BLUECAT™

DNS Edge and CDM BOUND-F

The BOUND-F portion of CDM Phase 3 includes network filters and boundary controls. These tools apply sets of rules to regulate the flow of traffic on the boundaries between network enclaves, ensuring that transmission of data is restricted to authorized locations and recipients.

DNS Edge falls in the content filtering subcategory of BOUND-F. With its placement as the “first hop” recursive server, DNS Edge sits between client devices and upstream DNS servers. This allows DNS Edge to block, monitor, or redirect DNS queries from every client device on the network without the need for an on-device agent.

The unique value of DNS Edge in CDM BOUND-F

Its **placement at the client level** makes DNS Edge unique among BOUND-F offerings. Products positioned at the network boundary can identify the presence of malicious activity, but the source of that activity is obscured by the layers of DNS servers between the network boundary and the client device. DNS Edge provides the source IP, response data, query type, and other contextual information vital to identifying and cutting off “patient zero” in the event of a breach.

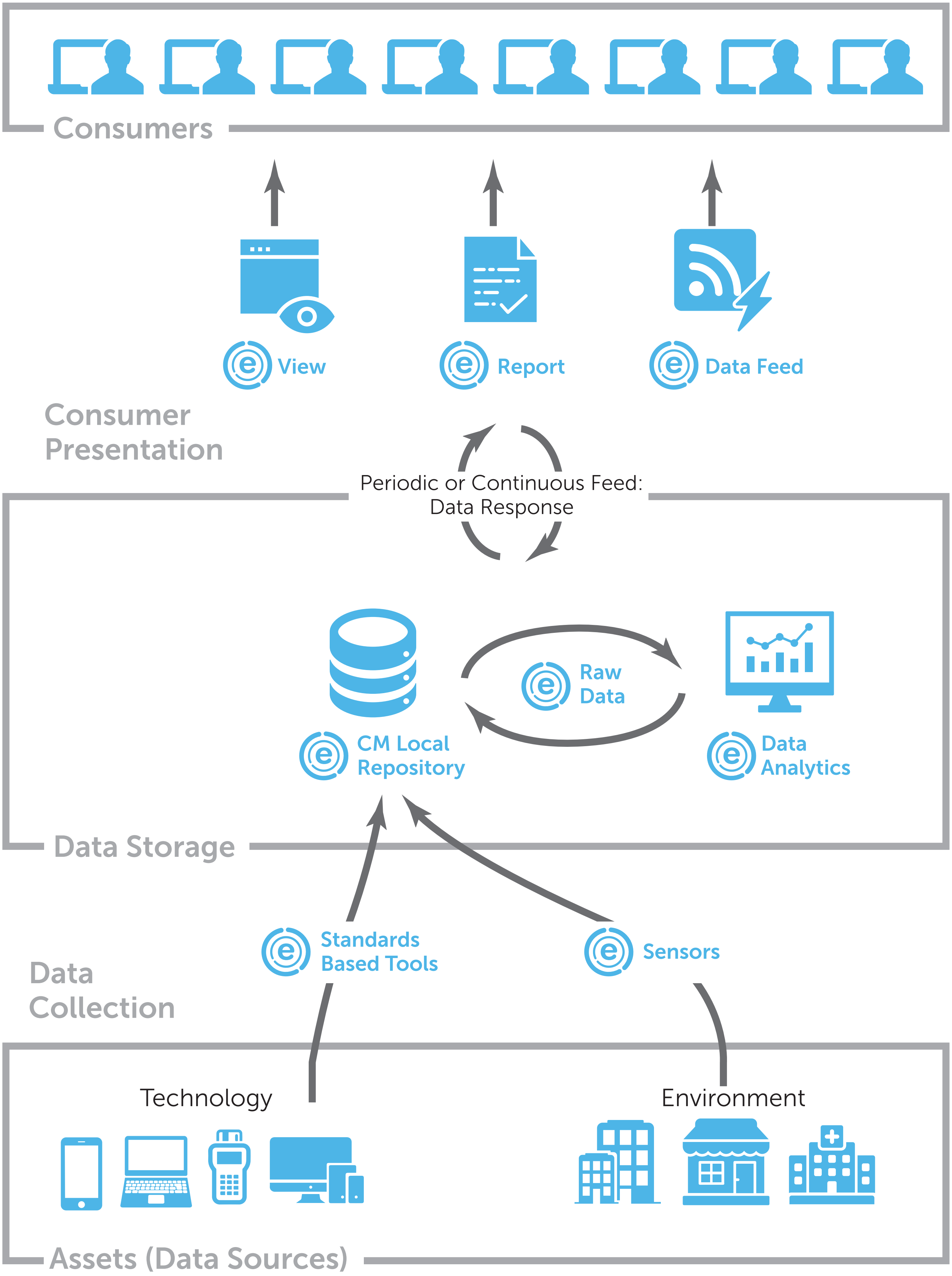
DNS Edge also **prevents lateral movement** within networks through the use of security policies to cut off unauthorized access. This makes it ideal for securing unmanaged IoT devices, hemming in advanced persistent threats, and preventing damage from malicious insiders.

DNS Edge in context: BOUND-F operational requirements, functional requirements, and tool functionality

BOUND-F Requirement	Requirement Description	DNS Edge
Operational Requirement 4.1.1.1.a	Content filtering to filter traffic based on the application content of the traffic, including both the syntax and the semantic content	DNS Edge filters content on a wide variety of indicators embedded in queries and responses, including data to identify DNS tunneling and domain generation algorithms.
Functional Requirement 4.1.1.2.a	Content filtering that directly filters traffic based on the application and application content.	Security policies in DNS Edge can be defined to filter traffic known to be associated with specific applications.
Functional Requirement 4.1.1.2.f	Boundary filtering of policies (including metadata about that policy) to determine what traffic can flow and what traffic is blocked across a boundary	DNS Edge filters traffic through security policies applied to source IPs or a set of source IPs. Policies can be applied based on a wide spectrum of DNS data.
Tool Functionality 4.1.1.3.g	Network access protection or control devices	As the first hop recursive server, DNS Edge enforces access protections and controls for both "north-south" and "east-west" traffic.

Learn more about DNS Edge and CDM Phase 3 BOUND-F at:

https://www.bluecatnetworks.com/blog/what-bluecat-brings-to-cdm-phase-3/


Consumers
View
Report
Data Feed
Consumer Presentation
Periodic or Continuous Feed:
Data Response
CM Local Repository
Raw Data
Data Analytics
Data Storage
Standards Based Tools
Sensors
Data Collection
Technology
Environment
Assets (Data Sources)