opentext™

WHITE PAPER

Securing the enterprise with 360° visibility: Don’t leave a gap in defenses

Every day, organizations are relentlessly fighting cyber threats. With more at stake than ever before, including customer data, intellectual property and company reputations, one successful attack can mean game over. This white paper demonstrates the need for organizations to have 360-degree visibility into people, systems and things to see every route a threat can take and make informed decisions to remediate them.

opentext™

Contents

opentext™

Executive summary

The endpoint is involved in almost every breach, and each user and software interaction leaves a footprint on that endpoint. That is why the most effective approach to endpoint detection and response (EDR) is to have 360-degree visibility into all endpoints—from desktops and laptops to servers, the IoT and everything in between. This paper details the capabilities of an EDR solution with 360-degree visibility and demonstrates how such a solution can defend an enterprise against cyberattacks.

360-degree endpoint visibility—the best cybersecurity defense

Organizations are under constant attack from external, and even internal, threats. Despite significant investments in security solutions, many still fall prey to attacks and data theft. Recently, 89 percent of surveyed enterprises reported experiencing at least one type of security breach.[1] To make risk management even more challenging, regulatory efforts, such as the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCIDSS) and local laws mandating breach disclosure and response, require organizations to demonstrate that they can respond effectively to security incidents.

As attackers are becoming increasingly sophisticated at avoiding detection, 360-degree visibility is critical to incident response. Organizations need the ability to detect threats designed to evade perimeter defenses. To ensure business continuity, they also need rapid and comprehensive incident response capabilities, including the following:

Comprehensive detection at a forensic level leverages the relationship among deep system artifacts to uncover hidden threats. This approach helps incident response (IR) teams uncover activity indicative of a threat, perform root cause analysis, establish incident timelines and detect an attacker's attempt at obfuscating their activities at the operating system (OS) or application levels.

Total coverage across all systems within your environment. Most EDR technologies support only Windows©, macOS and perhaps even Linux. But since most IT environments are complex and varied, EDR solutions should also support legacy and purpose-built operating systems, as well as IoT devices that run critical applications or hold sensitive data.

Complete and effective response EDR technology enables IR teams to surgically remediate the complete threat by killing all processes from the malicious code, deleting any files that spawned it and resetting affected registry keys. This holistic EDR approach ends any persistence mechanism related to that attack and eliminates the threat without taking machines offline. Complete and effective response goes far beyond merely containing a threat or reimaging a machine to return the network to a fully operational state.

Forensic depth trumps speed

Much is made of speed and how quickly security tools can run queries on certain endpoints. While speed is important, the depth of endpoint visibility enabled by your EDR solution is far more critical. An EDR solution should be able to see beyond the standard APIs and system logs of the OS and, ideally, reach inside email, the cloud and on-premises repositories.

Most importantly, EDR should be able to identify the forensic residue left on the endpoint by every user and application interaction, including those hidden in file systems and memory that OS vendors never intended you to view.

1. DarkReading, The Impact of a Security Breach 2017, 2017.

opentext™

Augmenting EDR across the cyber kill chain

Incident response and forensic analysis once required highly skilled individuals trained in the art and science of disk and file carving. However, in recent years, investigative needs have increased due to regulations, such as the GDPR, and the alarming rate of cyberattacks by both insiders and outsiders. Manual, skill-intensive methods are no longer sufficient. Automated EDR augmented with artificial intelligence (AI) and deep learning is needed to fight cyberattacks across all stages of the cyber kill chain.

Authored by Lockheed Martin, the seven-stage kill chain model describes the various threat activities undertaken by attackers during security breaches. Embedding EDR into the final five stages of activity occurring within your network can prevent or remediate cyber threats.

Early stages: Initially, hackers build custom tools to weaponize companies.

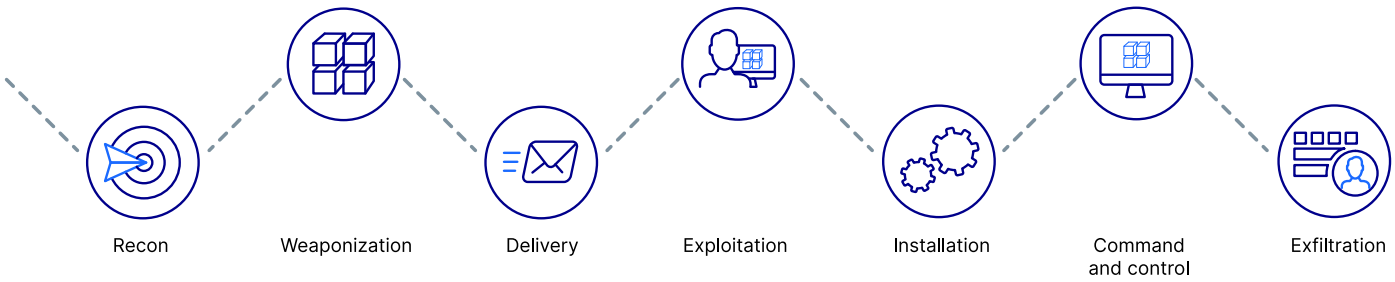
Delivery stage: Cyber attackers implement social engineering by sending targeted phishing emails. However, a robust EDR solution can view the delivery stage, revealing the infection point of a social engineering attack using email, web history and download visibility. If the attack comes from a malicious USB drive, the EDR solution can also identify USB usage history and content.

Exploitation stage: After the user inadvertently clicks a malicious URL in the phishing email, a browser's vulnerability is exploited. Within minutes, malware enters the endpoint. Robust visibility into the exploitation stage enables users to see the email, website or USB drive that started the infection as well as the email attachment cache, process history and malicious files that were created.

Installation phase: During the installation phase, bad actors install Advanced Persistent Threats that 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, such as PlugX or Gh0st RAT, are popular choices for cyberattacks. During this stage, malware communicates with malicious servers on the internet and files are created, deleted and run. An EDR solution that provides kernel level visibility into the OS and file systems can identify all these activities.

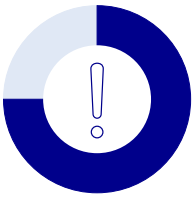
Command and control phase: While the prior stages of the breach require only days to complete, the command and control stage typically lasts many months or even years. Attackers move laterally between machines, gaining additional access as they begin searching for customer records and intellectual property.

Attackers then escalate their privileges by stealing passwords or leveraging other vulnerabilities to reach more endpoints and data stores. At this point, attackers may also begin to cover their tracks through data deletions and anti-forensics. Once a bad actor has command and control of key user accounts, he or she can easily hide in plain sight by remotely logging into machines and appearing as another user or admin. By compromising the right account, the attacker can access databases, email, document and cloud repositories as well as search the hard drives of privileged users.

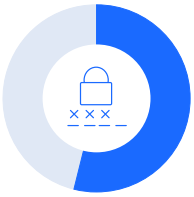


opentext™

Multinational telecommunications giant reduces incident validation from days to minutes with OpenText EnCase Endpoint Security



Situation: High rate of false positive alerts due to unpatched anti-virus software.



Challenge: The existing validation process dictated that InfoSec contact local IT to look at the anti-virus version and report back. Service level agreements dictated a two-day response time, and with numerous such incidents every week, the backlog of alerts was increasing, introducing unnecessary risk to the enterprise.

Solution: OpenText™ EnCase™ Endpoint Security was implemented and integrated with the existing alerting system. EnCase Endpoint Security was configured to automatically detect these alerts, reach out to the potentially affected endpoints and report on whether the anti-virus solution was current. Within minutes the security team knew whether the alert was a false positive or a real threat.

Yet every interaction within the operating system—even that of anti-forensic activities— leaves 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.

The end goal of command and control is to locate customer records, intellectual property and other sensitive data. That is why the right EDR solution makes a critical difference. In addition to locating lateral movement that others see in network and system logs, EDR technology can also identify forensic residue within the Windows Registry. As hackers often operate under the radar using advanced rootkits, gaining direct visibility into physical memory can expose processes and data unknown even to the OS.

A solution that provides complete coverage of endpoint hard drives, on-premises and cloud email and document and data repositories allows companies to locate sensitive data and ensure that data is protected, reduce its attack surface and prioritize defense strategies.

Exfiltration stage: Once cybercriminals discover the crown jewels of an organization, they can then package customer records and intellectual property and upload them to malicious servers across the internet. To avoid setting off suspicion, cybercriminals compress, obfuscate or encrypt this data. By scanning for sensitive data—including inside archive files and encrypted data—the right EDR solution can locate stolen data gathered from the endpoints hackers use to extend their malicious activities.

The AI/machine learning advantage: Across every stage, vast amounts of data must be gathered to expose or detect what is essentially a needle in a haystack. Automation and machine learning can augment forensic visibility to quickly spot suspicious anomalies across the entire cyber kill chain. The net result is the correlation of terabytes or petabytes of data in near-realtime, which ensures that security threats are detected before they become data breaches.

Realizing 360˚ endpoint protection

Certainly, 360-degree visibility is the only completely reliable approach to endpoint detection and response and is critical for IR teams. OpenText™ Guidance has pioneered working with the endpoint in digital investigations. Through deep forensic and electronic discovery experience, OpenText has become the only Enterprise Information Management company with a forensic security technology stack that provides 360-degree visibility into all the stages of a security breach on any endpoint device. For more information about our endpoint detection and response solutions, please visit: opentext.com/security.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

opentext.com/contact