GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Nadel, Brian

Title: "The Best Endpoint Detection and Response Solutions of 2020"

Website: Business.com blog

Organization: Business.com

Date: 14 October 2019

URL: https://www.business.com/categories/best-endpoint-detection-response/

Accessed: 19 October 2019

Synopsis: Nestled in the southwestern corner of Tennessee, the town of Collierville seems like the epitome of small-town America. With a population of 44,000, a $70 million annual budget and 511 employees, it can also be thought of as a typical small business today. When it was recently hit by a ransomware attack, the town's key files were encrypted, nearly grinding its operations to a halt.

Likely the result of an employee clicking on a phishing email, the town's anti-malware software found the Ryuk virus but couldn't contain it to the initial infection, setting off a cascade of lost data. While it may not seem so, Collierville was lucky. Thanks to diligent work rebuilding its data infrastructure, the town was back in business in a couple of days. In fact, a month later, the only indication that anything is amiss there is that utility bills to homeowners might be a little late.

Best Endpoint Detection and Response

Intro

Nestled in the southwestern corner of Tennessee, the town of Collierville seems like the epitome of small-town America. With a population of 44,000, a $70 million annual budget and 511 employees, it can also be thought of as a typical small business today. When it was recently hit by a ransomware attack, the town's key files were encrypted, nearly grinding its operations to a halt.

Likely the result of an employee clicking on a phishing email, the town's anti-malware software found the Ryuk virus but couldn't contain it to the initial infection, setting off a cascade of lost data. While it may not seem so, Collierville was lucky. Thanks to diligent work rebuilding its data infrastructure, the town was back in business in a couple of days. In fact, a month later, the only indication that anything is amiss there is that utility bills to homeowners might be a little late.

Editor's note: Looking for an endpoint detection and response solution for your business? Fill out the below questionnaire to have our vendor partners contact you about your needs.

The Ransomware Target

Businesses have a big bull's eye on their backs. As consumer malware attacks have declined, they have risen more than threefold for businesses, according to cybersecurity company Malwarebytes. Last year, 7 out of 10 ransomware attacks were directed at small businesses, according to Beazley, a London-based insurance company specializing in cybersecurity. If that isn't ominous enough, the average ransom to get back company data can run into millions of dollars.

However, there's a lot you can do to protect your company and its valuable data from attack. It's better to be safe with the right protection than scrambling to recover your company's data and dignity. Defending your company's computers, customer data, intellectual property, and employee records against a wide variety of threats is minor compared to the cost, hassles, and embarrassment of dealing with an attack's aftermath.

Enter endpoint detection and response (EDR) software. These programs are for companies that have outgrown internet security software and need industrial-strength protection for every system they own.

Reviews

What Is Endpoint Detection and Response?

As its name implies, endpoint detection and response, aka EDR, covers the gamut of commercial cybersecurity these days. In addition to keeping an eye out for the worst

the web has on tap with advanced malware detection, EDR systems continuously monitor, collect, record and store all digital activities that each system performs.

Think of it as akin to a plane's flight recorder or black box that archives every major aspect of the computer's operation. It can provide IT professionals with an early warning of trouble ahead and an avenue to investigate cyberthreats.

The program keeps its archived telemetry from monitored systems and threat attributes in a central repository for easy access. Plus, the EDR software can update and deploy new apps to the company's computers as needed, regardless of whether it's a desktop PC in Kansas City or a tablet in Kuala Lumpur.

EDR goes beyond the abilities of traditional internet security software by being proactive. It uses a software agent that monitors the system's behavior with advanced heuristics. It often accomplishes this with machine learning and artificial intelligence that's been trained to spot anomalies or the patterns of an infection.

At the first sign that a system is under attack (such as the moving, copying or encrypting of system files), the EDR software springs into action. It simultaneously alerts an administrator to the potential breach, blocks the rogue software from running if it can and returns the system to its pre-infection state.

Because monitoring is at the heart of EDR, each security element must mesh with the EDR software. It needs to work with other security tools, including email inbox monitoring for phishing attempts, a firewall to block unauthorized code from entering or leaving a computer or network, and updates to the system's software.

EDR Pricing

The cost of deploying and maintaining an EDR solution varies. If you don't have IT staff, you'll likely want to hire some. The EDR company will want to work with you on an individual quote based on your needs, but it's a fair bet that the price will be on a per-endpoint basis, which can vary from $30 to $50 per seat. Other pricing models include subscriptions and volume-based discounts, though you'll still want to get an individualized quote in these cases. Many solutions offer a free trial.

Endpoint Detection and Response Dashboard

A well-designed dashboard or management console is key to effectively using EDR's wide scope of services. It allows an IT administrator to not only monitor what's going on inside each system your company owns but to make changes to the basic security stance of systems individually or in groups.

When a new threat appears on a company computer, the dashboard alerts your IT administrator to what's happening and how severe the threat is. In addition to showing whether it's a new or old threat, the dashboard starts the remediation process. In a matter of seconds, the administrator can poll all connected systems to see if they have also picked up the virus.

While the dashboard is usually web-based, some EDR systems have app-based consoles that require special software. Forward-thinking EDR companies have added a new component: an app that displays a mini-dashboard on a phone, tablet or

digital watch. The app summarizes the vital elements and alerts, but you'll need to consult the full dashboard for a meaningful response.

EDR goes a step further in cybersecurity with the ability to follow up on an attack with an in-depth investigation of what went wrong. Each EDR agent has the ability to record and centrally store exactly what happens inside every computer. This allows the program to play back how an attack occurred to show aspects that became vulnerable and – hopefully – insights to prevent a recurrence.

Endpoint Detection vs. Internet Security Software

The difference between EDR and internet security software is like the difference between an army tank and an armored car: Both can protect their contents under dire circumstances, but only the tank can go on the offensive.

To go after threats, the EDR program plants traps throughout the system and network that look like unprotected areas. These decoys are like honeypots that look too good to be true to malware writers – and often are. The decoys provoke an attack in a less critical, less protected area of the system, giving the EDR software information about its intent and techniques without endangering the system's operation or your company's data.

To fully protect a small business, where computers of all sorts are used, the EDR apps need to cover all popular platforms. Today, this starts with PCs, Macs and Linux computers, and extends to mobile devices like iPhones, iPads, and Android phones and tablets.

On the downside, EDR requires more overhead than traditional Internet security software. It's often a deal-killer for small businesses struggling to get the day's work done with their current staffing, because EDR often needs a dedicated employee to design and maintain it while reacting to threats.

As a result, the threshold for EDR is somewhere between 50 and 100 employees, although smaller security-conscious firms also use this powerful software. Some EDR vendors actually concentrate on large enterprises with a minimum number of seats they license or a base licensing fee that can reach five figures.

In this age of lean business, there is another way: EDR can take the form of software as a service (SaaS) over the web. With this solution, the protection and follow-up is deployed and monitored remotely. This can provide the right balance between security and costs while letting you and your employees concentrate on your business operations.

The Rise of Endpoint Detection and Response

With hackers and malware writers seemingly hiding behind every URL, the need for endpoint detection and response has never been greater. In fact, market analysis firm Gartner has forecast that EDR sales will continue to grow by more than 40% a year.

The top vendors of EDR software range from established leaders in enterprise security such as McAfee, Trend Micro, Symantec, and Sophos to relative newcomers

such as Cynet and SentinelOne. Each has a different way of dealing with threats, but one thing is common: The EDR has one or more software agents that watch over the computer and archive all its actions. These agents keep track of the computer's data, monitor it for malware, and record everything the computer does. EDR software that has consolidated to a single agent often gives the benefit of simplicity, ease of installation and maintenance, and extra performance.

The key to success with EDR is to maintain a low profile on protected systems. In fact, EDR works best when it doesn't interrupt the daily use of the computer and data but is always ready to pounce on a threat when needed.

It can be a tough balance to find. If you're too compulsive, the heavy hand will make employees feel like they're working in a prison, but with too little attention, malware can slip onto a computer, potentially infecting your network and entire company. Each company needs to find its own equilibrium between safety and the ability to get the job done.

That's where next-generation antivirus protection comes in. It not only goes after the traditional malware threats but can detect common attacks as well as those below the surface. With threats hidden in scripts or the system's startup commands and fileless attacks that exist only in the computer's memory, an exploit might even be packaged in two or three separate pieces of harmless software that together form an attack.

In a world where we don't know what threats tomorrow might bring, next-gen protection is mandatory. It's all based on advances in artificial intelligence and machine learning that can spot rogue behavior early enough in the infection process to stop it, quarantine the sample and restore the system's files.

A key point about machine learning in this context is that the EDR improves its detection abilities as it gains more data about threats, how employees work and the threat landscape in general. The quicker and more accurately this trigger is pulled, the better it will fit into a company's way of doing business.

Endpoint Response

Detecting incoming malware is just the start. The response portion of EDR is just as important to cyber defenses.

Once the system has been cleared of the threat, the EDR software goes into investigation mode. Based on its sequence of recorded events, it presents how the attack played out on your company's computers, noting every change to the system. This playback of the event often looks like a branching flowchart that starts with the initial incursion and proceeds to describe which parts of the system and network were infected, when, and what the result was.

More than a roadmap of an attack's progress, the software's response can be thought of as a window into a newfound weakness. In other words, it's like a microscope in the hands of a bacteriologist to examine the contagion and prevent a fresh infection.

Because employees do weird and sometimes dangerous things with their company computers, EDR software sets limits. The most important limit is keeping employees away from websites with a history of delivering malware. This extends to pornography, gambling and gaming sites but doesn't stop there. Because many

ransomware attacks start with a phishing attempt, this URL filtering is a good way to stop malware before it ever starts.

In fact, the current thinking is that employees should play no part in EDR-based cybersecurity. While the best consumer security programs revel in allowing a huge amount of customization, personalized options and often the ability to turn protection off, EDR's activities are off limits. In fact, all actions are triggered and configured remotely. In the interests of never letting your guard down, most programs don't allow the actual user of the computer to make any changes to the security stance or its individual security components.

Endpoint Detection and Response: What to Look For

The goal is to protect every computer your company owns – such as the CEO's iPhone and desktop PC, the R&D department's Linux workstations, the designer's MacBook, and the salespeople's tablets. This requires a stunning array of software working together to protect your company's digital infrastructure and data. Here's what you should look for in EDR software.

- The idea is to keep all malicious code – malware, phishing attempts, ransomware, etc. – off your company's computers. Look for a system with advanced behavioral monitoring and the ability to eradicate threats old and new.
- The software should capture and archive all aspects of a computer's operations to provide samples of new viruses for analysis and the raw data for post-infection follow-up.
- Keeping employees from using their company-issued computers for nefarious purposes, like viewing porn or gambling, might seem like a lost cause, but your EDR software needs to block company computers from sites that have a reputation for dispensing malware.
- Choose an EDR program that can prevent the user from adjusting or turning off the protection. You should be able to lock the systems down so that your company's fleet is always protected.
- EDR software entails a lot of remote operation and configuration with a dashboard. Make sure it's easy to use and won't overwhelm users.
- The software needs to update itself to keep its protection current. The best EDR programs can also stream entire apps to any or all employees.
- While EDR can help defend against and respond to attacks, the software still needs an effective backup policy to restore key data to infected systems.
- Look for EDR software that is independently appraised for stopping malware by an organization like Mitre, AV-Comparatives and AV-TEST. Unfortunately, none of these organizations cover every EDR product.
- Forensics and investigation are two aspects of EDR that companies often ignore until there's an attack. With the software's extensive database of activities and the changes made to each computer, the attack can be dissected, hopefully preventing a future occurrence.

You don't want your company to stay the same size forever, so the top-ranked EDR systems can grow as your business grows. The best can scale without changing the basic software structure. Shutting down systems for former employees and adding new ones should be quick and easy.

Endpoint Detection and Response to the Rescue

EDR software should be protecting your employees, computers and networks. Not only is it a good defense against the latest threats, but it can dissect the attack's method of sneaking into your digital infrastructure so that the vulnerability that led to the infection can be eliminated.

In fact, Collierville's endpoint software did detect the ransomware, but it could do nothing to stop its spread. The town's backed-up data saved its digital infrastructure, and the town administrator is looking into getting new EDR software that can form a more thorough response.

The only defense against malware is a good offense. The right EDR software can provide just that.