EnCase Endpoint Security

360° VISIBILITY

Why Nothing Less Will Do for Risk and Security Teams

GUIDANCE SOFTWARE™

From beginning to endpoint.

In the IT arena, 99% reliability is often cited as an acceptable standard. Or, is it? If that benchmark was applied to air travel, there would be an average of 300,000 plane crashes a year! At 99% reliability, critical structures such as freeway bridges, would crack or collapse at 50x their current rate in the US alone. How many travelers would be willing to board a flight or cross a bridge with this level of risk?

We know from experience that when it comes to risk and security involving your systems, anything less than complete detection and resolution is unacceptable. Guidance Software, makers of EnCase, is the global leader in forensic security. Our technology has helped IT professionals identify and mitigate digital threats where a 1%-- or even .1%-- failure rate would trigger disaster for their businesses. We attain that level of performance through our 360° visibility approach to cyber threat detection and response. 360° visibility is critical for incident responders because attackers are increasingly sophisticated at evading detection by fooling operating system level queries. Guidance Software's lightweight agent works at the endpoint to identify and remediate threats at the kernel level, where intruders cannot hide their digital footprints.

Guidance pioneered the discipline of digital investigations working with law enforcement in late 1990s. Our technology has evolved over the past 19 years, and today, our endpoint security solutions provide peace of mind to corporate enterprises and government agencies by addressing the advanced persistent threats that get through traditional cyber defense strategies.

360° VISIBILITY MEANS:

TRUE DETECTION

The forensic security enabled by 360° visibility helps IR teams to quickly find known threats by ingesting IOC's and leveraging whitelists & blacklists, as well as detect unknown threats through behavior analysis. Incident Responders can then perform root cause analysis, establish a timeline for an incident, and be aware of an attacker's attempt at obfuscating their activities at the OS or Application levels.

COMPLETE RESPONSE

Forensic security provides IR teams the ability to surgically remediate all iterations of a threat by killing all processes from the malicious code, deleting any files that spawned it, and resetting the registry keys-- which kills any persistence mechanism of that attack.

REDUCED DOWNTIME

To us, *complete and effective* response goes far *beyond* merely containing a threat, or accepting that wiping and reimaging a machine is the only suitable remedy to return the network to a trusted state-- despite all of the resulting endpoint downtime. We know that time is money, and partner with you to prevent losses.

Our digital solutions heritage makes Guidance Software the only cybersecurity company with a security-forensic technology stack that provides 360° visibility into all stages of a security breach.

Every interaction a user or software has with an endpoint leaves forensic residue. Our software empowers our customers to travel back in time and examine virtually all activities that have touched a compromised system without the need to install resource-intensive monitoring software.

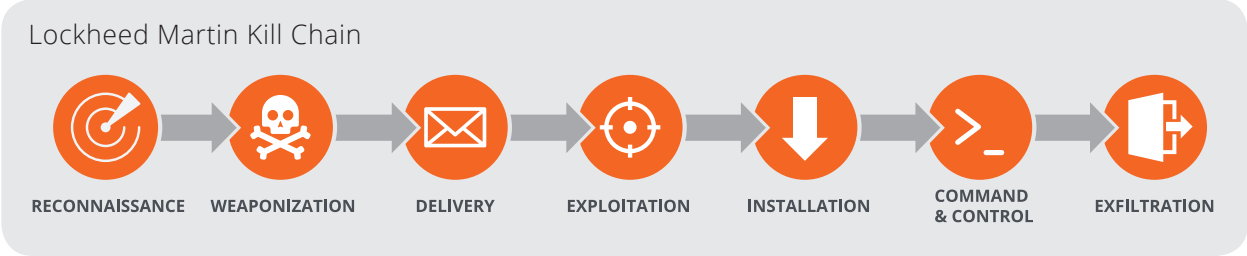
FORENSIC LEVEL DEPTH TRUMPS SPEED

Much is made of speed and how quickly security tools can run queries on certain endpoints. From our experience, incident response is comparable to surgery. A speedy operation may be necessary if the patient is in a life-or-death circumstance requiring instant action. Given a choice, however, most surgeons would prefer a more thorough, meticulous approach. A lack of detail could lead to later complications or less successful results for the patient. Like a surgeon during an operation, IR teams are better off seeing more data, enabling full visibility of what's happening across their organizations. Quick fixes can lead to undesirable results. A broader depth of view empowers incident responders to understand and address the root cause and full impacts of a data breach.

What really differentiates Guidance's security forensic technology is our visibility into the forensic residue on the endpoint by every application interaction. Unlike some security vendors, we get into the trenches to see beyond this shallow level. We can investigate the nooks and crannies of file systems and memory that OS vendors never intended us to view. Our solutions support digital investigations in memory, email, as well as cloud and on-premises repositories.

THE CYBER KILL CHAIN

Lockheed Martin authored the seven-stage "kill chain" model to describe common procedures hackers exercise during a security breach. This is an excellent benchmark for your security awareness and ability to detect ongoing breaches. Guidance provides discreet yet vital 360° visibility into the entirety of a security breach. Let's consider the cyber kill chain, a popular model describing the seven different activities attackers pursue during security breaches:



EARLY STAGES

Initially hackers operate on the public internet in the reconnaissance stage, and build custom tools in the weaponization stage. The final five stages of kill chain activity, occurring within your network, are the most relevant in this post-perimeter world. Why does that matter? Deep forensic technology unveils all stages of an attack.

DELIVERY STAGE

The next stage progresses to an actual security breach. During the delivery stage, social engineering is implemented by sending a targeted phishing email. Forensic security technology can see the "delivery" stage, revealing the infection point of a social engineering attack utilizing our visibility into email, web history and downloads. If the attack comes from a malicious USB drive, we can also identify USB usage history and content.

EXPLOITATION STAGE

In the Exploitation stage, after the user inadvertently clicks a malicious URL in the phishing email, a browser's vulnerability is exploited. Within minutes, malware has entered your endpoint. Guidance's forensic visibility into the exploitation phase enables users to see the email, website or USB drive that started the infection—but that's just the beginning. We can also view the email attachment cache to see if it was clicked, see the process history of what the vulnerability allowed to run, and what malicious files were created. Much of this visibility is found by reverse engineering forensic residue.

INSTALLATION PHASE

During the Installation phase, bad actors install Advanced Persistent Threats (APTs), which survive on endpoints for many months. They also install backdoors for return visits, after shallow cybersecurity triage tools remediate only some of their malicious files and processes. Remote Access Trojans (RATs), like PlugX or Gh0st RAT, are popular choices and were used to steal 18 million records from OPM. During the Installation phase, malware communicates to malicious servers on the internet, and files are created, deleted and run. Our kernel level visibility into the OS and file system, combined with our unmatched investigation experience, allow us to see all of these activities.

COMMAND & CONTROL PHASE

At this point the attacker has barely broken a sweat penetrating the perimeter and installing APTs and RATs. Next begins the lengthy Command and Control phase where hackers spend 90% of their time in your network. While the prior stages of the breach require only days to complete, Command and Control typically lasts many months, or even years. Attackers must move laterally between machines, gaining additional access as they begin searching for your customer records and intellectual property.

Guidance's forensic security technology provides unprecedented visibility during the Command and Control stage. In addition to the evidence of lateral movement that others see in network and system logs, we also identify forensic residue documentation, reverse engineered from the Windows registry. Often hackers hide beneath the radar with advanced rootkits, yet our visibility directly into physical memory allows us to see processes and data unknown even to the OS.

The next step for hackers in the Command and Control phase is to escalate their privileges, through stealing passwords or other vulnerabilities, to reach more endpoints and data stores. At this point attackers may also begin to hide their tracks through data deletions and anti-forensics. Once a bad actor has "Command and Control" of key user accounts, they can easily "hide" in plain sight, remotely logging into machines and appearing like any other user or admin. By compromising the right account, they can access your databases, email, document and cloud repositories, as well as search the hard drives of privileged users. Again, these Command and Control activities typically occur over a very long period.

Yet basically every interaction on an endpoint-- even that of anti-forensic activities-- leaves behind residue. Users or applications that touch files, for reading or deleting, leave residue in the Windows Registry, in Windows system files, and deep within the file system metadata. The longer they are on the network, and the more endpoints they touch, the more forensic residue they leave behind. With compromised accounts, while attackers gain the advantage of appearing like users, but they also leave behind the same forensic residue that any user would. Investigating these types of hacker activities is quite similar to what is done during insider threat or criminal cases. Many years have been spent reverse engineering obscure system files and the Registry, where Windows tracks most all user activities, files clicked, and directories browsed.

The end goal of Command and Control is to work towards locating your customer records, intellectual property and other sensitive data. Do you know where this data is? Our products enable you to easily access data stored on endpoint hard drives, on-premises and cloud email, document and data repositories-- allowing you to locate all your sensitive data at once. With this knowledge, your organization can ensure that data is protected, reduce its attack surface, and prioritize defense.

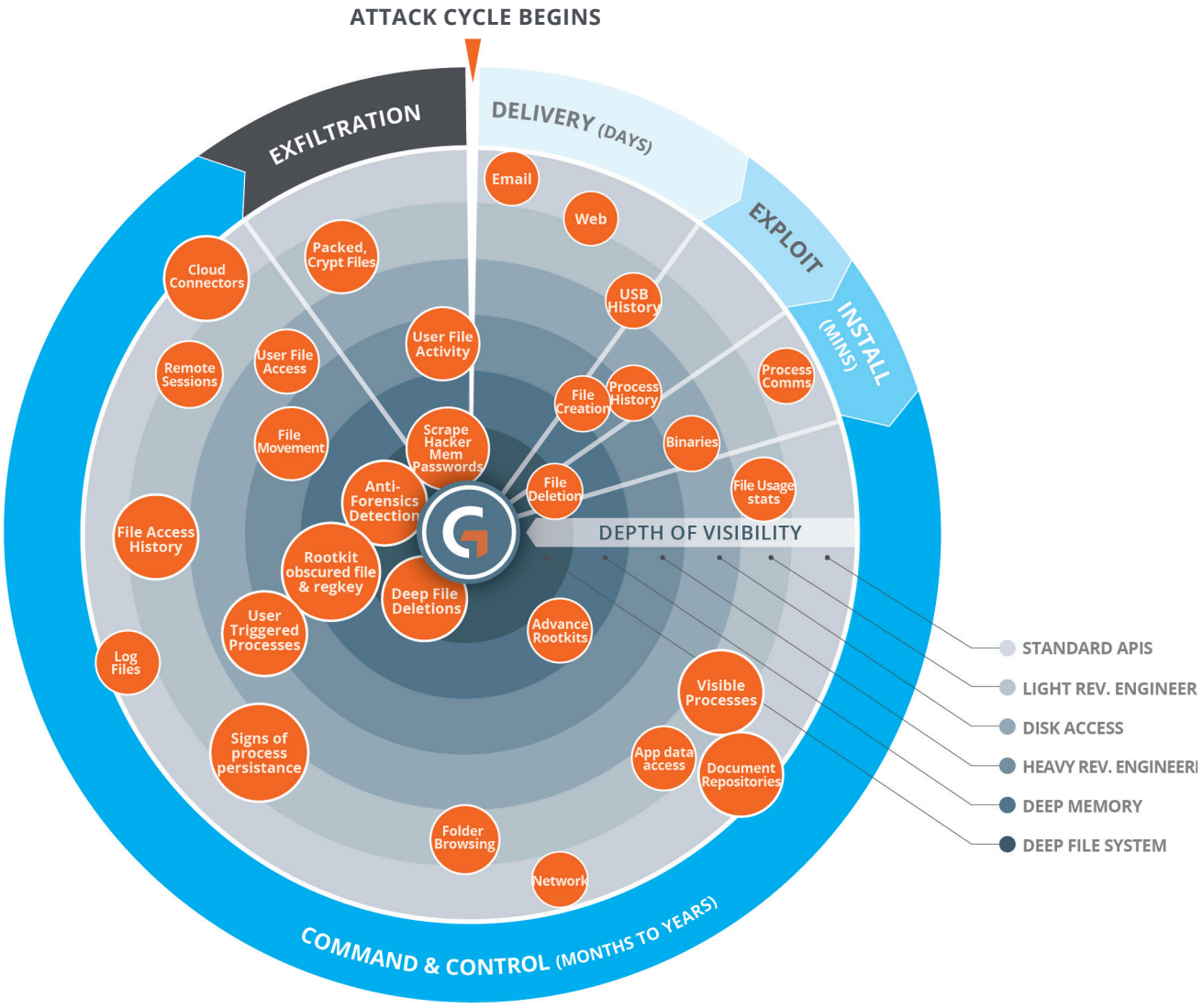
EXFILTRATION STAGE

Once the crown jewels of your organization have been located, culprits package customer records and intellectual property, then upload them to malicious servers across the internet. To avoid setting off suspicions, they may compress, obfuscate or encrypt this data. By being able to proactively scan for sensitive data-- including inside archive files and encrypted data-- you can locate stolen data being gathered from "jump boxes," or the endpoints hackers use to extend their malicious activities.

CONCLUSION: GET THE 360° VIEW

360° visibility is the only 100% reliable and effective approach to endpoint detection and response. It is critical for your IR team because the endpoint is involved in almost every breach, and every user and software interaction leaves a footprint on that endpoint. Guidance created the category of digital investigations and fueled the rise of endpoint security. Through deep forensic and eDiscovery experience helping our clients through crises, we have become the only cybersecurity company with a security-forensic technology stack that provides 360° visibility into all the stages of a security breach.

GUIDANCE SOFTWARE 360° VISIBILITY



GUIDANCE SOFTWARE

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.