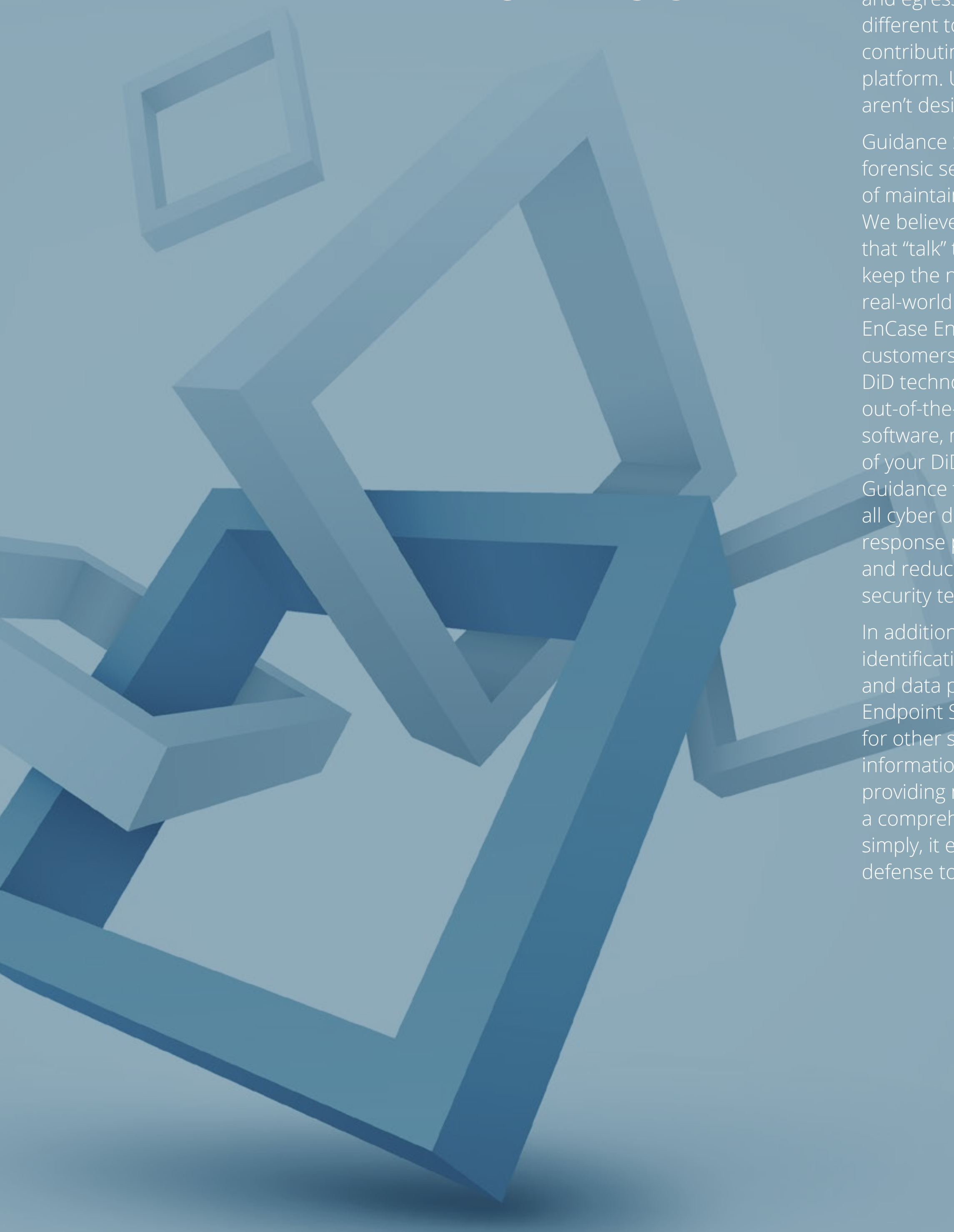
THE ENCASE® ENDPOINT SECURITY COMPLEMENT GUIDE

GUIDANCE SOFTWARE™

From beginning to endpoint.



HELPING CYBER DEFENSES WORK TOGETHER

In a Defense-in-Depth (DiD) security plan, multiple layers of security walls placed throughout the network create a “castle approach” to address potential vulnerabilities at several levels by monitoring major ingress and egress points. DiD systems employ many different tools with individual functions, all contributing to the success of the overall platform. Unfortunately, these tools often aren’t designed to work together.

Guidance Software, the global leader in forensic security, understands the problem of maintaining continuity between DiD tools. We believe the best security requires tools that “talk” to each other and work together to keep the network safe. With over 20 years of real-world experience, we’ve developed our EnCase Endpoint Security platform to help customers maximize investments in other DiD technologies. The result: tools with strong out-of-the-box connections with other security software, making each individual component of your DiD defense more powerful. Guidance technology enables a synergy of all cyber defenses, automating the incident response process to ensure faster decisions and reduce the number of false positives for security teams.

In addition to self-contained malware identification, data audit, incident response, and data preservation capabilities, EnCase Endpoint Security acts as a force-multiplier for other security technologies by auditing information on endpoint devices and providing meaningful response capabilities to a comprehensive network security plan. Put simply, it enables the individual layers in your defense to be the best they can be.

OVERVIEW

This document provides insight into how EnCase Endpoint Security software integrates with and amplifies the products and solutions that contribute to a comprehensive approach to enterprise security, maximizing security investments and initiatives. It answers these questions:

- **In what areas can EnCase Endpoint Security enhance existing investments in enterprise security?**
- **Which products complement EnCase Endpoint Security?**

There are an overwhelming number of data collection points that solve one or more security processes. This document references only those solutions typically associated with industry and vendor specifications in the categories of:

- **Automated Alerting Technologies**
- **Structured Data Repositories (such as DropBox)**
- **Threat Intelligence**
- **Asset Management**
- **Open Source Incident Response Tools**

IN A NUTSHELL

HOW ENCASE ENDPOINT SECURITY WORKS

Every day, hundreds of thousands of alerts are generated by the individual components of a DiD system. However, these components have no way to validate, triage, and analyze each event for signs of potential trouble. That's where EnCase Endpoint Security comes in. The EnCase Endpoint Security platform – designed specifically to coordinate with other tools – can be programmed to detect alerts that may pose a problem by validating information on the endpoint and verifying whether the event merits further investigation. It also enables security teams to access pertinent data more quickly to stop any potential data breach in its tracks.

EnCase Endpoint Security organizes data points into a timeline with individual events flanked by condensed information about what happened before and after the event. Armed with this intelligence, your security team can:

- Verify the individual components of a potential threat
- Search other endpoints for the same threat
- Remediate the issue using EnCase Endpoint Security

AUTOMATED ALERTING TECHNOLOGIES

Increasingly distributed and complex IT environments are challenging to manage – making security information and event management (SIEM) and log analysis a necessary part of enterprise security infrastructure. SIEM combines two key elements into one security management system:

- Security Event Management (SEM) centralizes the storage and interpretation of logs and allows near real-time analysis, enabling security personnel to take defensive actions more quickly
- Security Information Management (SIM) collects data into a central repository for trend analysis and provides automated reporting for compliance and centralized reporting

By uniting these two functions, SIEM tools provide quicker identification, analysis and recovery of security events. They also allow compliance managers to confirm that they are fulfilling an organization's legal compliance requirements.

SIEM INTEGRATION WITH ENCASE ENDPOINT SECURITY

EnCase Endpoint Security can be used to respond to various types of alerts and validate whether a security event actually happened. Although SIEM tools generate advanced correlation across many systems to issue alerts, they neither validate from the target host whether an event actually took place nor evaluate the extent of the compromise.

EnCase Endpoint Security enables you to take that critical final response step after an event has been identified. It accepts alerts generated by SIEM tools and automatically takes a real-time incident response "snapshot" of the affected systems' volatile data at the moment the alert is generated and subsequent snapshots to observe changes over time. If a malicious process is detected, EnCase Endpoint Security can return your machine to a trusted state and sweep the rest of the network for additional instances of the threat or similar versions.

Users can also schedule regular scans against past threats to ensure the same or similar threats aren't reintroduced into your network.

APT DETECTION TECHNOLOGY INTEGRATION WITH ENCASE ENDPOINT SECURITY

EnCase Endpoint Security can be used to respond to events automatically or manually. As with SIEM technologies, it integrates with existing advanced persistent threat (APT) detection solutions to capture endpoint snapshots. Immediate analysis from the source and the target machine can reveal details of known, unknown, or hidden processes, as well as TCP network socket information, open files, device drivers, services, and more. This intelligence can reveal whether machines have been compromised, virtually eliminating false positives.

Subsequent automated snapshots are triggered shortly after the event to show attack results in time slices. This enables security teams to determine if an event has actually occurred, in which case the impact and origin are visible. Security teams can use the same snapshot capability to quickly isolate and respond to security incidents manually. After confirming that a security event took place, EnCase Endpoint Security can analyze computers across your entire enterprise to find other machines compromised by the same or similar threats.

Most organizations have already adopted APT detection and sandboxing solutions that help automatically identify, act upon, and stop such threats from spreading beyond the initial infection point. Typically, such technologies feed data to a next-generation intrusion prevention system (IPS) that helps ensure that an organization's critical data remains secure, without impacting productivity and operations.

INTRUSION PREVENTION INTEGRATION WITH ENCASE ENDPOINT SECURITY

EnCase Endpoint Security can determine if unknown threats have bypassed an IPS or verify whether the responses of an IPS have been successful in protecting a targeted host. Through a connection (either direct or through a SIM) to the IPS, EnCase Endpoint Security can collect information from the affected machine at the time the alert is generated and perform subsequent scans to ensure that the malicious data was in fact blocked.

Managing all of these technologies can become exceedingly difficult. A comprehensive security analytics platform is necessary to deliver 360-degree network security visibility, advanced network forensics, and real-time threat detection for all network activity.

SECURITY ANALYTICS PLATFORM INTEGRATION WITH ENCASE ENDPOINT SECURITY

Integrating EnCase Endpoint Security with a security analytics platform enables an enterprise to proactively identify and validate undetected threats wherever they occur, protecting against advanced malware and zero-day attacks across the network and endpoints.

EnCase Endpoint Security is driven by experience-validated forensics processes and technologies configured to automatically deliver a complete, unobstructed view of the endpoint the moment an alert is received. A tiny, passive service on each system performs all needed activities and can be disguised to prevent deletion by malware or notice by malicious insiders. The multi-platform solution is undetectable 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 point-of-sale (POS) systems. The unique features of EnCase Endpoint Security helps users meet the challenges of detecting zero-day and unknown threats; like, for example, when attackers adopt new techniques or exploit new vulnerabilities.

THREAT INTELLIGENCE

Threat Intelligence is how threats are identified, classified, and alerted. But more than just an alerting feature, threat intelligence integrates into sources and relays this information to the cloud – creating an interactive knowledge source to keep devices secure with up-to-date intelligence.

INTEGRATION WITH ENCASE ENDPOINT SECURITY

EnCase Endpoint Security has the ability to quickly send potentially malicious files to threat intelligence applications for additional analysis and sandboxing. This enables incident responders to efficiently investigate suspicious files and dramatically reduce false positives, saving time and effort. With EnCase Endpoint Security, response teams have more time to focus on other priorities.

AGENT MANAGEMENT

A misconfigured agent can cause significant loss. With EnCase Endpoint Security, users can manage agents properly to ensure they have the right configurations, security settings, and permissions.

INTEGRATION WITH ENCASE ENDPOINT SECURITY

EnCase Endpoint Security can dig into agent endpoints and run a host of proactive and reactive processes to prevent, identify, or remove compromises. It can automatically verify the integrity of static files and processes running on a system. Finally, it can gather additional information such as data from the registry, file system, and network settings to identify whether a machine has been compromised.

EnCase Endpoint Security complements existing information security tools that block or quarantine data (such as firewalls, intrusion prevention systems, antivirus, or data loss prevention tools) or that trigger or correlate alerts (such as intrusion detection systems, configuration management, or SIM and SIEM tools). It provides:

- The ability to identify and analyze undiscovered threats, such as polymorphic or metamorphic malware, packed files, and other advanced hacking techniques that evade traditional network- or host-based defenses
- Risk mitigation by removing malware and malware artifacts from hard drives, RAM, and the Windows Registry on laptops, desktops, and servers
- Visibility into endpoint risk, leveraging disk-level forensic access to data on endpoints, with the ability to compare endpoints against a trusted baseline and/or an included hash database (both whitelist and blacklist)

McAfee ePolicy
Orchestrator

OPEN SOURCE TOOLS

Drawing on more than 20 years of experience in forensic digital investigation, EnCase Endpoint Security was designed as a best-in-class tool to not just detect, but combat and neutralize hackers. As part of that strategy, Guidance built a user interface that seamlessly integrates with the most popular open-source applications. This enables incident responders to be more efficient without the need to upgrade or purchase additional integration software.

Our open source toolkit improves your IR team's productivity and speed by:

- Streamlining and optimizing your existing unique processes
- Organizing incident response analysis and reporting through one central user interface
- Maximizing the capability of each open-source tool by extending reach to all endpoints
- Reducing the learning curve for incident responders by replacing command line operations with point-and-click functionality

Incident Responders can be more confident in their analysis of endpoint data with EnCase Endpoint Security and its integration with the following most popular open source tools:

- **Strings**
- **PDF Parser by Didier Stevens**
- **Find Temp Executable Search**
- **MD5 Module**
- **PreFetch Parser by Yogesh Khatri**
- **Disk Capture**
- **MFT Parser by Kelcey Tietje**
- **MWD Registry Search**
- **RegRipper by Harlan Carvey**
- **Malware Grab**
- **UsnJrnl Parser by Lance Mueller**
- **Ram Dump**
- **Volatility for Windows, Linux & Mac**
- **Malware Entropy Date Range Search**
- **Known Malware Paths Search**

CONCLUSION:

The components of DiD security plan are only as effective as their ability to work together. Security tools need to go beyond reporting breaches and help security teams understand which ones may be serious and how to quickly remediate them. EnCase Endpoint Security is supported by the pioneers and foremost experts in forensic security and stands alone in its ability to integrate all protective layers into a unified platform to quickly and accurately understand and address potential data breaches. EnCase Endpoint Security offers peace of mind and the knowledge that security solutions are performing to the highest standard available.

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 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.