Overview

DETECT, HUNT, RESPOND

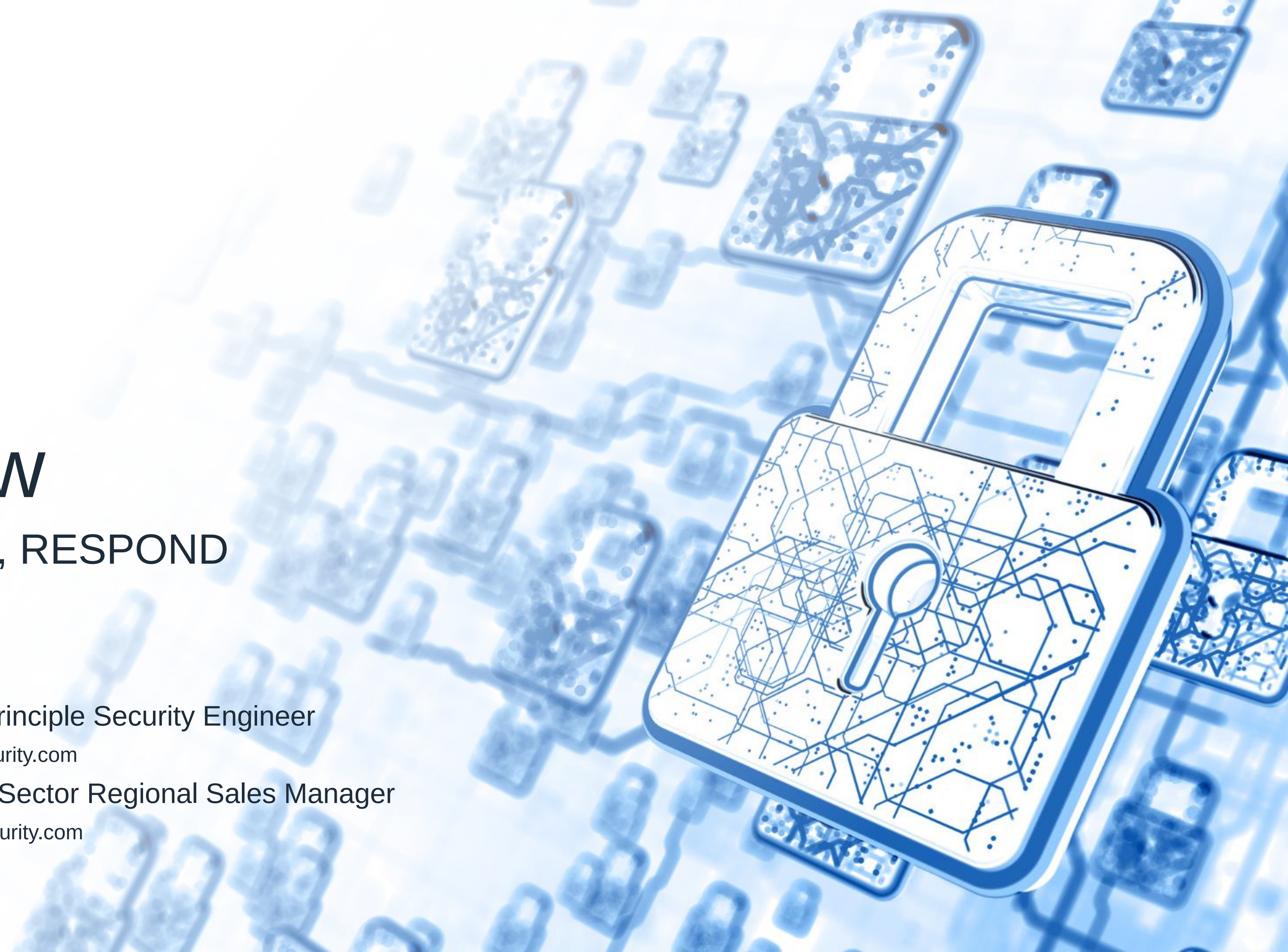
Kevin Harvey - Senior Principle Security Engineer

Email: Kevin.Harvey@fidelissecurity.com

Jake Voorhees – Public Sector Regional Sales Manager

Email: jake.voorhees@fidelissecurity.com

Number: 757-784-7038



Expanding Attack Surface

Data Is Everywhere

Increasingly Sophisticated Attacks and Adversaries

Complex and Redundant Security Stacks

Staff/Resource Limitations

5 Critical Capabilities

Proactive Capabilities

- **Terrain Mapping** — Identify and categorize All Managed and Unmanaged Assets; assess and identify High-Risk Assets / Paths
- **Hunting for Indicators of Compromise (IOCs)** — Integrated and automated tools supported by threat intelligence to enable security analysts to detect, investigate, and track anomalous activity
- **Automated Threat Detection & Response** — Rich metadata, custom rule sets, event correlation analytics to produce high confidence & actionable alerts; playbooks drive automated response
- **Dynamic Deception** — Continuously changing Attack Surface to increase Adversary Cost, Complexity, & Risk

Protective Capabilities

- **Network-based Threat Detection & DLP** — Network-based IPS, Deep Session Inspection across all ports and protocols, enhanced E-mail and Web detections; TLS decryption
- **Endpoint Detection and Response** — Signature and Behavior based analysis and blocking; Cross-platform, Script Execution Platform

Reactive Capabilities

- **Threat-Driven Operations** — Automated Post-Breach Detection & Response Actions supported by integrated and automated tools enable security analysts to investigate, determine extent of breach, and take corrective actions

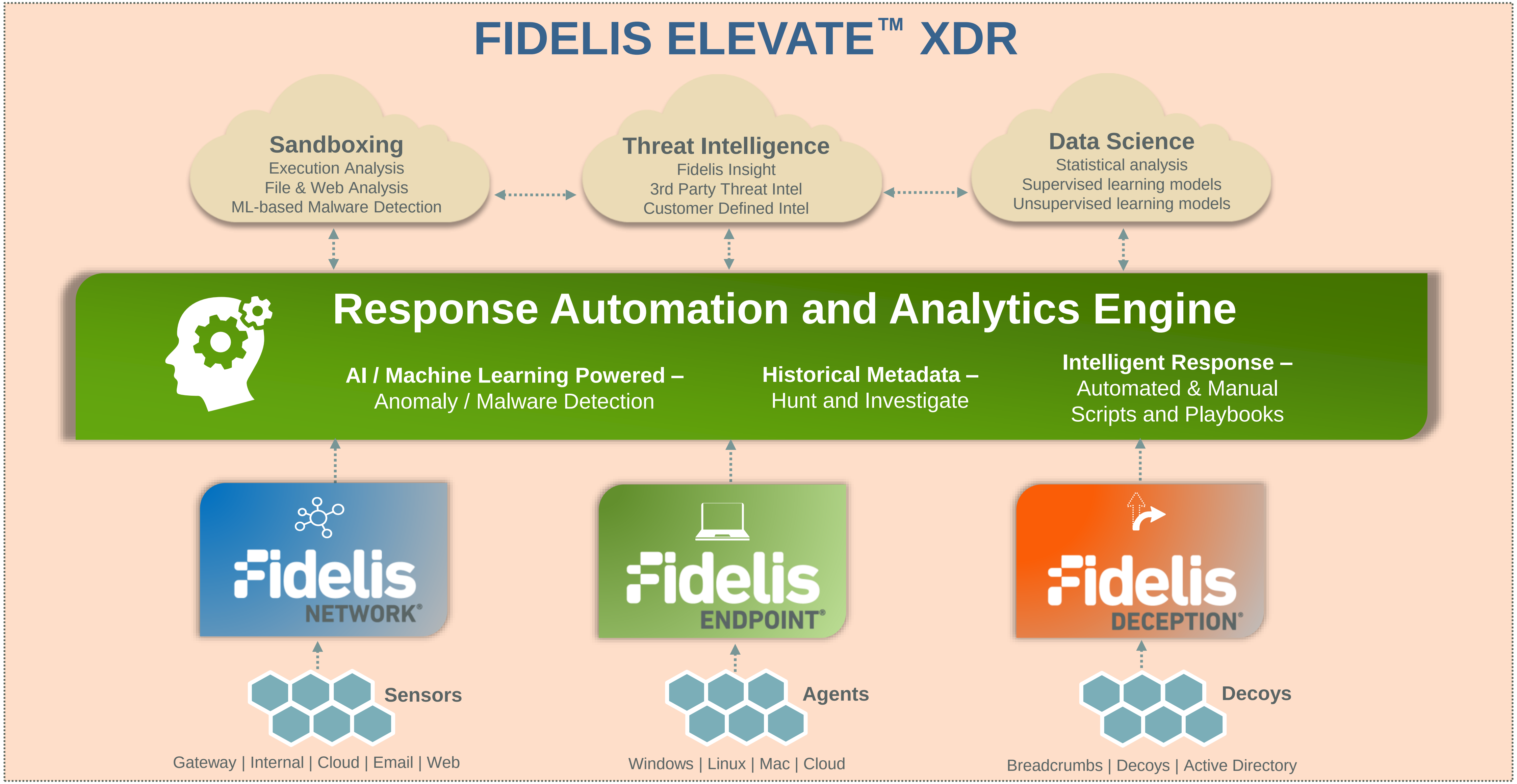
Predictive Capabilities

- **Machine Learning/Artificial Intelligence Based Analysis** — Detect Anomalous Activity, Determine Probability of Compromise, Analysis of Metadata in Search of Known/Unknowns, produce high confidence & actionable alerts

Retrospective Capabilities

- **Automated Retrospective Analysis** — Continuously collect and (re)assess metadata (all communication paths) against new threat intelligence

A Curated Security Stack— Integrated, Automated & Correlated



FIDELIS ELEVATE™ XDR

Sandboxing
Execution Analysis
File & Web Analysis
ML-based Malware Detection

Threat Intelligence
Fidelis Insight
3rd Party Threat Intel
Customer Defined Intel

Data Science
Statistical analysis
Supervised learning models
Unsupervised learning models

Response Automation and Analytics Engine

AI / Machine Learning Powered –
Anomaly / Malware Detection

Historical Metadata –
Hunt and Investigate

Intelligent Response –
Automated & Manual
Scripts and Playbooks

Sensors
Gateway | Internal | Cloud | Email | Web

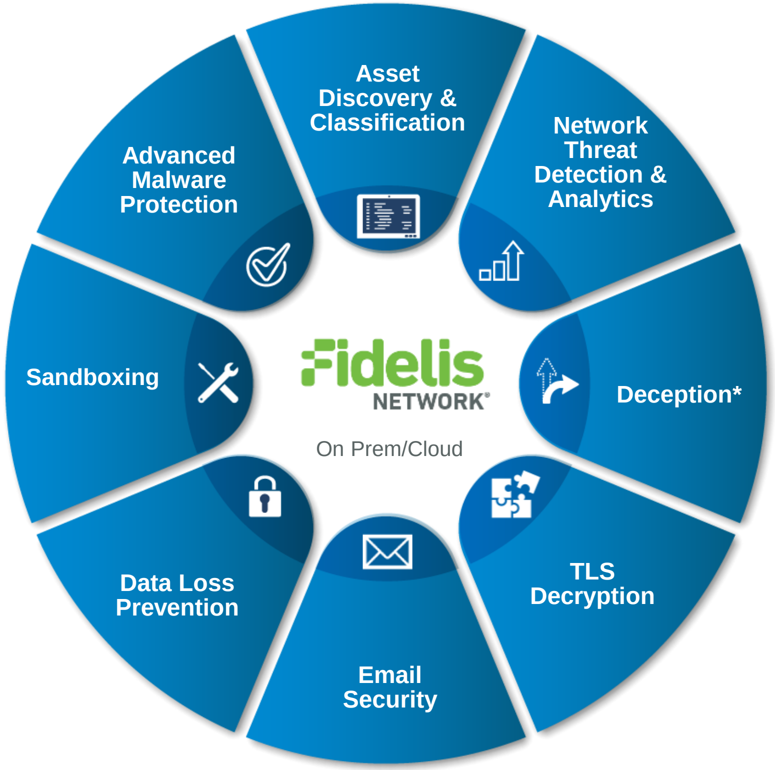
Agents
Windows | Linux | Mac | Cloud

Decoys
Breadcrumbs | Decoys | Active Directory

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

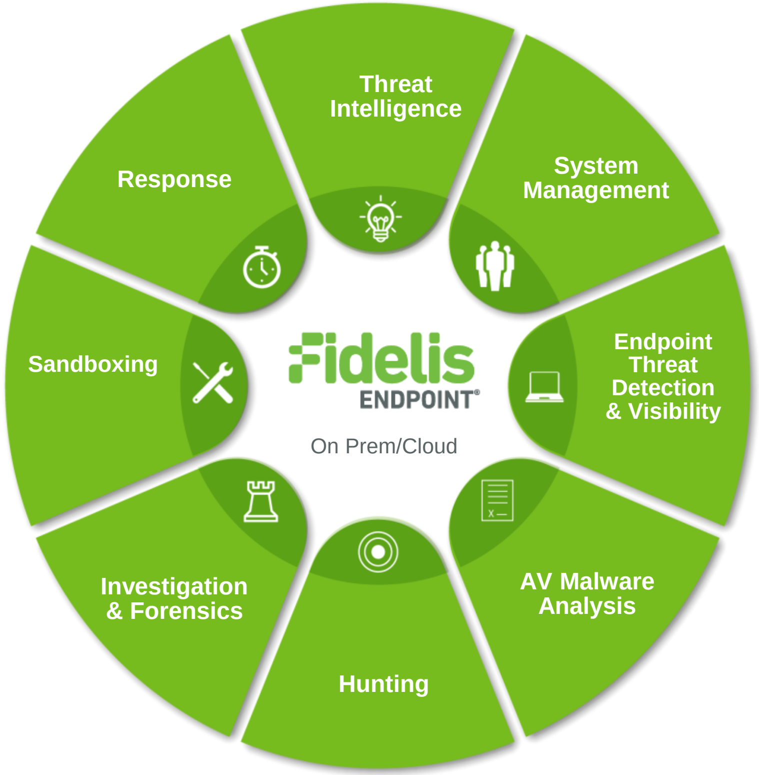
Fidelis Elevate™ XDR Platform

Comprehensive, Integrated, Best-In-Class Network, Endpoint & Deception Security



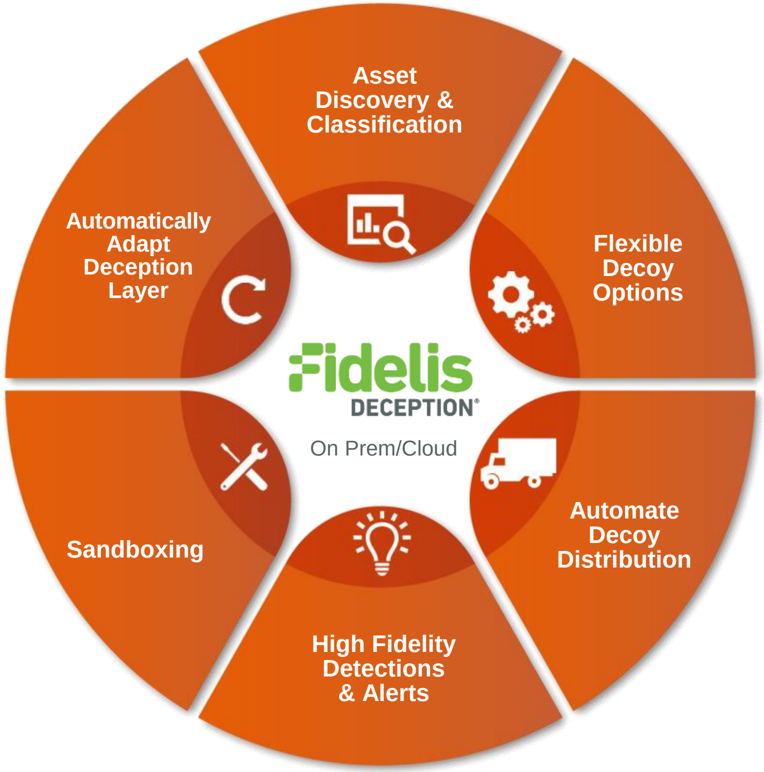
Network Traffic Analysis

- Providing 8 Critical Capabilities in a Single Solution



Endpoint Forensics & Response

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


Asset Discovery & Classification
Flexible Decoy Options
Automate Decoy Distribution
High Fidelity Detections & Alerts
Sandboxing
Automatically Adapt Deception Layer
Fidelis DECEPTION®
On Prem/Cloud

Deception Capabilities

- With a Wide Array of Decoys and Breadcrumbs

* Fully integrated – requires Deception™ license

Fidelis Coordinates Defense Across Attack Surfaces

Fidelis Elevate®: A platform to effectively detect, hunt, and respond to threats

Available On-Prem, Cloud, and Hybrid

WEB STACK

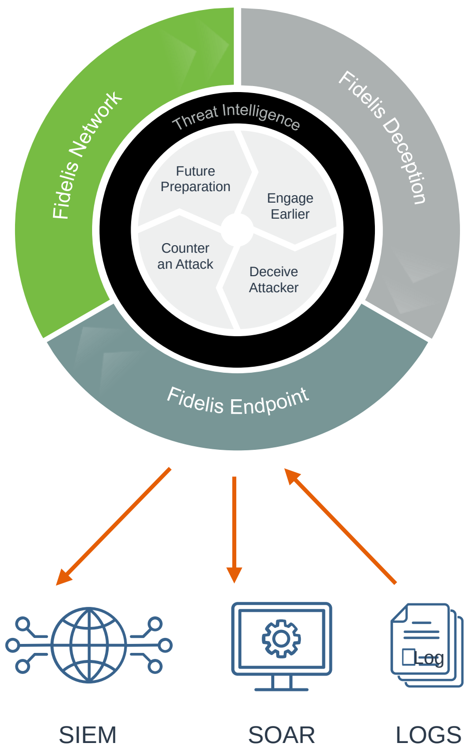
- Deception
- Content Analysis and DLP
- Sandboxing
- Advanced Malware Detection
- Secure Web Gateway
- Web Proxy

NETWORK STACK

(All Ports and All Protocols)

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

Fidelis Elevate®



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

Fidelis Security®

Thank You

Operate from the Advantage with Speed and Context

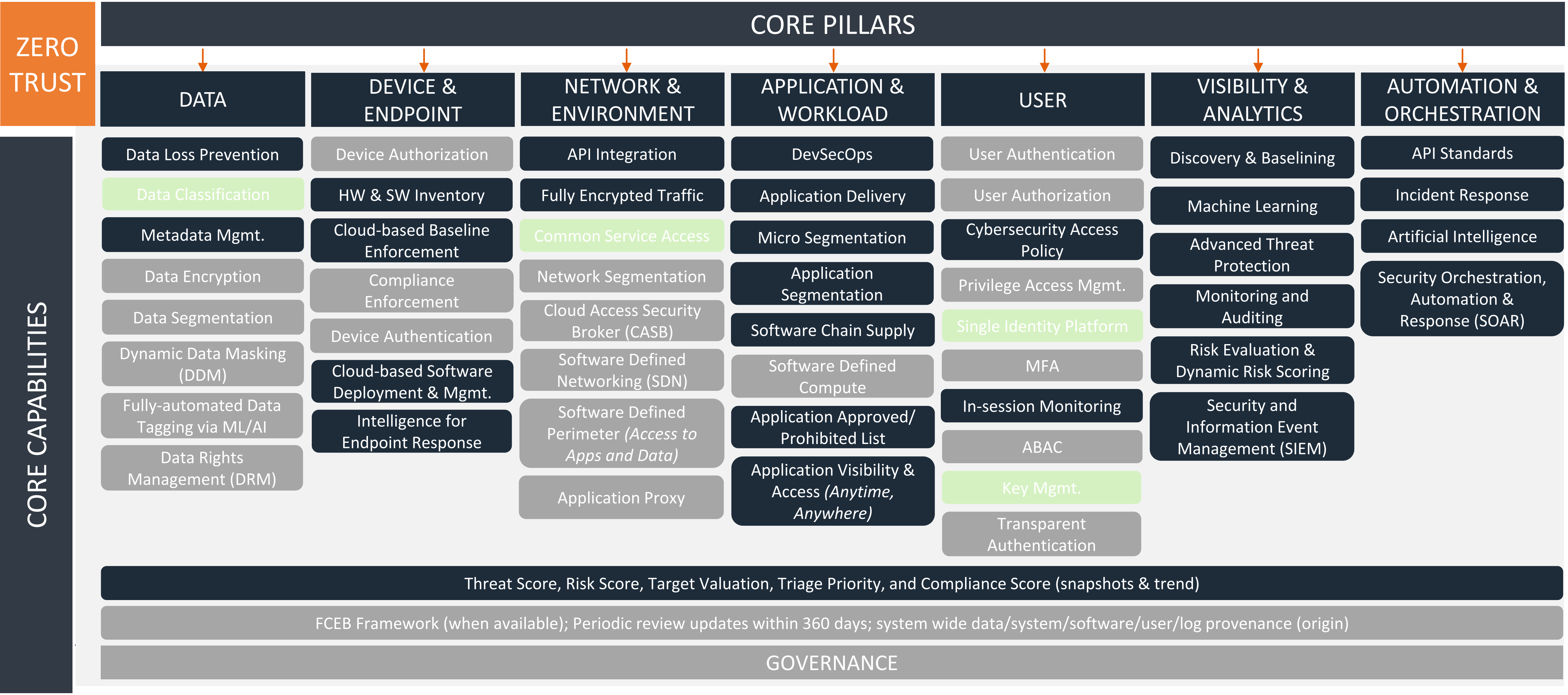
- **Know your terrain better than your adversary:** Holistic visibility allows for threats to be analyzed and neutralized faster
- **Automate response by understanding motives and objectives:** Know the attacker’s tactics, techniques, and procedures
- **Shape the attacker’s experience:** Dynamically alter the percentage of exploitable terrain to increase the cost, risk, and complexity of their operations
- **Proactively find and engage adversaries prior to impact:** Avoid the cost and impact from “too little and too late” defensive actions
- **Level the playing field against adversaries:** Neutralize your adversary by using automated defenses and AI

Make it harder and more costly for adversaries to complete their mission

Zero Trust

Fidelis Security

Capability Model: Core | Enabling | N/A



ZERO TRUST

CORE PILLARS

CORE CAPABILITIES

DATA	DEVICE & ENDPOINT	NETWORK & ENVIRONMENT	APPLICATION & WORKLOAD	USER	VISIBILITY & ANALYTICS	AUTOMATION & ORCHESTRATION
Data Loss Prevention	Device Authorization	API Integration	DevSecOps	User Authentication	Discovery & Baselining	API Standards
Data Classification	HW & SW Inventory	Fully Encrypted Traffic	Application Delivery	User Authorization	Machine Learning	Incident Response
Metadata Mgmt.	Cloud-based Baseline Enforcement	Common Service Access	Micro Segmentation	Cybersecurity Access Policy	Advanced Threat Protection	Artificial Intelligence
Data Encryption	Compliance Enforcement	Network Segmentation	Application Segmentation	Privilege Access Mgmt.	Monitoring and Auditing	Security Orchestration, Automation & Response (SOAR)
Data Segmentation	Device Authentication	Cloud Access Security Broker (CASB)	Software Chain Supply	Single Identity Platform	Risk Evaluation & Dynamic Risk Scoring	
Dynamic Data Masking (DDM)	Cloud-based Software Deployment & Mgmt.	Software Defined Networking (SDN)	Software Defined Compute	MFA	Security and Information Event Management (SIEM)	
Fully-automated Data Tagging via ML/AI	Intelligence for Endpoint Response	Software Defined Perimeter *(Access to Apps and Data)*	Application Approved/ Prohibited List	In-session Monitoring		
Data Rights Management (DRM)		Application Proxy	Application Visibility & Access *(Anytime, Anywhere)*	ABAC		
				Key Mgmt.		
				Transparent Authentication		

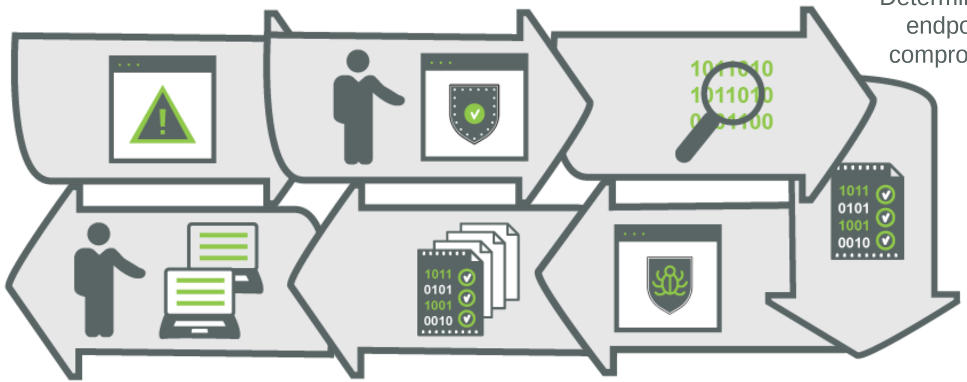
Threat Score, Risk Score, Target Valuation, Triage Priority, and Compliance Score (snapshots & trend)

FCEB Framework (when available); Periodic review updates within 360 days; system wide data/system/software/user/log provenance (origin)

GOVERNANCE

Think and Act Faster than Your Adversaries

WITHOUT US



Review alert. Determine what's needed for validation.

Open a ticket with IT.

Get limited info back.

Review info. Determine if the endpoint is compromised.

If compromised, determine what to do.

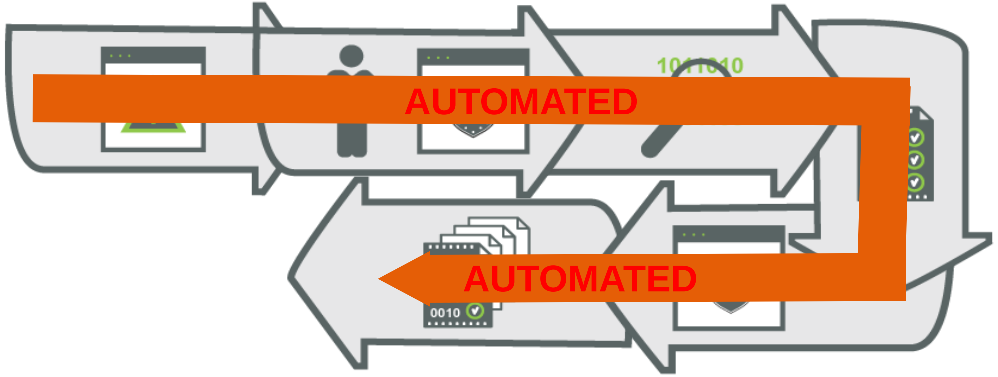
Manually check other endpoints or move on.

Manually update your firewall and breach detection rules.

BEST CASE
Hours or Days

Accuracy and Speed Matter

WITH FIDELIS



We detect, validate and create alerts.

We gather all relevant info for investigation.

We find all threats now and in the past.

We automate response playbooks.

You decide on remediation activity and initiate it.

We automatically prevent the threat going forward.

TYPICAL CASE
MINUTES
(vs. Hours or Days)

Remember… Adversaries Use AI to Accelerate Their Attacks

Deception Use Cases

Security Research

- Learn TTPs
- Capture Tools
- Attribution/Mitigation
- *Real OS Decoys*

Smart Alarm System

- Detect & Defend
- Automation/Scale
- Post Breach Visibility
- *Decoy Emulation*

Enterprise IoT Devices

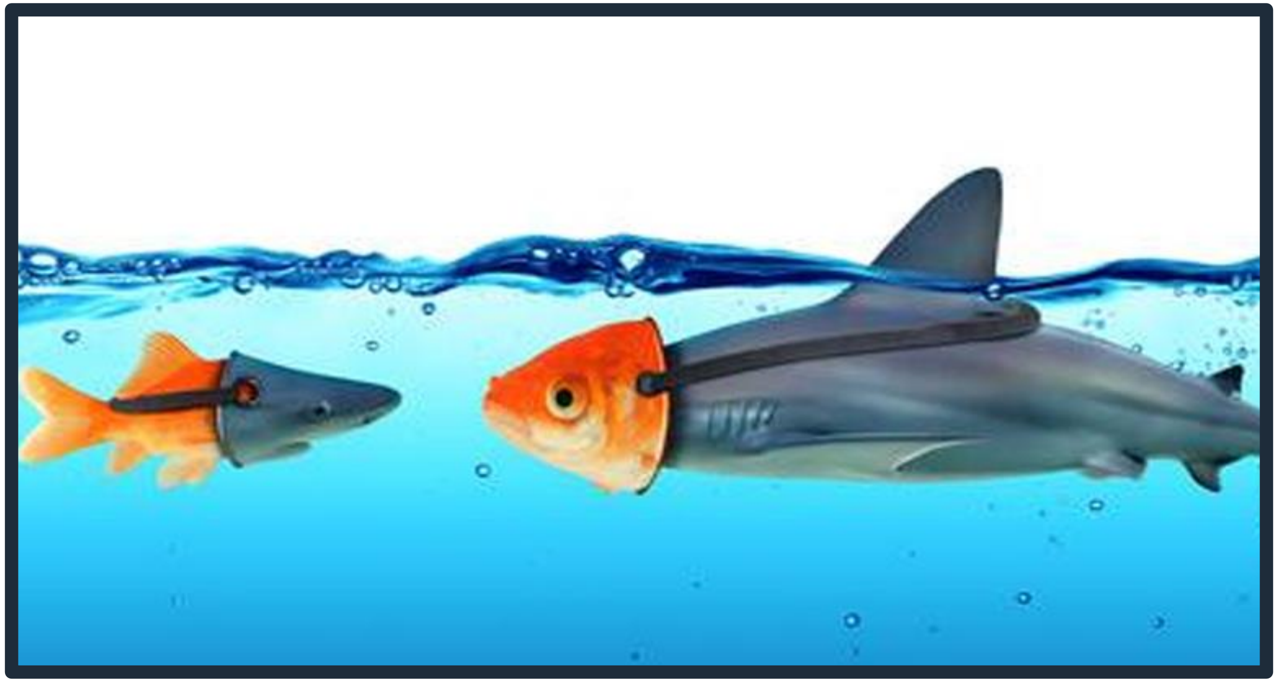
- Detect & Defend
- Automation/Scale
- No Agents
- *Decoy Emulation*

Non-Standard Devices

- Operational Tech
- Oil/Gas, Medical
- Golden OS Images
- *Real OS Decoys*

Deception Challenges

- ❑ **Automatic Deployment**
- ❑ **Adaptive**
- ❑ **Luring Attackers**
- ❑ **Authenticity**
- ❑ **Scalable**
- ❑ **Agentless**



Fidelis Deception

Deception

- Real OS & Emulated Decoys
- Breadcrumbs & Fake Files
- MITM Traps
- AD Fake Activities
- Enterprise IoT Devices
- On-Premise & Cloud (AWS)
- Cloud-based Sandboxing

Profiling and Classification

- Internet Communications
- Separates Human Traffic from Automatic Traffic
- Shadow IT & Legacy Systems
- 10G Sensor Performance

Security Visibility

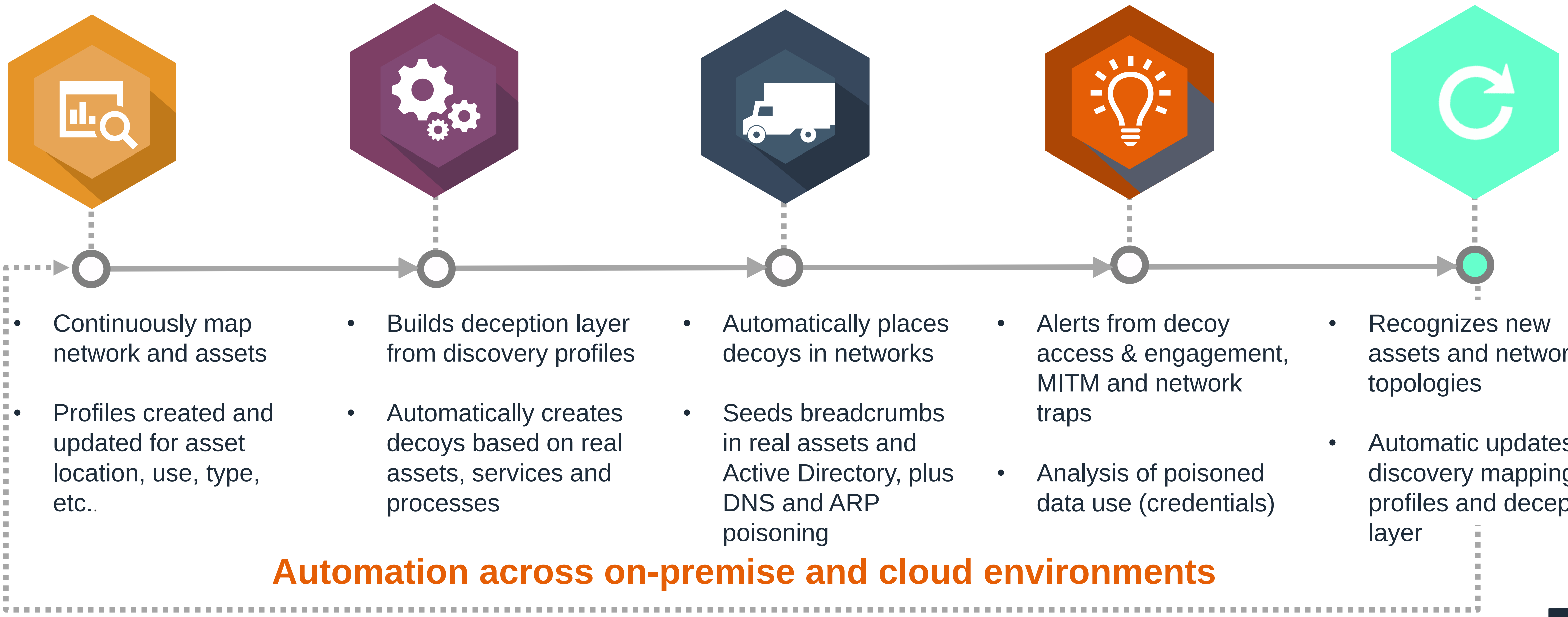
- Networks, Assets, OSs, Ports, Protocols, Networking, Paths, Applications, and Servers
- Deception Coverage
- Forensics

Integration – API, SIEMs (CEF/Syslog), Threat Intelligence (STIX/TAXII), Fidelis Network & Endpoint

No impact to operations or processes
No agents or on-demand agents
No risk to data or users

High fidelity alerts, few false positives
Visual dashboards with incident story telling
Seamless workflow with Fidelis Network & Endpoint

Fidelis Deception Approach



Discover

- Continuously map network and assets
- Profiles created and updated for asset location, use, type, etc..

Decoys

- Builds deception layer from discovery profiles
- Automatically creates decoys based on real assets, services and processes

Distribute

- Automatically places decoys in networks
- Seeds breadcrumbs in real assets and Active Directory, plus DNS and ARP poisoning

Detect

- Alerts from decoy access & engagement, MITM and network traps
- Analysis of poisoned data use (credentials)

Adapt

- Recognizes new assets and network topologies
- Automatic updates to discovery mapping, profiles and deception layer

Automation across on-premise and cloud environments