SOLUTION OVERVIEW

ENDPOINT SECURITY

Protection and response for your network end points

Endpoint Protection and Response stops threats and coordinates enforcement with network and cloud security to prevent successful cyberattacks; blocking known and unknown malware, exploits, and ransomware by observing attack techniques and behaviors.

The threat landscape and adversary strategies have evolved from simple malware distribution to a broad set of automated, targeted, and sophisticated attacks that can bypass traditional endpoint protection. This has forced organizations to deploy multiple products from different vendors to protect against, detect, and respond to these threats. Endpoint security brings powerful endpoint protection technology together with critical endpoint detection and response (EDR) capabilities in a single agent.

STOP MALWARE AND RANSOMWARE

Prevent the launching of malicious executable files, DLLs, and Office macros with multiple methods of prevention, reducing the attack surface and increasing the accuracy of malware prevention. This approach prevents known and unknown malware from infecting endpoints by combining:

- Local analysis via machine learning: Examine hundreds of characteristics of a file without relying on prior knowledge of the threat and deliver instantaneous verdicts
- Deep inspection of unknown files, combining the benefits of multiple independent techniques, including static, dynamic, and bare metal analysis - for high-fidelity and evasion-resistant threat identification.
- Scanning for dormant malware: Perform scheduled or on-demand scans for malicious executable files, DLLs, and Office macros to remediate them without malicious files being opened.

BLOCK EXPLOITS AND FILE-LESS ATTACKS

Rather than focusing on individual attacks, block the exploit techniques used in an attack. By doing so at each step in an exploit attempt, you break the attack lifecycle and renders threats ineffective, using multiple methods to prevent exploits:

- Pre-exploit protection blocks reconnaissance and vulnerability-profiling techniques before they launch exploit attacks, effectively preventing attacks.
- Technique-based exploit prevention works to prevent known and zero-day exploits, without any prior knowledge of the threats, by blocking the techniques attackers use to manipulate legitimate applications.
- Kernel exploit prevention is able to prevent exploits that take advantage of vulnerabilities in the operating system kernel to create processes with escalated, system-level privileges; also preventing injection techniques used to load and run malicious codes, such as those used in the WannaCry and NotPetya attacks.

IN PARTNERSHIP

aruba
a Hewlett Packard Enterprise company

Ensign Communications Ltd
Unit 10 Winchester Place
North Street, Poole, BH15 1NX

03330 150 250
info@ensign-net.co.uk
www.ensign-net.co.uk

LEVERAGE BEHAVIOUR BASED PROTECTION

Sophisticated attacks that use multiple legitimate applications and processes for malicious operations have become more common, are hard to detect, and require visibility to correlate malicious behaviour. For behaviour-based protection to be effective, including identification of malicious activity occurring within legitimate processes, it's critical to understand everything happening on the endpoint.

- **Behavioral Threat Protection** detects and stops attack activity by monitoring for malicious sequences of events across processes and terminating attacks when detected.
- **Granular Child Process Protection** prevents script-based and fileless attacks used to deliver malware by blocking known processes from launching child processes commonly used to bypass security.
- **Behavior-Based Ransomware Protection** safeguards you against encryption-based behavior associated with ransomware by analyzing and stopping ransomware activity before any data loss occurs.

INVESTIGATE AND RESPOND TO ATTACKS

To facilitate faster response and investigation, a number of actions admins can be used to further the investigation, collect necessary information, and take action to make any changes to the endpoint in question. Following an alert or investigation, when remediation on the endpoint is needed, administrators have the option to:

- **Isolate endpoints** by halting all network access on compromised endpoints except for traffic to your endpoint management service, preventing them from communicating with and infecting other endpoints.
- **Quarantine malicious files** and remove them from their working directories.
- **File retrieval** allows admins to pull specific files from endpoints under investigation for further analysis.
- **Terminate processes** to stop any running malware from continuing to perform malicious activity on the endpoint.
- **Block additional executions** of a given file by blacklisting it in the policy.
- **Initiate live terminal connection** to the endpoint to navigate/manage files, explore the registry, run command line, and manage processes.

PROTECT CONSISTENCY ACROSS OPERATING SYSTEMS

Using multiple methods of prevention to consistently protect endpoints running all major operating systems—Windows®, macOS®, Linux, and Android®, by stopping known and unknown attacks before they compromise systems. In contrast, native OS security features only protect their respective endpoints, which creates fragmented protection, leaves the endpoints vulnerable to attacks, and slows down incident response.

Coordinate Enforcement with Network and Cloud

Traps tightly integrates with WildFire and the Next-Generation Firewall to broaden the perspective for endpoint attacks. This integration enables a continually improving security posture, including coordinated prevention from zero-day attacks.

DETECT, INVESTIGATE AND RESPOND TO THREATS

Store all event and incident data captured, using a first detection and response app that natively integrates network, endpoint and cloud data to stop sophisticated attacks. Speed up alert triage and incident response by providing a complete picture of each threat and revealing the root cause automatically.

By stitching different types of data together and simplifying investigations, you will reduces the time and experience required at every stage of security operations, from triage to threat hunting.

IN PARTNERSHIP

a Hewlett Packard Enterprise company

Ensign Communications Ltd
Unit 10 Winchester Place
North Street, Poole, BH15 1NX

03330 150 250
info@ensign-net.co.uk
www.ensign-net.co.uk