BAE SYSTEMS
INSPIRED WORK

Endpoint Monitoring with Host Agent

Endpoint is the key security battle ground

The Problem

Data is at the heart of modern businesses and the primary target for cyber criminals. The easiest way to this data is via the endpoint, making it the key target in the majority of attacks. The explosion of endpoints combined with a mobile workforce makes it increasingly difficult to gain complete visibility and protection.

Breaches at the endpoint occur through many routes. Employees, maliciously or innocently, provide access to data or credentials. People share passwords or use administrative accounts. The use of insecure storage for the transfer or disposal of sensitive information. Clicks on rogue web advertising or email. Loss or theft of devices. Not to mention intentional data theft and privilege abuse. It is easy to see why the endpoint is the key security battleground when there are so many threat vectors.

What is our Approach?

We believe that although Endpoint is the key battleground we must take a wider view on detection and response. When activity at the endpoint is given wider context from other monitoring sources across the organisation, we can quickly and confidently uncover clandestine activity. This approach delivers tremendous value when investigating and responding to attacks, cutting down the time taken, ensuring completeness of response and hampering any further threat activity related to that campaign.

Why are we doing it?

BAE Systems scoured the market for a partner who could provide the array of features and configurability supporting our vision of organisation wide detection and response. Some vendors were limited in the types of processes and data they could monitor and collect. Some were limited in the granularity and configurability. No vendors were able use flexible batching of data - either real time or batch. Vendors either ran heavy computing resource, hampering performance, or were cloud only, causing issues in data transit and connectivity. Given the available solutions did not match our requirements, we developed our own.

BAE Systems joins the Battle at the Endpoint

BAE Systems Host Agent Technology enables endpoint detection and response. The Host Agent monitors laptops, desktops and servers for the presence of advanced threats and potential misuse. A lightweight and comprehensive endpoint monitoring agent, it is able to monitor for changes in state including memory, process, network, registry and file system activity.

When combined with our real-time threat models as part of the Complete Security Monitoring (CSM) and Managed Detection and Response (MDR) Services, it can uncover hidden relationships allowing for the detection of sophisticated cyber-attacks that traditional methods typically miss and immediate and thorough remote investigations in the event of a suspected attack.

Developing a Real Customer Solution

It is important that we continue to leverage the advantages of our host agent as a means of differentiation amongst the monitoring services we offer. Host agent 3.0 brings some major improvements, most notably in monitoring coverage of roaming users. This capability is currently being rolled out and is expected to bring considerable value to our customers. Ongoing development will bring further threat coverage, by increasing the visibility of endpoint activity, and remediation capabilities, giving analysts the ability to stop or limit any ongoing attack on an endpoint.

Customer Needs

I need Faster and easier deployment of endpoint monitoring which is more scalable and flexible to support my business model.

We delivered **HTTPS communication** allowing deployment of host agent controllers in the Cloud

HTTPS allows secure communications over untrusted networks, for example the internet, which facilitates monitoring of endpoints which are roaming outside of the corporate perimeter and supports flexibility in the way the customer needs to operate.

I need increased threat detection coverage for roaming users

We delivered **Offline Data Caching** allowing activity pertinent to external and internal threats to be registered whilst not connected to the corporate network

Host Agent v3.0 monitors even if no controllers are visible to the endpoint, information is cached to local disk and uploaded next time a controller connection is made. This means malware cannot manifest on endpoints whilst offline and remain undetected when a connection to the corporate network and HAC is re-established.

I need live, real-time monitoring to take immediate action on known threats and bad behaviours and unnecessary data volumes and associated costs.

We delivered **Enhanced Real-Time Reporting** allowing increased realtime detection, faster investigation and remediation.

Host agent 3.0 provides live monitoring of the registry areas where autoruns and service are defined. This enables near real-time alerting on registry area activity without the data overload that comes with monitoring the entire registry.

I need to know that my detection is working and hasn't been disabled

We delivered **Enhanced Health Monitoring** allowing constant monitoring of the effectiveness of endpoint monitoring.

Host Agent v3.0 reports any internal errors to its controller, which allows them to be stored and analysed in a central location. The Host Agent monitoring is compatible with existing IT health monitoring systems. The health of an enterprise-wide deployment is continuously monitored and any issues quickly rectified.

I need to align data capture and communication to the resources and capabilities of my network to not denigrate business network traffic performance

We delivered **Preferred and Mandatory Controller** allowing endpoints to be segmented, ensuring no data is wrongly sent to controllers hosted in undesired locations.

Host Agent v3.0 automatically connects back to their preferred controller after a failover event. Additional configuration allows for selection of a mandatory controller. This means the host agent reverts to offline caching mode rather than a different controller, ensuring that data communication does not hamper sensitive pathways used for critical business operations.

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

UK: +44 (0) 1483 816000

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai