GUIDANCE SOFTWARE is now opentext™

HPE Security ArcSight + EnCase Endpoint Security

APPLYING ENDPOINT DATA FOR FASTER, SMARTER INCIDENT RESPONSE

Endpoint data is critical to quickly validate alerts and remediate threats.

Security teams face an overwhelming volume of security alerts. As a result, they often spend an inordinate amount of time, energy, and resources dealing with alerts – or worse yet – ignore some alerts altogether. Working together, HPE Security ArcSight and EnCase Endpoint Security help reduce alert fatigue and reduce the time to identify, triage, and mitigate threats.

Any alerts generated via HPE ArcSight will automatically trigger EnCase Endpoint Security to rapidly scan endpoints for potential intrusions. Integrated threat intelligence then instantly analyzes and contextualizes endpoint data to provide clear threat scores. This allows security teams to focus on high-priority activities and, if needed, launch forensic-grade remediation to completely eradicate threats and return networks back to a trusted state.

Prioritizing what threats to look at and respond to is the foundation for effective security management.

With HPE ArcSight and EnCase Endpoint Security, teams can improve their signal-to-noise ratio, overall security effectiveness, and ROI.

experts@guid.com

KEY BENEFITS:

- Reduced time to identify, triage, and mitigate threats, resulting in fewer false alarms and less alert fatigue
- Automated threat validation and clear threat scoring to understand which events are important, or not.
- Kernel-level visibility into all endpoints
- Maximize the value of your security investments
- Ability to create a forensic record of any incident for reporting, compliance, and working with law enforcement

Use Cases

Manage the volume of incoming alerts through integration

The integration between ArcSight and Endpoint Security helps triage security alerts by automatically examining suspect machines to eliminate false positives. With Endpoint Security, security analysts are able to:

- Understand which events are most important and require immediate attention
- Determine if malware actually executed based on information gathered from endpoints
- Close the gap between receiving an alert and responding to a threat by quickly examining the target machine(s)
- Prioritize alerts by determining whether there was lateral spread to quickly isolate machines and contain the threat

Accurately triage and remediate all traces of an intrusion

After validation and scope of assessment, EnCase Endpoint Security can launch remediation commands, allowing incident responders to completely eradicate a threat and return systems back to a trusted state.

- Using endpoint telemetry data and automated threat scoring, Tier 1 security analysts receive clear threat scores that indicate the presence of potential threats
- The Tier 1 analyst can then escalate suspicious activities to Tier 2 incident responders for investigation or remediation - which can be conducted without the need to wipe and reimage
- Tier 3 digital forensic incident responders can then launch forensic investigations like reverse engineering, threat hunting, and intelligence gathering

Validate the existence of detected intrusion on endpoints

HPE ArcSight alert data is automatically passed to EnCase Endpoint Security to quickly validate alerts by investigating target endpoints for telemetry on both known and unknown threats. With Endpoint Security, users are able to:

- Gain real-time glimpse into the state of a compromised computer at the time of the attack
- Understand what level of action is necessary to remediate the problem
- Capture ephemeral endpoint data in near real time

More Info

For additional Guidance Software information visit: guidancesoftware.com/encase-endpoint-security

For additional HPE Security information visit: hpe.com/software

GUIDANCE SOFTWARE

Hewlett Packard Enterprise

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 35 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.

ABOUT HPE SECURITY

HPE is leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading profits from HPE Security ArcSight, HPE Security Fortify, and HPE Security—Data Security, the HPE Security Intelligence Platform uniquely delivers the advance correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Guidance Software®, EnCase®, EnForce™ and Tableau™ are trademarks owned by Guidance Software and may not be used without prior written permission. All other trademarks and copyrights are the property of their respective owners.