DATA SHEET

eSentire Host Interceptor™

Quarantine of Compromised Devices

Host Interceptor works in conjunction with eSentire Network Interceptor™ to provide core network containment capabilities. Host Interceptor leverages technology and human-driven analysis to assist with the containment of laterally spreading threats within the core of the network. This provides our Security Operations Center (SOC) with real-time detection and isolation of any network connected devices deemed compromised.

Despite steeply increased spending on cybersecurity, data breaches continue to occur with alarming frequency. Cyber criminals easily bypass traditional security technology to steal customer funds and credit card data, intellectual property, and other confidential business information. More and more cyberattacks are the result of internal threats, perpetuated by the use of mobile devices used in the workplace today. Reliance on security technology doesn't solve the problem. eSentire Managed Detection and Response™ closes the gaps in traditional cybersecurity, maximizing the safety of our clients' most valuable data.

- Is agentless and easy to deploy and maintain in a cost-effective manner.
- Does not require any changes to typical network infrastructure.
- Provides SOC with visibility to devices connecting to the corporate network.
- Isolates compromised devices to minimize the impact to clients' business operations.

Identifying, Containing and Controlling Network Endpoints

Host Interceptor is delivered as a managed service combining technology that detects suspicious devices, a suite of tools that captures and analyzes rich forensic data, and human experts who engage to resolve threats that technology alone cannot prevent.

Host Interceptor is a new managed security service that enables the identification, containment and control of network endpoints exhibiting malicious behavior within the enterprise. It helps to prevent the spread of malware within the network, which may otherwise elude containment.

Working in conjunction with Network Interceptor, Host Interceptor leverages technology and human-driven analysis to identify and isolate devices deemed compromised, augmenting eSentire's endpoint behavioral analysis.

Attack and Intervention Architecture

1. Externally infected device enters corporate network
2. Infected device calls command-and-control server
3. Infected device weaponizes
4. Network Interceptor detects suspicious traffic
5. SOC sends command to Host Interceptor which isolates the infected device