber terrain table based on automatic profile and classification of asset and services enables holistic visibility and control.*

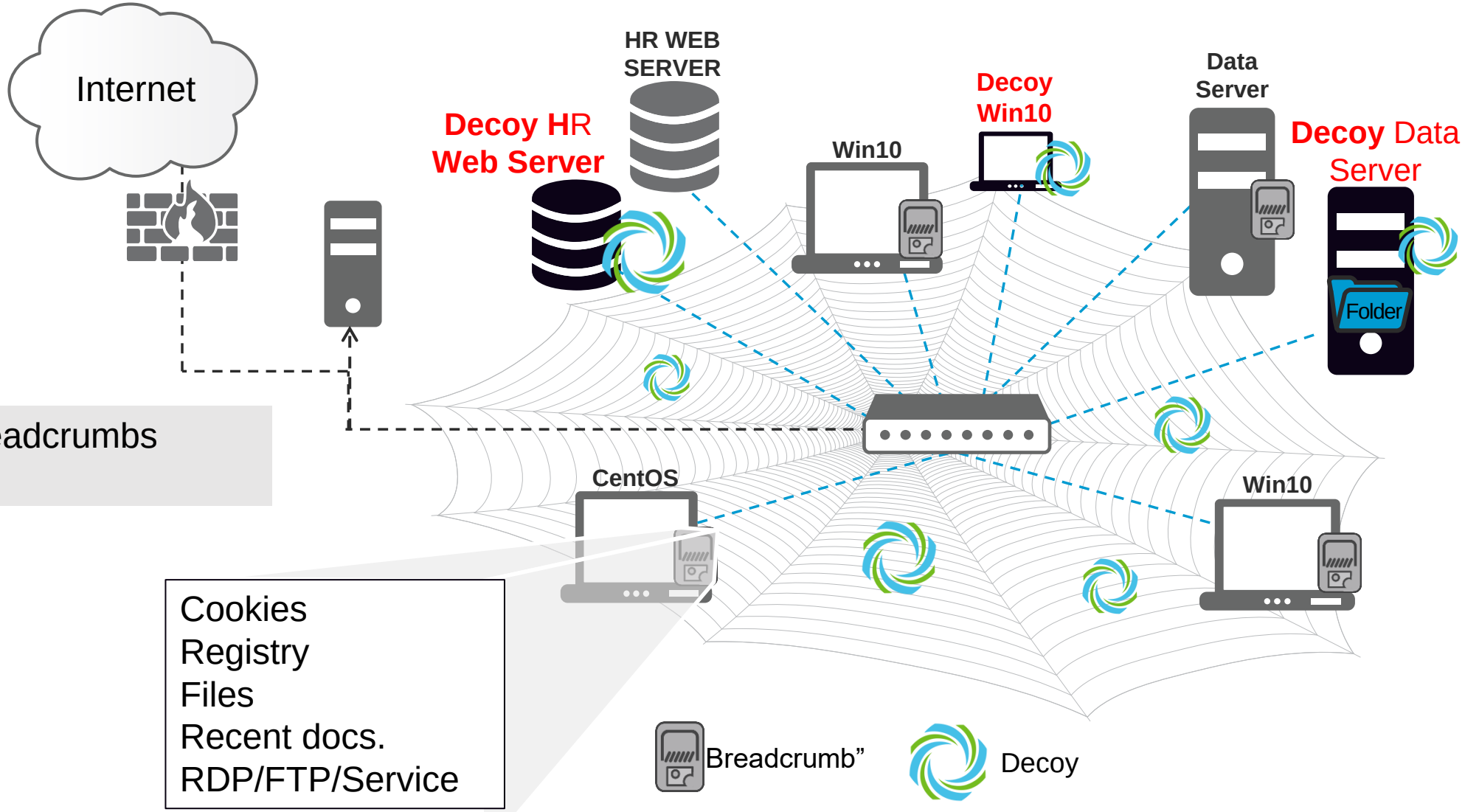
- Subnets
- Assets
- OS
- Ports
- Servers
- Applications

# Deploy Decoys




Automatic setup of decoys

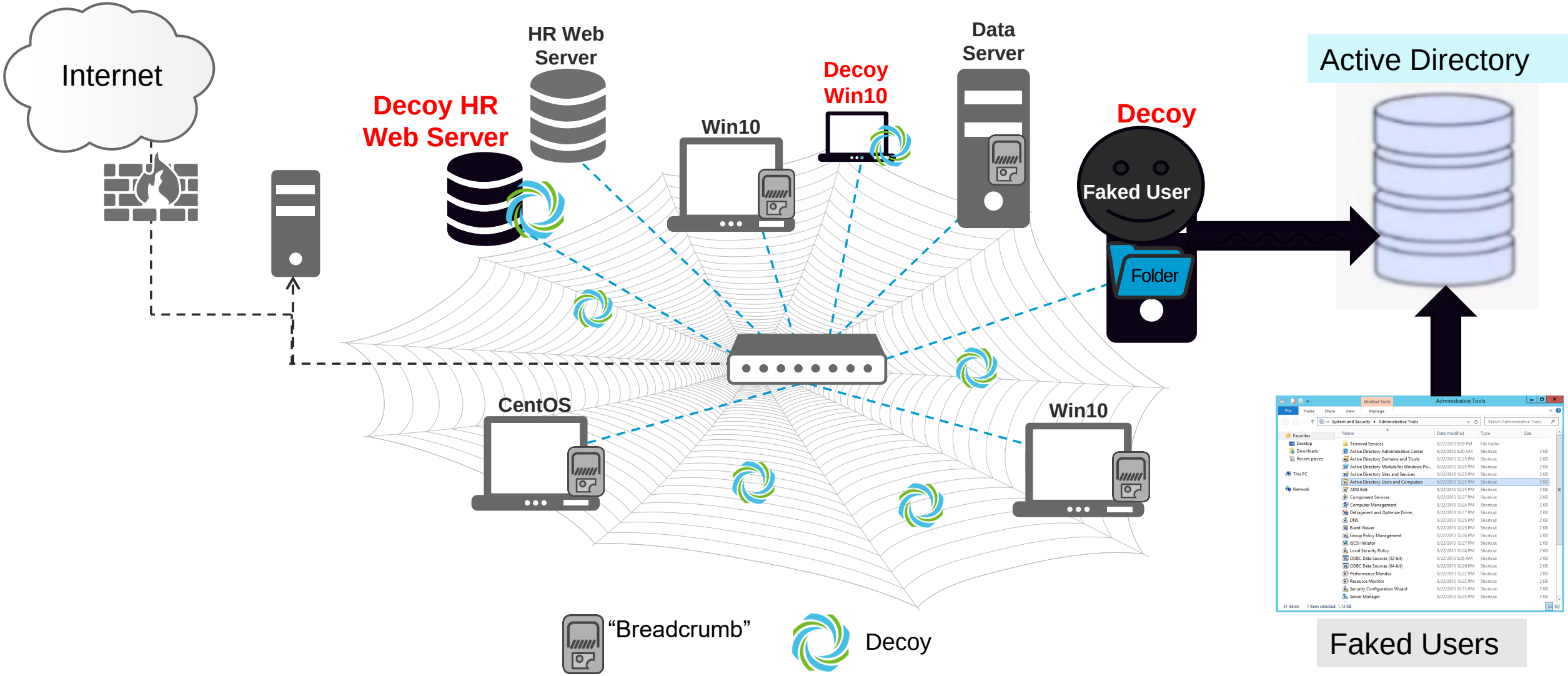
# Deploy Breadcumb




Targeted Breadcrumbs placement

Cookies
Registry
Files
Recent docs.
RDP/FTP/Service

# Deploy Active Directory Deception



Vendors | Fidelis Cybersecurity

Not secure https://demo2.fidelissecurity.com/deception/#/assets/vendors

Fidelis

Terrain / Assets / Vendors

05:03 | demouser

- Dashboard
- Terrain
- DETECTIONS
  - Conclusions
  - Alerts
  - Mail Quarantine
  - Deception Activity
- INVESTIGATION
- RESPONSE
- DECEPTION (44%)
  - Decoys
  - Network Deception
  - Data Deception
  - Breadcrumbs
- Fidelis Endpoint
- POLICIES
- Administration

ASSETS
- Assets
- Tags
- Subnets
- Groups/Domains
- Operating Systems
- Roles
- Vendors
- Services

ANALYSIS
- External Servers
- Internal Traffic
- Uploads
- Incoming Traffic
- Protocol Mismatch
- TLS Tools
- HTTP Tools
- Browsers

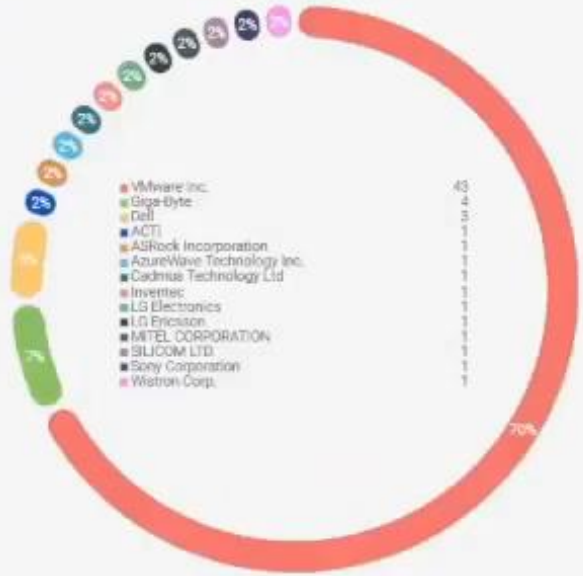
Tags | Filters

6 Vendors
9 Decoy vendors

Filter selected

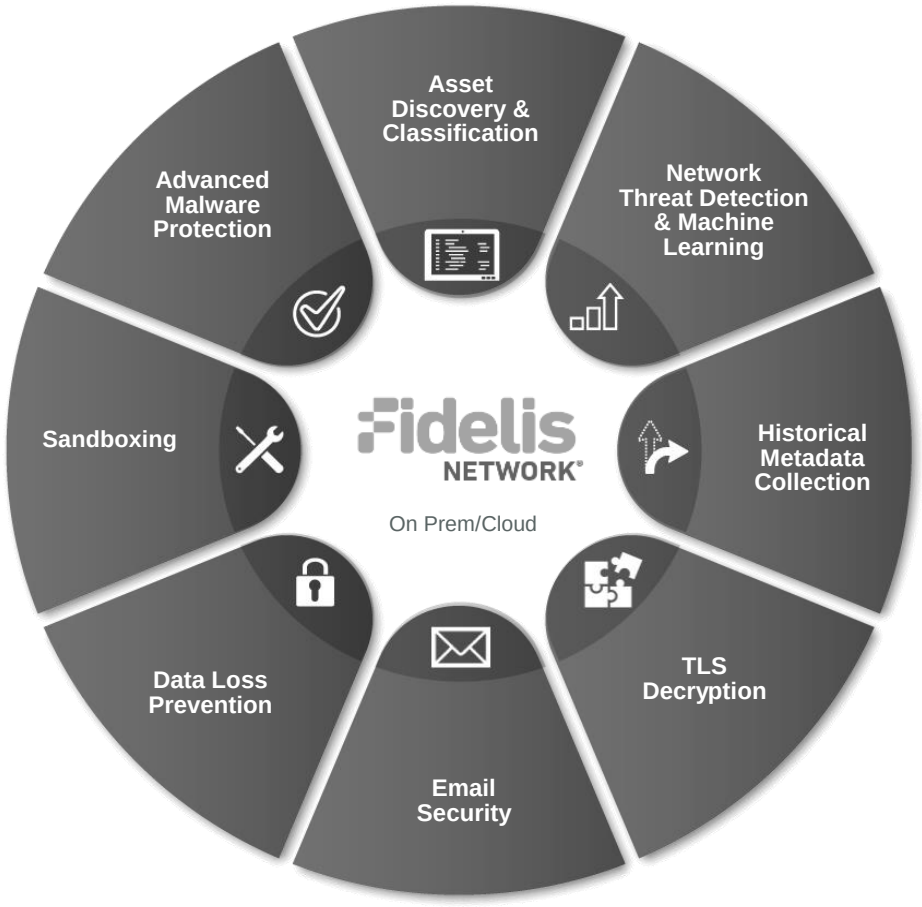
| Vendor | Size | Diversity |
|---|---|---|
| Giga-Byte | Assets: 0<br>Decoys: 4 | Tags: 2<br>Subnets: 2<br>Group/Domains: 3<br>Roles: 4 |
| Dell | Assets: 2<br>Decoys: 1 | Tags: 3<br>Subnets: 2<br>Group/Domains: 1<br>Operating Systems: 1<br>Roles: 2 |
| Wistron Corp. | Assets: 0<br>Decoys: 1 | Tags: 1<br>Subnets: 1<br>Group/Domains: 1<br>Roles: 1 |
| LG Ericsson | Assets: 0<br>Decoys: 1 | Tags: 1<br>Subnets: 1<br>Group/Domains: 1<br>Roles: 1 |
| LG Electronics | Assets: 0<br>Decoys: 1 | Tags: 1<br>Subnets: 1<br>Group/Domains: 1<br>Roles: 1 |
| Inventec | Assets: 0<br>Decoys: 1 | Tags: 1<br>Subnets: 1<br>Group/Domains: 1<br>Roles: 1 |
| AzureWave Technology Inc. | Assets: 0<br>Decoys: 1 | Tags: 1<br>Subnets: 1<br>Group/Domains: 1<br>Roles: 1 |
| ASRock Incorporation | Assets: 0<br>Decoys: 1 | Tags: 1<br>Subnets: 1<br>Group/Domains: 1<br>Roles: 1 |
| | Assets: 0<br>Decoys: 1 | Tags: 1<br>Subnets: 1<br>Group/Domains: 1 |

Environment | Deception




https://demo2.fidelissecurity.com/deception/#/assets/subnetId

# Fidelis Network




Network Detection and Response

Providing 8 Critical Capabilities in a Single Solution

SC 2019 awards Winner
BEST THREAT DETECTION TECHNOLOGY

## Providing 8 Critical Capabilities in a Single Solution

- Fully integrated, automated and correlated for you
- Automated Hunting Platform (Detect, Hunt, Response)
  - Asset Discovery  to Map your network terrain
  - Deep visibility into embedded content, inbound, outbound and lateral movement traffic, across all ports and protocols
  - Multiple detection methods across the kill chain
  - Real-time & historical detection
  - Gateway and Lateral movement monitoring and recording (Metadata)
  - Historical investigation (Malicious and Non-Malicious MetaData)
  - Analytical (Behaviorial) Detection
  - Prevent data exfiltration (NDLP)

# Fidelis Network®:
## Historical Metadata

**WHO:**

Domain user, Webmail user, FTP user, email address, device ID, organization name

**WHAT:**

filenames, SHA256, MD5, content tags, malware name, malware type

**WHEN:**

From right now back through time – as long as you're willing to store the data


**WHERE:**

Source, Destination, country, IP address, organization, URL, Domain

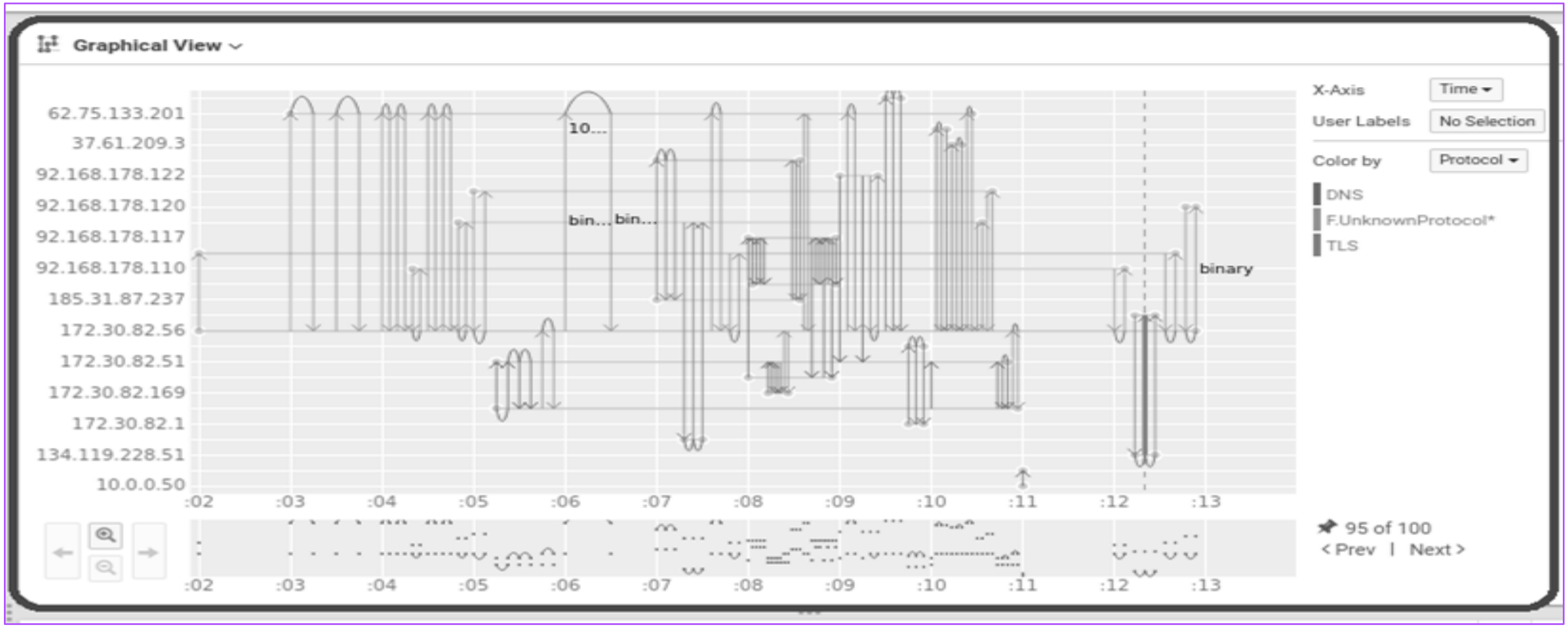
**HOW:**

protocols, applications, file type, User Agent, custom protocols, obfuscated files and scripts

***Manual searching, automatic analytics, anomaly detection…***
***At a fraction of the cost of full PCAP storage and much faster response times***

# Fidelis Network®:

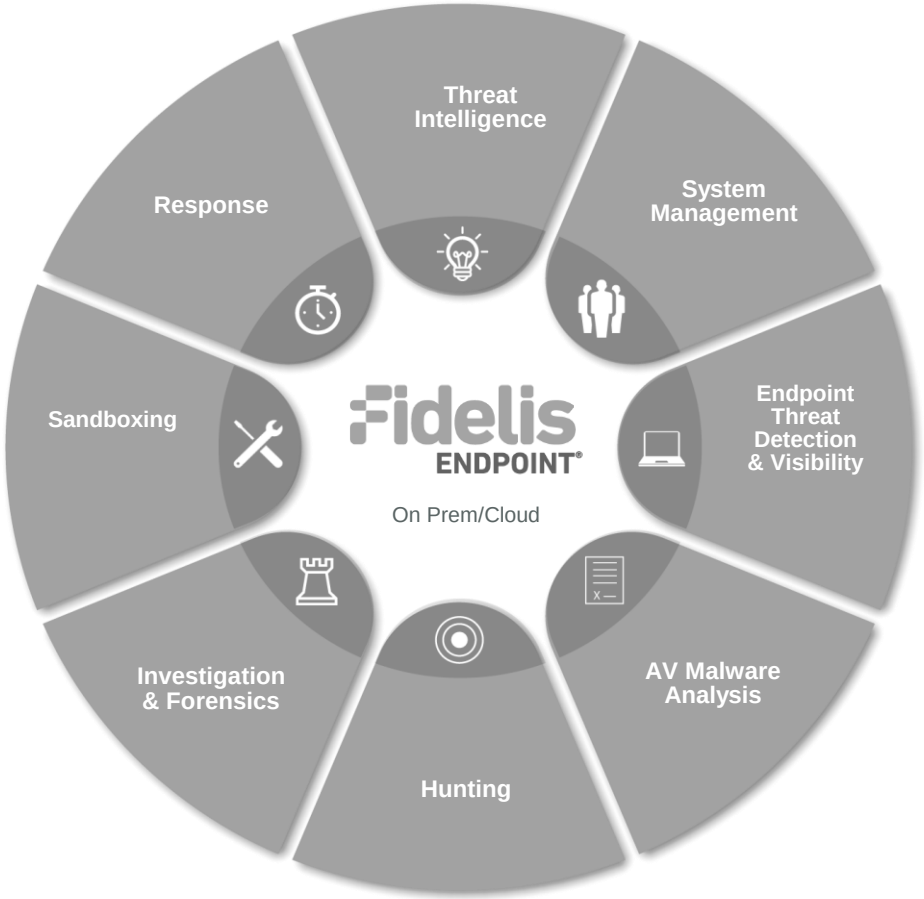
## Rich Historical Metadata



# Fidelis Endpoint®:

## Active Endpoint Detection & Response

MITRE ATT&CK™




**Best-of-Breed**

**Endpoint Forensics & Response**

**Providing 8 Critical Capabilities in a Single Solution & 1 Agent**

## Best-of-Breed Across 8 Critical Areas in a Single Solution

- Fully integrated, automated and correlated for you
- Automated Hunting Platform (Detect, Hunt, Response)
- EPP, EDR, System Management, Forensics – all via a single management (investigation UI) and single Agents
  - Visibility of all endpoint activity in the environment
  - Real-time threat detection and proactive hunting
  - Process Metadata - Timeline Analysis View of all malware and endpoint behaviors (Malicious & Non-Malicious)
  - Real-time and historical validation and investigation
  - Remote forensics (DFIR): Live Console, Live Directory Preview, memory analysis, collection, full disk imaging
  - Script Execution: Out-of-the-box and customizable remediation
- Easy integration with Fidelis Network and SIEMs
- Managed in the Cloud & On-Prem

# What You Get With Fidelis Endpoint

## PREVENTION

- Block malware with leading AV engine
- Prevent via machine learning behavioral models
- Know your endpoint hygiene and what software is installed

## DETECTION

- Apply threat intelligence
- Scan for IOCs and YARA indicators
- Real-time and retrospective analysis
- Custom search and hunting
- On-demand scanning

## FORENSICS & INVESTIGATION

- Full disk imaging
- Full memory capture and live memory analysis
- File and folder collection
- Event context
- System isolation

## RESPONSE

- Automate playbooks and triaging tasks
- Restore to good configuration
- Terminate processes, collect or delete files
- Script library
- Integration with SIEMs, SOARs, and NGFWs

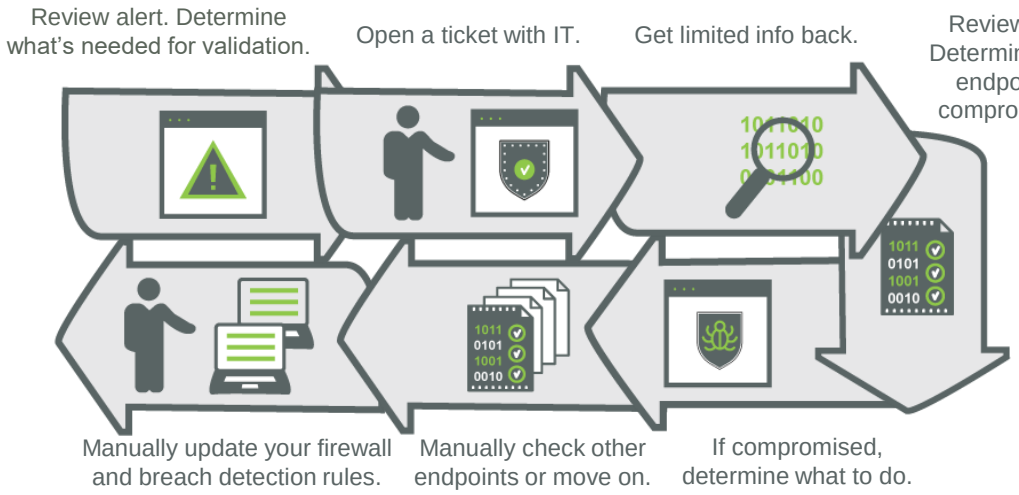
## MANAGEMENT

- Alerts Subscription
- System management scripts
- Connected agent status
- System health page
- Roles & permissions
- Secure agent communications

# Accelerate time to Response

## *Triaging, Investigating and Responding to an Incident*

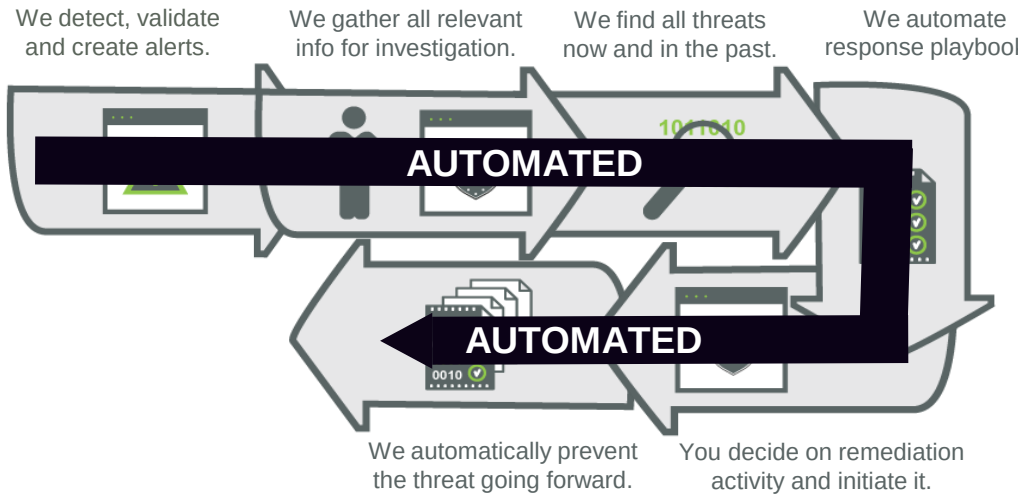
**MANUAL PROCESSES**
**(Without Fidelis)**


**BEST CASE**
**Hours or Days**

***Accuracy and Speed Matter***

**FIDELIS AUTOMATION**




**TYPICAL CASE**
**MINUTES**
**(vs. Hours or Days)**

# Fidelis Coordinates Defense Across Attack Surfaces

**Elevate™ gives security teams a platform to effectively detect, hunt and respond to threats.**

Available On-Prem, Cloud and Hybrid

## WEB STACK

| | |
|---|---|
| Deception | |
| Content Analysis and DLP | |
| Sandboxing | |
| Advanced Malware Detection | |
| Secure Web Gateway | |
| Web Proxy | |

## NETWORK STACK

*(All Ports and All Protocols)*

| | |
|---|---|
| Asset Classification | |
| Deception | |
| Network Traffic Analysis | |
| Content Analysis & DLP | |
| Sandboxing | |
| Advanced Malware Detection | |
| TLS Decryption | |
| Firewalls / IPS | |

Fidelis ELEVATE™

Integration

SIEM

SOAR

## E-MAIL STACK

| | |
|---|---|
| Deception | |
| Content Analysis and DLP | |
| Sandboxing | |
| Advanced Malware Detection | |
| Secure E-mail Gateway | |
| Exchange | |

## ENDPOINT STACK

| | |
|---|---|
| Endpoint Protection Platform | |
| System / Vulnerability Management | |
| Endpoint Detection and Response | |
| Endpoint Forensics | |
| Endpoint DLP | |
| Firewall / IDS | |

Available on cloud and managed service

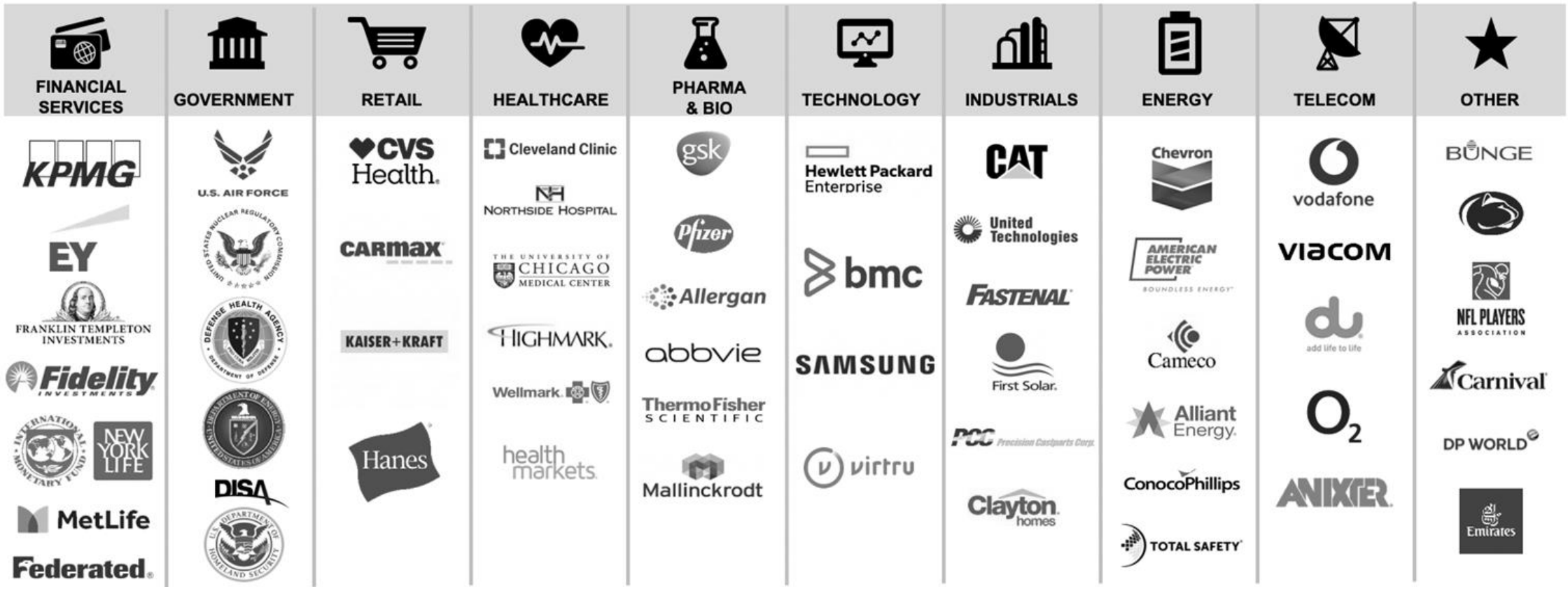
Fidelis Cybersecurity

# Trusted by the World's Largest Brands and Government Organizations

Relied on by **40+** U.S. government agencies

Trusted by **12** of the Fortune 50

Depended on by **24** of the Fortune 100



# Companies Rely on Fidelis

Fidelis™ Cybersecurity

## Global Presence

- Founded since 2004
- 350+ employees
- Headquartered in Washington, DC
- Local Support in Indonesia

Apple · Microsoft · U.S. Air Force · Pfizer · IBM · Samsung · Post (Chunghwa Post Co., Ltd.) · American Electric Power · 臺北市稅捐稽徵處 TAIPEI REVENUE SERVICE

**Active eXtended Detection and Response (aXDR)**

**NDR since 2004 and MetaData Collection since 2012**

**EDR since 2013 and Deception since 2017**

**Incident responders for over 3500+ cases**

#SuccessStory Indonesia

One of the largest energy company in Indonesia with 50 thousands employees

## TRUST FIDELIS ELEVATE TO PROTECT IT AND OT

#FidelisReference

#SuccessStory Indonesia

Oil and gas regulator in Indonesia

## TRUST FIDELIS ELEVATE TO PROTECT ITS INTERNAL NETWORK

#FidelisReference

#SuccessStory Indonesia

Big media broadcasting company

## TRUST FIDELIS MANAGED SERVICE TO PROTECT ITS INTERNAL NETWORK


#FidelisReference

Fidelis Cybersecurity

# Why Fidelis Network

**All-in-one active XDR**

All-in one active extended network detection and response, hacker deception, and endpoint protection

**Rich-metadata**

To understand what, when the attack happens, how it happens, who does it with 300++ Metadata attributes

**Integrate with existing investment**

Seamless integration with many solution for investment protection

**Available in perpetual license and managed service**

Fidelis available in cloud, subscription as well as perpetual licenses

**Trusted by famous organizations**

Fidelis is a standard security solution for Apple, Microsoft, US Airforce, and many more.


Log Collection
Reporting
Research &
Development
Threat
Intelligence
Knowledge
Ticketing
SIEM
Aggregation
Correlation
Security
Operation
Center (SOC)

deltadata

# Cyber Security Managed Service

| PRICE TABLE | ENTERPRISE | LARGE | MEDIUM | SMALL |
|---|---|---|---|---|
| | **Rp 99 Ribu** Per EP Per Month | **Rp 136 Ribu** Per EP Per Month | **Rp 250 Ribu** Per EP Per Month | **Rp 99 Ribu** Per EP Per Month |
| Network Detection And Respond | ✓ | ✓ | ✓ | ✓ |
| Asset Mapping And Alert | ✓ | ✓ | ✓ | ✓ |
| DLP Network | ✓ | ✓ | ✓ | ✗ |
| DLP Endpoint | ✓ | ✗ | ✗ | ✗ |
| Metadata Retention | ✓ | ✓ | ✓ | ✓ |
| Deception | ✓ | ✓ | ✓ | ✓ |
| Endpoint forensic and investigation | ✓ | ✓ | ✓ | ✓ |
| Integration NDR and Deception | ✓ | ✓ | ✓ | ✗ |
| Hardware Included | ✓ | ✓ | ✗ | ✗ |
| www.deltadatamandiri.com. | >10,000 Karyawan | Min 5,000 Karyawan | Min 1,000 Karyawan | Min 300 Karyawan |