Fidelis Cybersecurity

DATASHEET

Fidelis Collector

Metadata enables fast and accurate detection of advanced threats and data theft/loss – in real-time and retrospectively.

Metadata Drives Post-Breach Detection

Content and context are critical for post breach detection and response of advanced threats and data theft or loss. Metadata is the DNA for security analysts and services to drive cross-session analysis, multi-faceted and behavior analysis. Structured and enhanced metadata are also the basis for machine learning models within specific use cases. Metadata is information about other information resulting in 90 percent of the data for about 20 percent of the expense to store it. Imagine having 10,000 recorded phone calls – you could listen to them tirelessly to learn details, however, even better would be metadata about the phone calls, including specific tags about the content and context to quickly query and investigate.

Detecting the Unknown Requires Metadata

There are multiple sources of data for post-breach detection of the unknown. NetFlow records cover the basics of sender, receiver, service, transport, date/time and duration, however, they lack content. Log collectors and SIEMs normalize unstructured data to timeline activities, correlate events and meet compliance regulations, however, they rarely detect advanced threats and data theft, and due to size queries can be slow to process. Packet captures record everything for forensics, however, you cannot query them or apply threat intelligence without significant effort to decode and reassemble. Metadata is indexed, ready to query, fast and provides content and context not seen with other data options.

Enable Real-Time and Retrospective Analysis

Fidelis Collector is an optional addition to Fidelis Network® to store metadata up to 360 days, providing hundreds of attributes of standard and enhanced metadata with the ability to define custom tags. Patented Deep Session Inspection® within Fidelis Network leveraging direct, internal, cloud and email sensors provide broad coverage of metadata, including of all ports and protocols without data sampling or dropping packets. Less is more with metadata providing massive storage savings, plus incredible optimizing and performance on queries. This enables real-time and retrospective analysis for the following use cases.

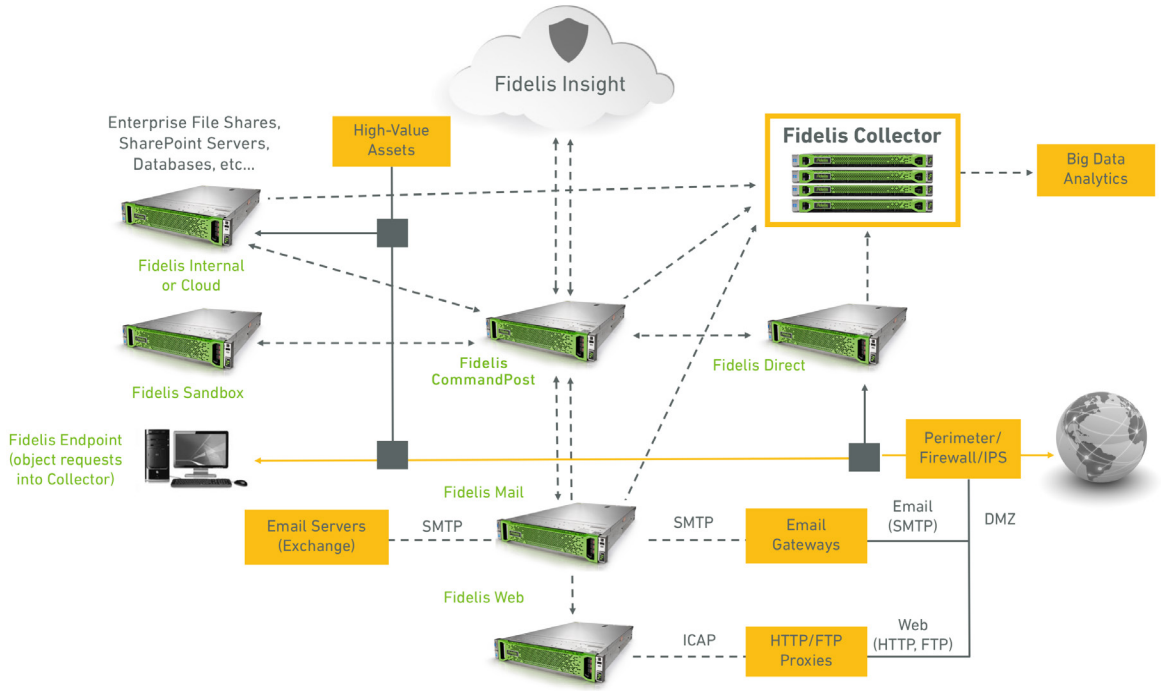
- **Investigation and Response** – pivoting and hunting by switching between content and context related to alerts for broader analysis.
- **Threat Intelligence** – automatically apply new threat intelligence for real-time and retrospective analysis.
- **Security Analytics** – search metadata across multiple axis for cross-session relations, multi-faceted related attributes, and behavioral event sequences and frequency.
- **Network Visibility** – understand network traffic and patterns not seen in firewall logs or SIEM dashboards.
- **Anomaly Detection** – using baselines to compare metadata for frequent or rare instances of attributes.

Over 300 Attributes, Plus Custom Tags

Fidelis Collector is the optional storage and analytics component of Fidelis Network. Over 300 attributes are provided for standard and enhanced metadata and includes the following as examples.

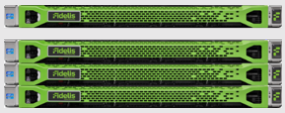
- **Application and Protocol-Level Metadata** – including attributes for web browsing and applications, social media, email, encrypted web access, internal file shares, remote connections, database content, FTP and TFTP, Telnet, BitTorrent, and many more.
- **Content Level Metadata** – including attributes for documents, executable files, archives, certificates, embedded objects, Flash, JavaScript, XML and many more.
- **Enhanced Metadata** – including attributes for alerts, threat intelligence, geo-location, policy tagging, IP2IP and many more.
- **Custom Tags** – users can define a vast array of tags and apply them to metadata.

Fidelis Collector stores metadata from direct, internal, cloud and mail sensors with analysis and queries performed within the Fidelis CommandPost administration console.



Collector Appliances or Fidelis Managed Cloud Storage

Metadata conversion equates to approximately two percent of network traffic as a rule of measurement. Duration is the storage capacity provided and then new metadata overwrites the oldest stored. No objects or files are stored and the average customer stores 60 days of metadata with the ability to expand to 360 days or beyond. There are three appliances series for Collector with the option of having them as a managed cloud service by Fidelis.

Collector SA (Stand Alone) – single appliance (2U) or VM with combined controller and database, 1Gbps peak ingest rate, 3TB storage capacity (approximately 60 days of network metadata), non-expandable, often used for Network Assessments or proof of concepts.	
Collector Enterprise Cluster – single Controller2 appliance (2U) with one or more XA2 appliance nodes (2U) providing parallel functions for performance, 1GbE copper interfaces, expandable to 25 XA2 nodes for over 75TB storage capacity (25 nodes x 3TB).	
Collector High-Capacity Cluster – single Controller 10G appliance (2U) with one or more XA4 appliance notes (4U) providing parallel functions for performance, 10GE copper of fiber interfaces, expandable to 80 XA4 nodes for over 1.6PB of storage capacity (80 nodes x 20TB)	

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.

