GUIDANCE SOFTWARE is now

opentext™

EnCase® Endpoint Security + Splunk®

ENDPOINT VISIBILITY EMPOWERING AUTOMATED RESPONSE

You are using Splunk® Enterprise to monitor your security operations, aggregating logs, clickstreams, sensors, network traffic, application data, cloud services, and more to keep sensitive data safe and secure. However, you may be missing one vital connection. Endpoint activity data is critical to quickly validate alerts and remediate threats.

How do you protect against threats you cannot see?

With Splunk + EnCase Endpoint Security, you can close the gap between alert and response. EnCase Endpoint Security provides 360-degree visibility into the target of attacks — the endpoint — and automated response actions enrich Splunk visualizations with details on specific incident effects. With this information, security teams have the power to take definitive remediation actions without bringing systems offline.

MANAGE THE VOLUME OF INCOMING ALERTS THROUGH INTEGRATION.

Splunk alert data is automatically passed to EnCase Endpoint Security to apply advanced detection and best-of-breed threat intelligence to determine if malware actually executed based on information gathered from endpoints. After validation and scope assessment, EnCase Endpoint Security launches remediation commands, allowing incident responders to completely eradicate a threat and return the network to a trusted state.

By integrating Splunk with EnCase Endpoint Security, security teams can quickly answer pertinent questions about the source and scope of a threat, including:

- **Which events are most important?**
- **Was the attack successful?**
- **Was sensitive data compromised?**
- **Was there lateral spread?**
- **What actions are necessary to remediate the problem?**

This integration makes it simple for Splunk to invoke any combination of actions from EnCase Endpoint Security. Triggers can be set to any level of granularity and can be based on a variety of thresholds, trend-based conditions, and complex patterns, such as those exhibited by brute force attacks and fraud scenarios to automate the response process.

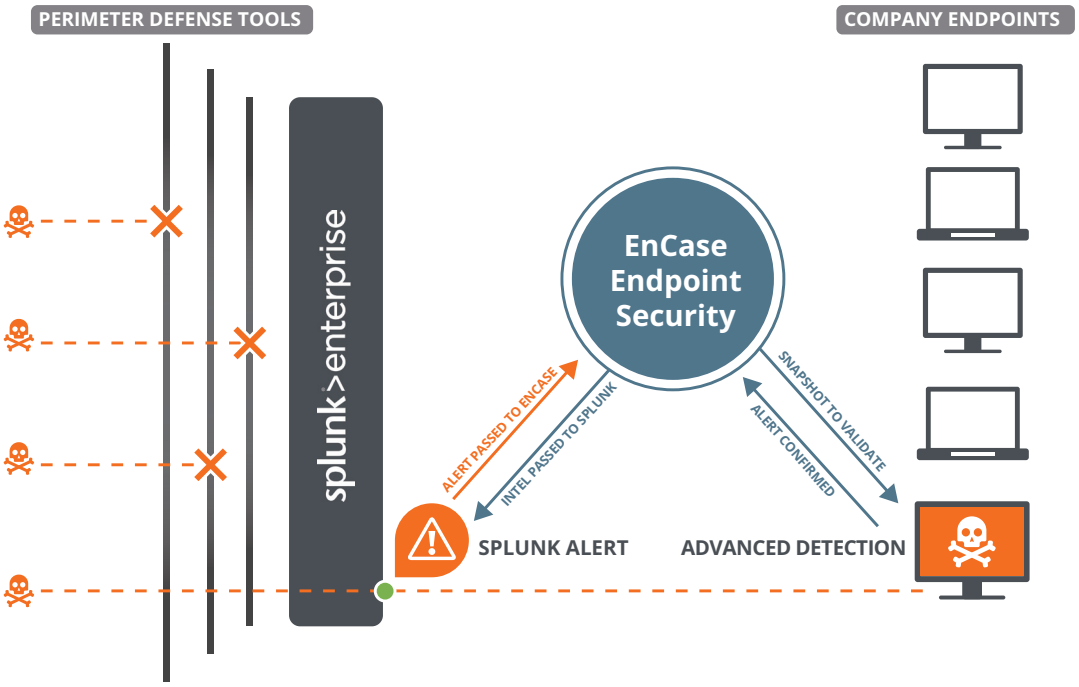
USE CASES INCLUDE:

- Validating the existence of detected intrusion on endpoints
- Understanding immediately if sensitive data is at risk
- Capturing ephemeral endpoint data in near real time
- Accurately triaging and remediating all traces of any intrusion

experts@guid.com

guidancesoftware.com

THE COMBINATION OF SPLUNK ENTERPRISE AND ENCASE ENDPOINT SECURITY DELIVERS THE MOST COMPREHENSIVE VISIBILITY INTO NETWORK AND ENDPOINT THREAT INFORMATION AND PROVIDES POWERFUL REMEDIATION CAPABILITIES.



How it works

1. Splunk is configured to trigger response actions on critical conditions
2. Once conditions are met, Splunk event data is sent to EnCase Endpoint Security — automatically triggering response
3. Results are passed to a .csv file, ready for pickup by Splunk for further analysis

ABOUT ENCASE ENDPOINT SECURITY

EnCase Endpoint Security, the gold standard for digital investigations, is built on proven forensic security technology. EnCase Endpoint Security is driven by forensics processes and technologies configured to automatically deliver a complete, unobstructed view of the endpoint the moment an alert is received. A lightweight agent on each system performs all needed activities and can be disguised to prevent deletion by malware or notice by malicious insiders. The entire operation is invisible to users to avoid disruption or tipping off potential suspects, and works on a wide variety of operating systems for laptops, desktops, file servers, email servers, print servers and even POS systems. This ensures that as attackers adopt new techniques your security technology can adapt to meet the challenges associated with detecting zero-day and unknown threats.

ABOUT SPLUNK ENTERPRISE

The Splunk Platform for Operational Intelligence monitors and analyzes everything from customer clickstreams and transactions to security events and network activity. Splunk Enterprise helps you gain valuable operational intelligence from your machine-generated data. And with a full range of powerful search, visualization, and prepackaged content for use-cases, any user can quickly discover and share insights. Just point your raw data at Splunk Enterprise and start analyzing your world.

GUIDANCE SOFTWARE

From beginning to endpoint.

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.