GUIDANCE SOFTWARE

From beginning to endpoint.

360° ENDPOINT THREAT ASSESSMENT SERVICE

Cyberespionage, hacktivism, and cybercrime syndicates create ongoing security hazards for businesses and organizations. Guidance Software enables customers to keep pace with these threats, utilizing cutting edge detection, analytics, and forensic expertise. The new 360° Threat Assessment Service from Guidance locates active adversaries that may be present on your network and identifies signs of past breaches so security teams can take action. Guidance can be complete a comprehensive assessment in a single week without organizational disruption.

Three transformational technologies have been combined into a new assessment service:

Deep Forensic Visibility
Guidance can find malware in memory, or locate its residue on the disk. The forensic trail of user accounts provide an edge when investigating Command and Control activity.

Advanced Analytics
A Guidance assessment delivers multi-pronged detection, including analytics, machine learning, and behavioral analysis. Detection modules provide weighted votes, expressed as a unified threat score that clearly shows malware, rogue user accounts, and unauthorized lateral movement.

Cloud-Based Agentless Architecture
Eliminates installations, change management delays, and agent deployments so collections can begin on day one.

- Ensure adversaries are not active in your network
- Sanitize your organization before major deployments
- Augment your capabilities with new analytics, artificial intelligence and forensics technologies

Experience firsthand how these technologies enable the shortest detection and response SLAs in the industry while saving you money.

experts@guid.com

guidancesoftware.com

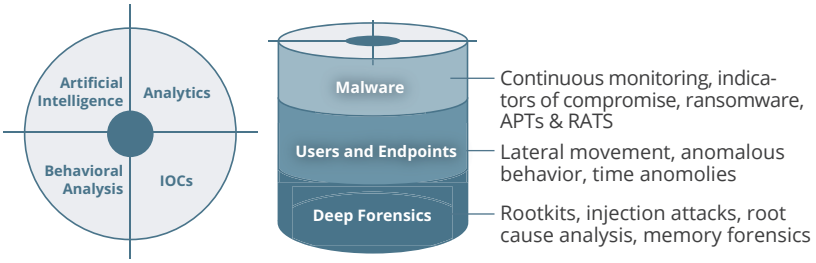
SCIENCE OF THREAT DETECTION AT FORENSIC DEPTH

We leverage a neural network utilizing artificial intelligence to detect the latest ransomware, advanced persistent threats (APTs) and remote access trojans (RATs), including their polymorphic variants and the latest Indicators of Compromise (IOC) to find known threats.

Unlike typical analytics approaches that can take a month or longer, we can detect anomalies from day one. Guidance provides 360-degree visibility into your endpoints and sees anomalous user and endpoint behavior, which can signal an active adversary.

The ability to operate off forensic artifacts is paramount, as malware may be long gone from your environment, or operate below OS awareness. Behavioral analysis scores forensic residue, detecting signs of injection in memory, time sequence anomalies, and examines installation methods for root cause analysis.

DEEP FORENSIC THREAT SCORING



RAPID TRIAGE

Outlier Analytics approach reduces automates threat scoring behavior and forensic evidence analysis to reduce time and cost of investigations.

AGENTLESS ARCHITECTURE BYPASSES CHANGE MANAGEMENT

This service is delivered from the cloud and utilizes agentless technology. This enables Guidance Services to be up and running faster than any services team in the industry. Endpoint control occurs over the existing SMB port, already open in standard networks. Collections occur in micro-increments and are extremely light on the wire, avoiding end user disruptions.

PEACE OF MIND IN ONE WEEK'S TIME

Threat- Assesment Steps

1. **Setup:** A single task scheduler component -- which can fit on a laptop can be downloaded and installed in minutes. This single component talks to the cloud on port 443.
2. **Collection:** A light-weight scan ensures no end user disruption. Unlike other analytic solutions, Outlier Analytics doesn't require prior knowledge of your network and only a single scan is needed.
3. **Analytics:** Endpoint processes, binaries, logs, forensic disk and memory artifacts are all run through multi-tier analytics. Ten detection modules employ machine learning, forensic behavioral analysis, and IOC signature scans to find threats.
4. **Triage:** Endpoint alerts are vetted at extremely rapid rates. Our technology makes this possible through automated forensic and malware analyses.
5. **Actionable Findings:** In one week's time, Guidance will determine if you've been compromised and you will receive a detailed report regarding the malware, user, and endpoint threats with insights about lateral movement and any command and control activity. Finally, recommendations for investigative and remediation steps will be provided.

GUIDANCE SOFTWARE DIFFERENCE

- Guidance Services are field-tested and court-proven.
- Guidance has a long history of delivering incident response services to the largest businesses & agencies in the world.
- Guidance is the global leader in digital forensics. Our solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, Service providers such as FireEye, KP&G and Kroll all utilize Guidance technology.
- We provide comprehensive threat detection using multi-layered endpoint analytics — with no time required for agent deployment and no disruption to business activity

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

experts@guid.com

guidancesoftware.com