IDC WORKBOOK
Sponsored by: Palo Alto Networks

Endpoint detection and response (EDR) is evolving to create value by extending the view beyond initial boundaries of the endpoint. The "manifest destiny" of EDR is to be a tool that provides cross-platform visibility and response, stopping maliciousness that cannot be detected with endpoint activity and telemetry alone.

Key Requirements of EDR: Business Needs Mandate Visibility Beyond the Endpoint

October 2019

Written by: Frank Dickson, Program Vice President, Cybersecurity Products

AT A GLANCE

KEY STATS

- By 2021, businesses worldwide will be spending about $2.1 trillion per year on digital transformation (DX).
- By 2020, about 60% of organizations will have embarked on a DX journey.
- By 2020, 70% of CIOs will have developed a cloud-first strategy to support the infrastructure agility required by transformation.
- As DX changes IT architectures and makes them more permeable, the future of cybersecurity is coalescing around endpoints, identities, applications, and data.

Introduction

Digital transformation (DX) initiatives have helped businesses rapidly create new products and services. However, DX is built on a foundation of security and trust, and advanced cyberattacks threaten to disrupt the pace of DX innovation. DX platform initiatives increasingly rely on the integrity and resiliency of interconnected systems and a secure pipeline to enable sensitive data streams that enrich business intelligence systems and analytics repositories.

There is a lot at stake. In 2017, businesses spent $1.1 trillion transforming themselves into connected, intelligent, and technology-driven organizations. In 2018, businesses spent an additional $1.3 trillion. IDC projects that by 2021, businesses worldwide will be spending as much as $2.1 trillion per year just trying to transform, and that number will continue to increase. IDC believes that by 2020, about 60% of organizations will have embarked on a digital transformation journey and 70% of CIOs will have developed a cloud-first strategy to support the infrastructure agility required by transformation. That leaves a tremendous amount of digital transformation growth opportunity as much as three years from today.

Security operations (SecOps) teams are hard at work to protect their increasingly digital organizations. Evolving categories of security tools are designed to help businesses prevent as many adversaries as possible from entering systems and, subsequently, to detect and respond to those who manage to skirt their frontline defenses. For SecOps teams, the job of keeping up with advanced threats is not only more business critical than ever but also more complex as new technologies introduce new threat vectors.

As DX changes IT architectures and makes them more permeable, the future of cybersecurity is coalescing around the following four central control points:

- **Endpoints.** A dark internet will require presence at key termination points. Detecting the malicious must happen at the termination points, where the data is unencrypted. Additionally, endpoints are the source of most productive activity and the most common first stop in an attack. Endpoints provide key telemetry data for analysis and detection.
- **Identities.** Digital transformation requires a higher level of connectivity between applications and business processes. The aim of this connectivity is to increase business agility and meet the expectations of customers and business partners for a 24 x 7 uninterrupted experience. Digital transformation can come in many forms. Things that were once not connected are now, and services operate as one big machine. The goal is to integrate trust into the "machine."
- **Applications.** As applications are increasingly disassociated from specifically defined servers, networks, and infrastructure, network-centric security measures are increasingly ineffective. The only way to compensate is to apply security at the application level. For security applications, Layer 7 is the new Layer 3.
- **Data.** Data is the fuel of the DX machine. Data is also the cyberattacker's bounty of choice. Protecting access is a perpetual game of cat and mouse. Security measures that travel with the data can dramatically improve the integrity of the DX activity.

Endpoint Solution Vendors Are Working to Keep Up

Because endpoints are the "termination point" for DX initiatives, the need for trusted and secure endpoints has been met with a robust response from cybersecurity vendors. The response has come in two large categories: endpoint protection (EPP) enhancement and forensics tools (i.e., endpoint detection and response, or EDR).

EPP has gone from being signature centric to being behavior centric. New analysis types are being implemented, including static analysis that evaluates the potential maliciousness of a file based on file inspection, heuristic rules that prevent potential malicious actions by blocking exploits such as PowerShell manipulation, and behavioral analysis that evaluates the maliciousness of a file based on functions performed. Note that maliciousness may not necessarily be based on a single file — thus, malicious behavior can be implemented by the sequential stringing together of seemingly benign activities, so detection depends on the stringing together of operations.

EDR arms security professionals with a newer arsenal of forensics tools that are not of the historical log-based variety. EDR provides a host of endpoint telemetry to allow security professionals to discover malware that was previously hard to find. Subsequently, the "R" for "response" allows security professionals to actually do something, such as quarantine a file or move an endpoint off the network.

Security Teams Require Better Automation and Visibility

EDR has been a fantastic development. However, EDR has two major shortcomings. First, it requires a person to operate the tool. Security professionals are in short supply and their time is very valuable. As a result, the expectations for EDR and its usability have grown exponentially. EDR tools need to be easy to use, able to quickly correlate alerts to render a conviction or benign verdict, and provide guided search to enable security professionals to perform at a higher level than they traditionally could. Essentially, EDR tools must evolve to make security professionals more efficient and effective.

EDR's second weakness is speed, measured in mean time to detect (MTTD) and mean time to respond (MTTR). Many malware attacks, such as most ransomware, can be measured in seconds. Depending on EDR to detect ransomware is a fool's errand because a manual tool cannot respond quickly enough to stop an attack that happens in minutes or sometimes even seconds. Thus, the expectations we have for EPP must address some use cases that were not being addressed by EDR.

For EDR to add value in the modern era, EDR tools must do the following:

- Find threats that cannot be detected by using telemetry on the endpoint alone
- Provide forensics information that will illuminate how adversaries got past the other layers of security before they were stopped by EPP

Both use cases have a similar implication: The data that fuels EDR needs to come from more than just the endpoint. Telemetry needs to come from the network, cloud, and other security measures.

For example, PowerShell scripts are not necessarily malicious. However, if the PowerShell script was launched from a macro that was embedded in a Word file, and that Word file was found in recently delivered email, the chances of the script being malicious are high. The example is simplistic but very real. The response, however, goes beyond sequestering the individual endpoint. The security analyst needs to be able to sweep all email accounts for similar files, block a potential C&C IP address call-out, update firewall rules, and force an Active Directory password reset.

The data that fuels EDR needs to come from more than just the endpoint. Telemetry needs to come from the network, cloud, and other security measures.

EDR Feature Evaluation

With the previous discussion in mind, we must evaluate EDR capabilities to fulfill the forensics need and EPP capabilities to deliver effective prevention. As we think of the expectations for EDR, we focus on two primary attributes:

- **Visibility and efficacy.** Visibility and efficacy are, of course, self-explanatory. However, efficacy must be viewed through the lens of our previous discussion. EDR needs to be able to detect malicious activity that EPP is not expected to detect and block. Almost by definition, EDR must leverage data that is outside of the endpoint. Context matters. For example, PowerShell scripts are wonderful tools for managing endpoints, and running such a script is not necessarily malicious; seeing a lone script run on an endpoint does not necessarily provide insight into maliciousness. But what if a PowerShell script was launched from a Word document previously attached to an email? And what if that document came from an external sender?

  Clearly, context matters. What if an executable sends a beacon to a location from a known questionable IP range before it begins to encrypt a file? What happened before a file landed on the endpoint and tried to execute? What happened after? Does knowing the executable was unpacked on a networked printer or internet-connected fax machine before finding its way onto a laptop via an unknown or unfamiliar lateral movement provide context that may indicate a file's potential maliciousness?

  IDC once made the statement that visibility is binary — you can either "see" or "not see." That was true when complexity was lower. Today, the world that must be seen is immense. "Seeing" can be measured in degrees; more visibility is better, and understanding context has never been more important.

- **People efficiency.** People are our most precious assets. Experts are scarce. IDC has never heard anyone say, "I have an excess of qualified security analysts." The scarcity of security analysts has a very real implication. Except for extremely rare instances, security teams do not respond to all alerts. They address the maximum number of alerts for which they have allotted time. Informal or formal rules guide the investigation and remediation processes. For example, a company's security policy may state that the security team is required to address the highest-severity alerts first and that Level 4 alerts receive best effort. The attack plan is almost always prioritized; but by definition, prioritization means that some alerts receive an immediate response while others may not be addressed at all.

  Thus, the efficiency and ease of use of EDR have direct implications on its value. Analytics that correlate multiple alerts filter noise and allow Level 1 analyst work to be automated. Guided search and automated intelligence tools then allow Level 1 analysts, who now have newfound time gains by not triaging alerts, to alleviate work from Level 2 analysts. People and time thus become the new return on investment (ROI) metrics for EDR tools.

Given our discussion of the two vectors for analyzing EDR tools, Table 1 presents the attributes that should be considered in evaluating the visibility and efficacy attributes of an EDR tool. The people efficiency features are in Table 2. Some vendors in the space have a breadth of excellence on each feature; others, not so much. Each feature should be scored with a numerical weight attached — for example, troubling (1) to excellent (4).

TABLE 1: ***Visibility and Efficacy EDR Feature Evaluation***

Feature	Rating
Ability to continuously record events such as file create/update/delete, running processes, registry changes, command-line interface (CLI) arguments, etc.	
Data storage capabilities, either on endpoints, in an on-premises server, or in the cloud	
Wide range of remediation capabilities, including network isolation, file quarantine, file removal, process kill, behavior block	
Direct endpoint access to view and download files, monitor running processes, and execute commands and scripts	
Risk-prioritized views based on the confidence and severity of an incident	
Click-down attack chain visualization tools to allow investigators to pivot	
Fetching of suspect files or memory and disk dumps	
Automated integrated analysis of suspect processes or files in a sandbox	
Real-time scripting endpoint capabilities for incident response	
Ability to ingest third-party threat intelligence	
Ability to execute any standard system command on any endpoint	

Source: IDC, 2019

For people efficiency features, the same rating system applies — troubling (1) to excellent (4). Once again, the emphasis is maximizing the ROI of people.

TABLE 2: ***People Efficiency EDR Feature Evaluation***

Efficiency Feature	Rating
Graphing relationship interface to visualize the connectivity of seemingly disparate indicators of compromise (IOCs) in a historical timeline of a chain of events	
Ability to run simple and complex queries on activity across infrastructure	
Threat detection based on machine learning and behavioral analytics that can detect lateral movement, exfiltration, C&C, and malware	
Threat detection based on IOCs, such as file hash or IP address	
Custom and predefined rules to detect attacker tactics, techniques, and procedures	
Potentially malicious user behavior analysis/reporting capabilities	
Automated remediation workflows	
Scalable remote management capabilities	
Incident management to group related alerts together and assign owners	

Source: IDC, 2019

Don't Forget EPP

IDC recommends that as you make considerations for EDR, you also look at your existing EPP capabilities. In an evaluation of EDR, the conversation is as much about EPP. Expectations for EPP have grown dramatically.

Prevention is always the ultimate outcome; therefore, security teams should not rely on EDR to compensate for inadequacies in their endpoint protection. Some integrated solutions offer EDR and EPP functionality that aims to first protect and then detect. Whether EPP is integrated with EDR or not, IDC would challenge all users to expect more functionality from their EPP solution; basically, to fulfill its raison d'etre. Table 3 provides a list of features that should be considered standard in an EPP offering.

Prevention is always the ultimate outcome; therefore, security teams should not rely on EDR to compensate for inadequacies in their endpoint protection.

TABLE 3: ***Standard Features for an Endpoint Protection Offering***

Q *Does your EPP support the following standard features?*

EPP Feature	Yes/No
Blocking for known malware (Blocking can be based on signatures, hashes, or other such methodologies.)	
Blocking for unknown malware based on static file analysis or emulation	
Ability to block fileless and script-based attacks	
Ability to block suspicious behaviors and techniques	
Threat intelligence powering the solution	
Protection against known and unknown exploits	
Anti-ransomware protection	
Easy-to-use management console	

Source: IDC, 2019

The expectation for EPP should be that it protects endpoints independently from any integrated EDR functionality. As stated previously, EPP protects and EDR provides forensic augmentation of the solution. However, optional enhancements/features of EPP solutions can influence or augment the success of EDR. For example, a sandbox option is not and should not be a fundamental requirement for EPP. Your prevention system needs to stop the bad stuff, period! A sandbox option, though, can be leveraged to reduce the false positives being fed to an EDR solution. The example we frequently cite is an installer or packer file. In a static analysis, it will look, feel, and smell malicious. A sandbox will see that in fact, it did look and feel malicious but upon further review can determine it is greyware and will overturn the verdict.

Additionally, agent fatigue is real. The lighter the impact of agents and the fewer the agents, the lower the risk of potential problems in the future. Is an agent that has a low system impact a requirement? No, not formally. Is a single agent a "must have?" No, not officially. Good idea? You bet.

One final point: IDC is seeing EPP vendors include features that improve user protection through better authentication. For example, behavioral biometric features are being integrated into the solutions (see Table 4). The features will look at interaction patterns with applications, keyboard, and mouse to detect incongruent behavior. The features are not a requirement, but the enhancement aids the success of EDR.

TABLE 4: ***Optional Features for an Endpoint Protection Offering That Enhance EDR Success***

Q ***Does your EPP support the following optional features?***

Optional Feature	Yes/No
Cloud-based sandbox for deep inspection and second opinion analysis	
Lightweight agent to minimize impact	
Single agent for both EPP and EDR	
Hardening such as application control or other feature that reduces the attack surface	
Ability to collect data from and quickly share intelligence with network and cloud protection technologies	
Support for Windows, MacOS, and Linux operating systems	

Source: IDC, 2019

About the Analyst

Frank Dickson, *Program Vice President, Cybersecurity Products*

Frank Dickson is a Program Vice President within IDC's Cybersecurity Products research practice. In this role, he leads the team that delivers compelling research in the areas of Network Security; Endpoint Security; Cybersecurity Analytics, Intelligence, Response, and Orchestration (AIRO); Identity and Digital Trust; Legal, Risk and Compliance; Data Security; IoT Security; and Cloud Security.

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

This publication was produced by IDC Custom Solutions. The **o**pinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.