BAE SYSTEMS
INSPIRED WORK

Monitoring, Detection and Response for Endpoints

Convert Endpoints from potential weak spots to security strongpoints

The Problem

Speedy access to data is central to the functioning of modern organisations. It's also the target of choice for attackers. Employees and other users rely on end points: terminals, devices, printers, displays and more to find and access this data. This also makes endpoints a prime target.

More and more devices have become endpoints, often for multiple services from multiple organisations. This growth, combined with access by an increasingly flexible and transient workforce, makes it more and more difficult to understand what needs to be protected, what has been compromised and how breaches have occurred.

Data breaches often occur because an employee maliciously or innocently provides access to data or credentials. The insecure storage, transfer or disposal of sensitive information, loss or theft of devices not to mention intentional data theft and privilege abuse makes the endpoint a security battleground.

Monitoring the endpoint alone is also not the answer. It's a key and rich source of data, but the only way to detect this type of threat is to understand the behaviour of all of individual components of an attack across your organisation.

The Solution

Seeing a complete attack chain and all of its related components creates deep understanding, not least of the extent of the breach and potentially exposed sensitive data. This ultimately lessens the impact, contains the exposure and gives valuable control to ensure a swift and complete response.

BAE Systems' proprietary Host Agent provides the means to bring detection and response down to the level of individual endpoint. 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 and Big Data analytics as part of the Complete Security Monitoring (CSM) and Managed Detection and Response (MDR) Services, Host Agent uncovers hidden relationships allowing for the detection of sophisticated cyber attacks that traditional methods typically miss, enabling immediate and thorough remote investigations in the event of a suspected attack.

Host Agent Features

Detection of complex, advanced attacks

A key data source for our Threat Analytics Big Data analytics system, the Host Agent collects detailed information about an endpoint's status which can be used to directly identify malicious behaviour or to identify anomalies and suspicious patterns across an entire estate.

Remote investigation

The Host Agent provides a wide arsenal of capability to aid analysts; in the event of an attack it provides a window into each endpoint on the estate allowing immediate investigation to take place. The Host Agent can retrieve live memory images; system logs, suspicious files and registry content for forensic analysis, sweep an estate for indicators of compromise and provide snapshots of an endpoint's current state including running processes and open network ports.

(continued over)

Host Agent Features (continued)

Simple deployment and management

Deploying the Host Agent is quick and simple. Installation requires distribution of a single installer package to each endpoint using your existing deployment solution. The management controller can be supplied as either a virtual or physical appliance and BAE Systems will work closely with you to determine the most appropriate installation for your network.

Flexible and targeted monitoring

The Host Agent provides the flexibility for you to assign monitoring to machines based on operating system version, active directory properties or even user defined groupings. This allows for the most critical assets to be monitored closely without affecting the entire estate and provides a high degree of control over data volumes minimising the impact on your network infrastructure.

Proven solution

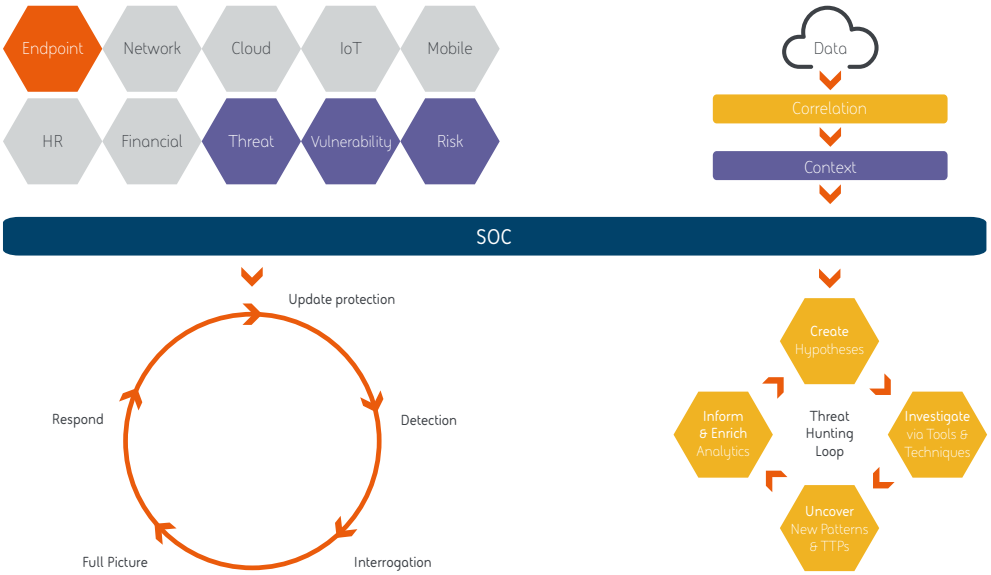
The Host Agent has been successfully deployed on over 500,000 machines across multiple client estates.

Host agent capabilities

- Process monitoring
- Network port monitoring
- Registry monitoring
- File system monitoring and investigation
- Alternate data stream detection and hash calculation
- Remote registry acquisition
- Detection of automatically-starting software
- Installed software and service listing
- Signature-sweeping for indicators of compromise (IOCs) including live process memory
- Enumerating local users and groups
- Live memory image acquisition
- Event log retrieval

Organisation-wide detection and response

Convert Endpoints from potential weak spots to security strongpoints as part of an organisation wide detection and response



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