# Conversational
# Endpoint Detection and Response

A ConversationalGeek® Book

Sponsored by GoSecure


## Learn about:

- New software security threats that put data at risk
- The shortcomings of traditional anti-virus against sophisticated attackers
- Behavior-based detection and proactive response tools to safeguard systems

2nd Edition

**By George Finney** (Chief Security Officer)

## Sponsored by GoSecure

GoSecure is recognized as a leader and innovator in cybersecurity solutions. The company is the first and only to integrate an Endpoint and Network threat detection platform, Managed Detection and Response services, and Cloud/SaaS delivery. The CounterTack Platform delivers predictive multi-vector detection, prevention, and response by applying a unique combination of behavioral analysis, memory forensics, machine learning, and reputational techniques to counter the most advanced threats. Our MDR Services are driven by aggressive SLAs for rapid response and active mitigation services that directly touch the customers' network and endpoints. Together, these capabilities provide the most effective response to the increased sophistication of continuously evolving malware and malicious insiders that target people, processes and systems. With focus on innovation quality, integrity and respect, GoSecure has become the trusted provider of cybersecurity products and services to organizations of all sizes, across all industries globally.


To learn more, please visit:

www.gosecure.net

# Conversational Endpoint Detection and Response

by George Finney




ConversationalGeek®

# Conversational Endpoint Detection and Response

Published by Conversational Geek Inc.
www.conversationalgeek.com



## Trademarks



## Warning and Disclaimer



## Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

## Publisher Acknowledgments

All of the folks responsible for the creation of this book:

| | |
|---|---|
| Author: | George Finney |
| Project/Copy Editor: | Nick Cavalancia |
| Content Reviewer: | J. Peter Bruzzese |

# Note from the Author

I love anti-virus, but in today's world of advanced threats, anti-virus alone leaves me vulnerable. This is going to sound weird, but writing this book has been a little like writing an unlikely love story. I have three pet peeves in my life: printers, people who get on an elevator without waiting for other people to get off first, and anti-virus. My feelings about printers can be summed up by that scene in the movie Office Space…you know the one. Elevators are like giant boxes of awkwardness and, as long as humans ride in them, that will never change. But I was wrong about anti-virus.

When I brought in a next-generation endpoint product into my life, I expected it to be like the anti-virus solutions that came before and I brought all the baggage from my old AV relationships into that decision. But since then, I can't think of endpoint protection in the same light. I sleep better at night. I've started focusing on bigger, more important problems, and my team is more productive than ever.

Endpoint Detection and Response (EDR) has given me a glimpse into a world where a computer can actually be secure. If I ever move to a new job at a new company, literally the first thing that I will do on day one will be to replace or enhance the old anti-virus with EDR. On the surface, this seems like an incredibly unsexy thing to do if you're a new CISO. But I think this success is what has allowed me to reach my potential as an experienced CISO. I hope that this book inspires you to fall in love with endpoint security all over again.

Peace,
George

## The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it in your own conversations (personal or business-focused) with confidence.

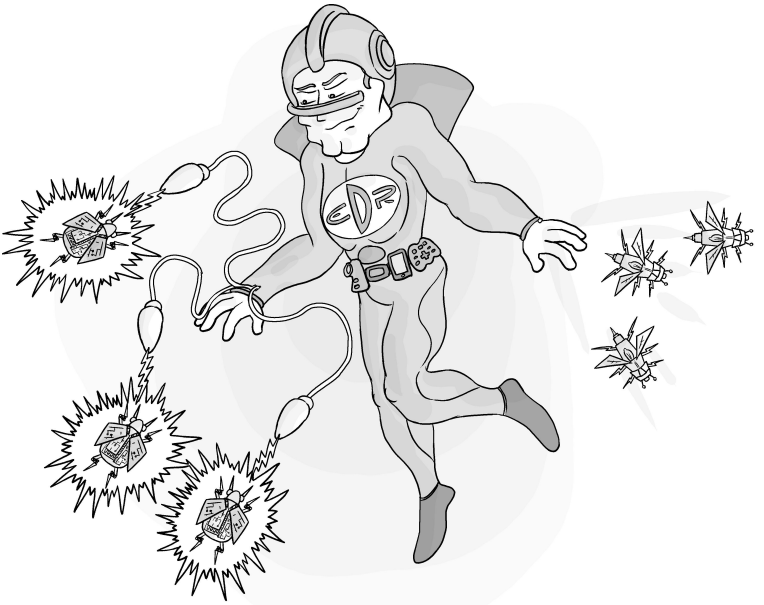
These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

## “Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes, it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Greetings. Within these boxes I can share just about anything on the subject at hand. Read ’em!

# From Anti-Virus to EDR




Every superhero has a weakness; Superman has his kryptonite, Daredevil can't handle loud noises, and the color yellow will beat the Green Lantern. Software has a weakness, too: *it's called malware*.

For a long time, anti-virus has tried to fix that weakness, but there hasn't been anything "super" about it. But there is another category of superhero whose power comes from their ability to use innovative tech to overcome their weaknesses; Tony Stark has his Iron Man suit and Batman has his toolbelt. Endpoint Detection and Response (EDR) is this latter type of superhero for the world of software.

In 2014, Symantec's Senior Vice President Bryan Dye famously said, anti-virus "is dead." At the time, this eulogy was actually a bit of an understatement. CISOs had been clamoring for years

that anti-virus had so little value that it should be given away for free. Somehow, almost four years later, companies are still paying for the same old anti-virus solutions.

Dye was only partially correct. Anti-virus is still the first line of defense. But with evolving threats, it does not provide protection against the most dangerous advanced threats like fileless malware, ransomware, and zero-day threats.

But perhaps there is a lesson to be learned from the zombie-like pervasiveness of traditional anti-virus solutions:

*We are waiting for anti-virus, or something like it, to come along and deliver on the promise of a computer that actually works without constant patching, rebooting, and reimaging.*

Anton Chuvakin, Research Director at the industry analyst firm Gartner, first defined the term Endpoint Threat Detection and Response (ETDR) in July 2013 as "the tools primarily focused on detecting and investigating suspicious activities (and traces of such) and other problems on hosts/endpoints." Over the last six years, these tools have continued to evolve to not just detect, but to enable response and actually prevent incidents before they happen.

To understand where EDR tools are going, we first need to understand where we've been. And that means understanding how anti-virus works, and what its limitations are. Traditional anti-virus tools use signatures to help detect malicious files on computer systems.

This is the functional equivalent of the FBI searching through its fingerprint database for a connection to a particular crime scene. Sometimes the FBI won't have seen a criminal before, so they won't have that fingerprint in their database.

And fingerprints aren't necessarily reliable; fingerprints can change over time through cuts and scarring. Hackers can also manipulate malware so that the signature file no longer matches the previous one, and hackers can change these signatures, or "hashes," infinitely.

This creates a cat and mouse game with anti-virus companies rushing to find samples of new files and hackers constantly shifting their code. Sophisticated hackers may create custom code for a single attack, similar to how they may spear phish a single individual, making this traditional signature-based approach ineffective at providing complete protection.

The real value today, if any, that anti-virus companies provide is that they employ thousands of threat hunters, training them in how malware works and how to find it. But instead of sending them in the field to stop criminals, they spend their days alone in cubicles, taking fingerprints of where hackers have been instead of trying to find out where they are going next.

Imagine if the FBI trained thousands of agents, had a budget of billions of dollars, and all the majority of those agents did every day was to collect more and more fingerprints of old crime scenes. Would you feel as though your tax dollars were being well-spent?

Putting it bluntly, traditional anti-virus isn't enough. It may stop some threats, but from experience we know that relying on this method means you'll be almost 8 months behind your hackers. A recent IBM/Ponemon report calculates that dwell times, the time between an initial compromise and when the malware is contained, averages 279 days. If anti-virus were working effectively, those dwell times would be measured in seconds or, preferably, be blocked in the first place.

EDR rejects this cat and mouse game of hunting for fingerprints with a process that looks a lot more like facial recognition. Behavior-based tools don't rely on hashes to search for known bad files, they look at how a given piece of software interacts with the operating system and how it behaves in memory to detect patterns of bad behavior, providing much greater accuracy with very few false positives. And EDR is already starting to make an impact.

Trustwave's 2019 Global Security Report found that it took an average of 55 days from intrusion to detection, down from 83 days in 2018. This is due, in part, to better EDR tools that can dramatically decrease investigation and response times.

I've heard that 63% of all data breach victims are notified by an external party: law enforcement, a customer, or a vendor. I don't know about you, but that would make me blush a little.

True Story: I was working for a startup early in my career and we got an unexpected ISP bill that was ten-times the normal cost. Our Internet connection was burstable, and for the past month we had been hitting our maximum threshold.

The Culprit: A hacker was using one of our servers (that had the latest anti-virus) to host a ton of movie files buried 100 layers deep in some system directories.

The Problem: A patch was missing and anti-virus failed to protect the server.

# Anti-Virus Isn't Enough

The world's first computer virus came out in 1971, only two years after the creation of the ARPANET in 1969. It would take another 15 years for commercial anti-virus products to come along, but when they did, there was an explosion of products.

In 1987, McAfee, ESET, and G Data would all release platform-specific anti-virus products. After that, anti-virus manufacturers would work to make their software cross-platform, and begin the fast growth process in order to keep up with the explosion of cybercrime. But modern anti-virus still works essentially the same as these first examples of anti-virus.

Today, every computer administrator knows that it would be irresponsible to deploy a computer on a corporate network without some sort of anti-virus product. There are hundreds of different anti-virus products on the market today. There is a whole industry, from Gartner to NSS Labs or AV Test, which rates the effectiveness of anti-virus solutions to help companies to make better decisions.

## How can you tell which endpoint product is right for you?

Endpoint protection solutions have evolved significantly over the last decade, and with all of those changes and marketing buzzwords it's difficult to know which solution will work in your environment.

There is a spectrum of solutions that are increasingly effective against unknown signatures, zero-day vulnerabilities, and fileless malware. Anti-virus is the first step on this spectrum, but has limited effectiveness because it is, by design, retrospective and reactive. Containerization is the next step but, as I'll discuss later, it only works with a small number of applications (mainly browsers).

The next level of effectiveness comes with Next Gen AV which utilizes machine learning for on-disk static file analysis. This requires frequent updates to the machine learning model to keep up with threats and doesn't work against fileless attacks.

Threat Intelligence takes a slightly different approach but, like anti-virus, is also retrospective and reactive, requiring indicators of compromise and extrapolating observations based on known threat data.

We don't really see effective solutions to combat fileless malware until we get behavior-based solutions that understand the threat techniques themselves to provide protection without prior knowledge of malware. The most effective protection against fileless attacks is In-Memory Analysis, which uses reverse engineering and binary analysis to understand malicious behaviors.

Most IT administrators are familiar with magazine reviews of products, industry analysts, and lab testing – and it makes sense to review this material before making a significant investment in an endpoint product – but these approaches also lag behind the new types of attacks that organizations are facing. Traditionally, anti-virus tests were run by looking at large sample sets of malware and each anti-virus tool would be run on a system to see how many of those malware samples could be caught. It was common over the last 10 years to see anti-virus vendors catch anywhere between 50 and 80 percent of those sample sets in a lab environment.

But these tests seldom mirror what actually happens in the real world. Vendors know what samples will be in the tests. The tests don't look at zero-day vulnerabilities. The tests don't use custom code targeted at a specific company for just that test.

All organizations will, at some point, reach this juncture when they must seek better measures of effectiveness and ask some serious questions:

*Can the product decrease dwell times?*
*Can the product catch custom code?*
*Can the product defend against fileless attacks or attacks that run in-memory?*

If the answer to any of these is "no," we need to find other products that provide a more complete solution.

**Pro tip:** if a product takes hundreds or thousands of hours of customization to get it to be 85% effective at doing what the vendor sold it to you to do, don't buy it in the first place. You're working for the vendor from that point forward instead of doing your job.

The reality is that, even though running anti-virus is considered table stakes today, the buy-in is already too high for most of us to have a seat at the table. Anti-virus constantly scans your computer for new files, eating up CPU.

In order to be "effective" new signature files need to be downloaded and applied every 5 minutes. And applying blanket signatures has caused massive outages for at least one major anti-virus vendor. And what if your computer isn't connected to the network for security reasons and you can't install updates?

Users have grown to despise anti-virus because of this.

Instead of helping to build a connection between security teams and the business, anti-virus is seen as another way security prevents the business from running. Users might even be tempted to disable anti-virus if they have the rights, and desktop or server administrators will sometimes disable or remove it as a troubleshooting step when processes mysteriously stop running.

We should all be asking ourselves: *how did we get here?*

Sometimes, keeping a computer off-network for security means you can't connect to the Internet for updates or patches. Accidentally connect it to the network again and you'll create a security nightmare. Once, I even used superglue to fill in the USB ports and network cards of several desktops to avoid this issue.

## Vulnerabilities Baked in with Security on Top

Software today is written and released according to a schedule defined by the pressures of an incredibly competitive market. As a result, computer programs are filled with bugs and potential security vulnerabilities, waiting to be discovered and exploited. Programmers haven't checked for buffer overflows and don't always validate input.

Sometimes, software will be available for years before a vulnerability is discovered, and a vendor will rush to release a patch, sometimes informing customers that they need to immediately update their computers. In the security industry, this day is referred to as "Day Zero."

That vulnerability, however, could have existed for years, potentially dating back multiple versions of the vendor's software. Because of this, these vulnerabilities are referred to as zero-day vulnerabilities and hackers as well as governments are known to stockpile these as weapons to potentially be used for their own purposes.

Sometimes, these vulnerabilities are sold on the black market for hundreds of thousands of dollars. But until that vulnerability is discovered, either by the vendor themselves or

by a security researcher or security company willing to share with the world, computers remain dangerously vulnerable.

Since anti-virus was invented, whole new categories of malware have been created, like ransomware or fileless attacks, that can't be detected by the traditional fingerprinting approach used by the old anti-virus products. Modern solutions to this problem shouldn't follow the same path that we've taken for years just because it's the way we've always done things.

To paraphrase Marshall Goldsmith, the New York Times bestselling author and leadership coach, "what got us here won't get us there."

## Grown-Up Endpoint Protection

Anti-virus is now in its 30s. It's graduated from college and has a steady job. It's moved out of its parents' house and has a mortgage of its own. But it's still trying to figure out what it wants to be when it grows up. When it introduced itself as "AV," people thought it was there to help with their VCRs and projectors. For a while, people were calling it "Anti-malware," which made it feel a little more mature.

Today, people have come to realize that our friend anti-virus exists in a world that needs a more diverse skillset. Sure, next-gen anti-virus uses some machine learning and behavior analysis, but even that's not enough to fill the gap between threat and defense.

The new security valedictorian is called EDR, Endpoint Detection and Response. This title is appropriate, as it can do more than just identify signatures and quarantine files. It can help respond; it can be a part of the solution instead of being a part of the problem.

EDR is behavior-based and uses in-memory analysis to deliver a more predictive capability that does not require prior knowledge of the specific attack. This puts the threat in context for the IT administrator by identifying the probability of whether a program is malicious and gives them the time they need to prioritize and remediate issues.

Because of the issues outlined in the previous section, legacy endpoint companies have rebranded their solutions from "anti-virus" to "anti-malware." In addition to giving it a snappy new name, they added new approaches to detect and respond to malware, to whitelist applications, to containerize, and to detect anomalies.

## Application Whitelisting

This technique is designed to prevent end users from running unauthorized software on their desktops. The challenge with this approach is scalability. For organizations with large numbers of desktops, there will be a correspondingly huge amount of software that has to be vetted, approved, and change controlled. BYOD and cloud computing models also prevent this approach from being fully realized. Security teams may spend months or years trying to get this approach to work for large environments.

## Containerization

Similar to how traditional anti-virus will "quarantine" infected files, this approach runs processes in a protected mode so that the anti-virus can detect malicious activity and shut it down before it infects or damages other parts of the computer. The challenge with this approach is that it requires significant additional processing power, and it only works with specific applications. It won't be a good fit for servers, where CPU is at a premium. And it doesn't work for end user workstations since even having unapproved browser plug-ins can make it unstable.

## Anomaly Detection

This approach takes me back to my high school days: *what is normal?* The assumption here is that you can detect when something weird happens and alert administrators. There will always be a high false positive rate with this approach because there is never an average baseline that can be captured. Filtering through all those false positives will keep your security teams from investigating and responding to real threats.

The trouble with these approaches is that, instead of making companies more secure out of the box, they shift the burden of work onto security teams. They give security teams tools they may have never had before, but unless the team is large enough and has the right skill sets, these "new approaches" can create some potential liability for them; some may point fingers, alleging the security team "knew" about an issue and didn't do anything about it.

One of the challenges with traditional anti-virus tools is that it is almost impossible to answer the question:

*How did the malware get there in the first place?*

This is a crucial question, whose answer leads to improving user behavior as well as improving security protections.

There are tools that create questions and there are tools that answer questions. Traditional anti-virus tools fall in the former category. They generate reports when they find suspicious files, but the natural question that follows is usually: *How did that virus infected file get there?*

EDR tools help answer that question.

EDR works like a DVR for your computer. You can rewind computer processes to see when the user clicked a malicious link or opened a suspicious attachment. The better the EDR tool, the more natural and fluid it is to follow a process or person through time. More importantly, you can see how the malware interacted with the computer, find other computers that may have been infected, and contain the incident rapidly.

There are two additional, noteworthy benefits of this approach to consider.

1) Unlike traditional anti-virus, EDR doesn't require signature updates every 5 minutes and machines don't have to be connected to the Internet to have protection.

2) Behavioral detection doesn't require constant scanning of a computer's file system, which means there will be little to no impact to CPU utilization; a common complaint against traditional anti-virus products.

Real-time protection is already too late. It takes minutes or sometimes hours for teams to respond to incidents, particularly when outbreaks happen. What we need is future-time protection or Minority Report-style precognitive ability.

Some EDR solutions require highly skilled technical admins to get good insight, but they give a very detailed view of what happened. Organizations that have Security Operations Centers or MSSPs can cut costs and still benefit from the analytic capabilities that some EDR tools offer. Others solutions are more set-and-forget, which may be better for smaller organizations with limited technical ability.

## Grown-Up Malware

Anti-Virus isn't the only thing that has grown up. The world's first computer virus had a child-like playfulness, posting a "catch me if you can" style challenge on monitors of computers that it infected. In the late 90s and early 2000s, hackers were still releasing malware more for notoriety than economic gain.

There are still significant financial motivations at play; Cybersecurity Ventures projects that the cybercrime industry will become worth over 6 trillion dollars by 2021. Nation state actors, not to be outdone, have become more and more willing to impact and influence the citizens of other countries as well, no longer limiting themselves to purely political or economic motivations.

The evolution, and revolution, of the cyber arms race can be traced back to one virtual "gunshot" heard round the world: Stuxnet. In the late 2000s, a computer virus was discovered inside power plants, air traffic systems, and other control systems across the world. The virus remained inert unless certain conditions were met, which was unusual for computer viruses of that day, which usually spread uncontrollably. Also unusual was the complexity of the virus, which was 20-times the size of the next biggest virus that had yet been observed.

As the virus was reverse engineered, it was discovered that Stuxnet had multiple modules that could be independently deployed, allowing the virus to morph as well as to be updated while still in the field; something which had never been seen before in malware.

Stuxnet took advantage of 20 different zero-day vulnerabilities, when most other viruses didn't leverage any at all. The zero-days that Stuxnet used would have been worth millions of dollars on the black market.

Notice that the creators of Stuxnet went through all this trouble to produce malware as complex as any commercially available software.

It turns out the specific conditions necessary to trigger Stuxnet's destructive capabilities required you to be running a nuclear power plant or uranium centrifuge in a specific country: *Iran*. Once triggered, Stuxnet did its job. Kim Zetter, author of Countdown to Zero Day, writes that Iran's nuclear program was delayed years because of the destruction unleashed by the virus.

Unlike a bomb, the code that powers a virus stays around well after it has been deployed. Since the code from Stuxnet had spread beyond just the computers inside Iran, the code that created it would give prospective cybercriminals a roadmap for building similar, commercial-grade malware to expand globally.

Good malware is like a bad salesperson; once you let them get their foot in the door, they want to talk to everyone.

It also demonstrated a demand for zero-day vulnerabilities, potentially adding to their black market value. This, combined with the widespread adoption of Bitcoin for anonymous currency transactions, has facilitated an explosion of the cyber black market.

Fast forward to 2016. The Washington Post reported that the NSA's spying toolkit had been leaked online and was up for sale in a black market auction that mirrors the plot of a James Bond movie. Whether this hacking toolkit was ever actually sold to anyone is still a mystery, but at least one vulnerability from this

toolkit would be found in the 2017 WannaCry ransomware outbreak.

The WannaCry outbreak was accidentally stopped only a few hours into the worldwide incident, prompting many to suspect that it was the work of an unsophisticated lone wolf. But this is actually worse news in my book because it means that even the least sophisticated script kiddy today has access to nation state-level hacking tools.

Malware that takes advantage of vulnerabilities in software isn't the only concern for security teams. According to TrendMicro, this year has seen a 256% *increase* in fileless attacks. Traditional endpoint protections won't work with fileless attacks, since this method of attack only runs in memory or use administrative tools already installed on a computer to achieve their goals. Regardless, real-world cybercriminals also steal valid credentials, making it nearly impossible to distinguish them from real users; traditional anti-virus is useless against this.

Modern malware is fast-moving and once it's in the door, it moves laterally to strengthen its position in an attempt to prevent removal from the network. Malware kits that are on the black market today have already begun to deploy increased automation and machine learning capabilities to help ensure their expansion and effectiveness. The creators of some ransomware kits, for example, have guaranteed success rates and dedicated customer service representatives to help ensure you get the highest return on your investment!

There is a very clear roadmap that almost all attackers follow. Lockheed Martin codified this process into what they call their "Cyber Kill Chain." They break all attacks down into seven distinct steps: *reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions or objectives.*

Phase one starts with cyber reconnaissance, which may come in the form of monitoring a company's LinkedIn profiles for employees or harvesting data from a corporate website. Next, hackers will choose an exploit that suits the target and put this exploit into a package. These first two steps in the chain can take an attacker hours to months of preparation and planning.

In the second phase of the kill chain, which can take just seconds, the package is delivered to the target via email or an infected USB stick, which – in the delivery stage – is physically transferred to the victim. Once the package is run, code is executed and the malware is installed on the target, in this case the target could be a laptop, mobile phone, desktop, or server.

In the third and final phase, the goals of the attack are realized. The computer joins a command and control network to receive additional instructions or additional attack payloads, and the attacks progresses toward their objectives (exfiltrating or destroying data, holding a victim hostage, or stealing secrets for a competitive advantage; for example).

Any part of this cyber kill chain can be outsourced to specialists in each area, further increasing the overall likelihood of success of an attack.

Hackers doing their reconnaissance will target you when you are least prepared, be it on a weekend, a holiday, or even when you're in the news for having just been attacked.

## Real-World Implications

I recently implemented next-generation AV/EDR, replacing multiple traditional signature AV-based solutions. And I ran the numbers.

With the old solution, we were still seeing about 1,000 endpoints, or over 20 percent, of our computers with some kind of malicious files every year. This had a huge impact on the business.

It takes several hours to reimage a computer, and an employee would usually be without a computer during that time. If I'd had to continue to do this, the impact could have been hundreds of thousands of dollars in lost employee productivity. With the next-gen product, I saved all that, plus infections went down to one or two per month. We pay nearly the same now as the old solution, and the savings in lost productivity alone justify the cost.

## The Key Takeaways

In 2019, 350,000 new malicious programs (malware) and potentially unwanted applications (PUA) are found *every day*. This monstrous statistic belies an important myth that traditional anti-virus helped to perpetuate: *attacks of the past were based on known threats and that those threats applied equally to everyone.*

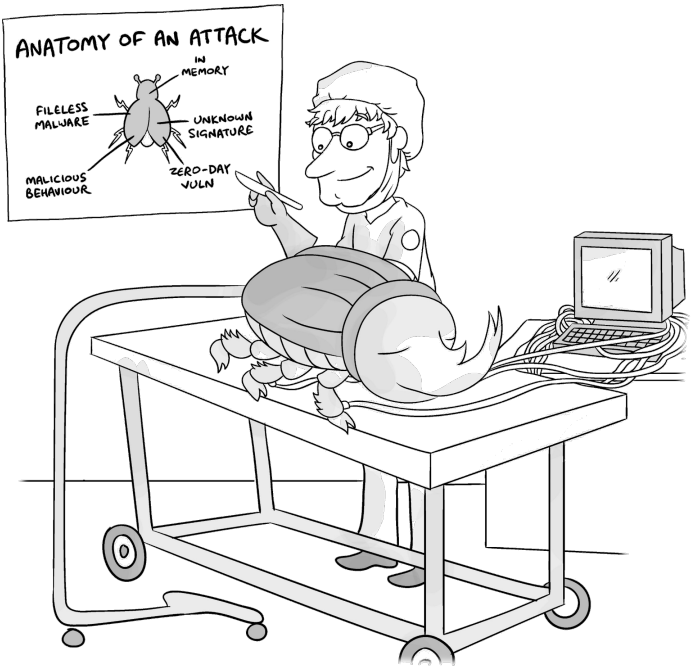
Today, attacks are custom to each target and have never been seen before. Because signature-based anti-virus just looks for known files, they don't actually look intelligently for behaviors that would exploit zero-day vulnerabilities, target weak or incorrect settings in your environment, or leverage valid credentials to exfiltrate data.

The Dark Web is now a diverse place where everything related to cybercrime is for sale: crimeware-as-a-service, exfiltrated data at wholesale prices, auctions for zero-day vulnerabilities, and on-demand denial of service attacks. There are now many fee-based threat intelligence services that monitor these networks and report when and if these services begin to mention your company or your company's executives.

Grown-up malware should make us ask ourselves, what is an endpoint? If cybercriminals don't distinguish between personal laptops and company laptops, why should we? If user accounts are so easily compromised, how do we distinguish between the good guys from the bad guys? Or better, how can we stop account credentials from being so easily compromised in the first place?

*EDR is the best place for us to start.*

# Vendor Sponsor Chapter – GoSecure




*Security teams are in a never-ending race against time.*

One of the biggest challenges facing security teams is dwell time; the time between an initial compromise and when the breach is fixed and new preventative measures are put in place. According to the most recent IBM Cost of a Data Breach report, it now takes a combined 279 days to identify and contain a breach, up from 266 in last year's report. Speedy responses could be a massive cost saver. Companies able to detect and contain a breach in under 200 days spent on average $1.2 million less. To protect your business, security teams need to reduce dwell times down from months to minutes.

Today's attacks are fast-moving. Inside the dwell time window, hackers will move laterally through the network until they reach your most critical assets. Any latency in detection and response

time increases exposure of sensitive data and businesses operations. Security teams need to look to new technologies and procedures to strengthen their security posture.

As I noted before, existing endpoint solutions are retrospective and reactive. They rely on signatures and indicators of compromise (IoCs) for detection, meaning they can't discover threats until after those threats have acted (post-breach). But there's hope, because…

*The security team of tomorrow will be able to predict the future.*

To win the race against time, successful CISOs, security teams, and visionary MSSPs are turning to a new class of endpoint security solutions – Predictive Endpoint Detection and Response (EDR). GoSecure's Endpoint Protection Platform makes this critical pivot, delivering a Predictive EDR solution that allows security teams to adopt agile and proactive threat management strategies. Predictive EDR solutions give security teams the tools and information needed to protect their sensitive data before an incident can interrupt business operations.

Predictive EDR is built on three pillars: In-memory threat detection, predictive analytics, and Big Data storage and management. They combine to detect the most threats, predict what they can do, and respond quickly to terminate and prevent lateral movement to other IT assets. The interplay between these key technologies enable GoSecure to fundamentally transform the standard for endpoint security solutions.

## Visibility

To have effective EDR, you can only stop what you can see. GoSecure provides visibility across endpoints, the network, email, and more, empowering correlation, analysis, response, and mitigation.

## In-memory threat detection

Existing anti-virus, next-gen anti-virus, and EDR vendors are locked in a continuous game of cat and mouse with cybercriminals. As fast as they update their signatures and IoCs, hackers devise new attacks to evade detection. With over 959 million new malware strains introduced so far in 2019, the reality is new threats penetrate today's defenses when those defenses don't know their enemy.

In 2009 GoSecure introduced its patented Digital DNA. Digital DNA captures new and unknown threats in memory, the only place that can't evade detection; it is the most reliable last line of defense. It is so powerful that leading security vendors, including Symantec, Rapid 7, and Digital Guardian are licensing Digital DNA to enhance their solutions.

## Predictive analytics

It's not uncommon for modern attacks to make their initial compromises within minutes. Security teams require timely information to prioritize forensic threat investigations and terminate them in the earliest stages.

The post-breach detection requirements of signature-based and IoC-based endpoint solutions put security teams in catch-up mode. Digital DNA transforms that into a prospective position, detecting and monitoring malicious behavior as it unfolds in memory. GoSecure combines this with a rich knowledge base and machine learning to deliver predictive analytics which provide insight into the future to terminate threats before they can act.

Predictive analytics puts malicious behavior in context. *Is it executing suspicious processes? Is it moving laterally through the network? Are privileges escalating?* Digital DNA reports on the threatening capabilities of a behavior, like a PowerShell script making a memory modification that's capable of injecting code

or data into another process, or making an HTTP connection, for example.

Predictive analytics sums up a behavior with an impact score to help security teams prioritize and focus their forensic and response activities.

## Big Data storage and management

Threat hunting is a critical component of any security strategy. With average dwell times of 279 days, there is a large data gap between what security analysts need – the correlation of 279 days worth of data to provide insight and faster response – and what traditional endpoint solutions provide.

Effective detection of new and unknown threats requires collection, storage and management of more data than before. Most endpoint security solutions are architecturally limited to holding data for 90 days or less. Some hold data for only one or two days.

GoSecure's Predictive EDR is architected on a Big Data backend. It is designed for high availability. All nodes in the cluster are functionally equivalent and run the same services. Need to store and manage more data? Simply add another node to the cluster. The Big Data backend stores an unlimited amount of data for an unlimited time, a necessity to support effective and accurate threat hunting.

## Integration and deployment

Data and performance can make a powerful Predictive EDR solution, but integrations with third-party security tools are key to evolving the security landscape, and are an important feature to look for in an EDR solution. GoSecure enables a new layer of actionable data proliferation with API integrations with other security solutions, aggregation tools (HP ArcSight, IBM QRadar) and network-based security solutions (BlueCoat Security Analytics, CAS/MAS VMware NSX).

Finding an EDR solution with multiple deployment models will help you meet distinct budgetary and organizational needs, rather than forcing you to squeeze in the wrong tools or carve out room for a bigger price tag. This includes the availability of Managed Detection and Response services and MSSP partnerships, valuable resources for small-to-medium enterprises with limited security budgets and staffing. For larger enterprises with more-established security teams, look for Predictive EDR solutions which can be deployed on-premises or as a cloud-based service via reliable providers like AWS.

And throughout this whole process, keep in mind… *Predicting behavior is the key to preventing breaches.*

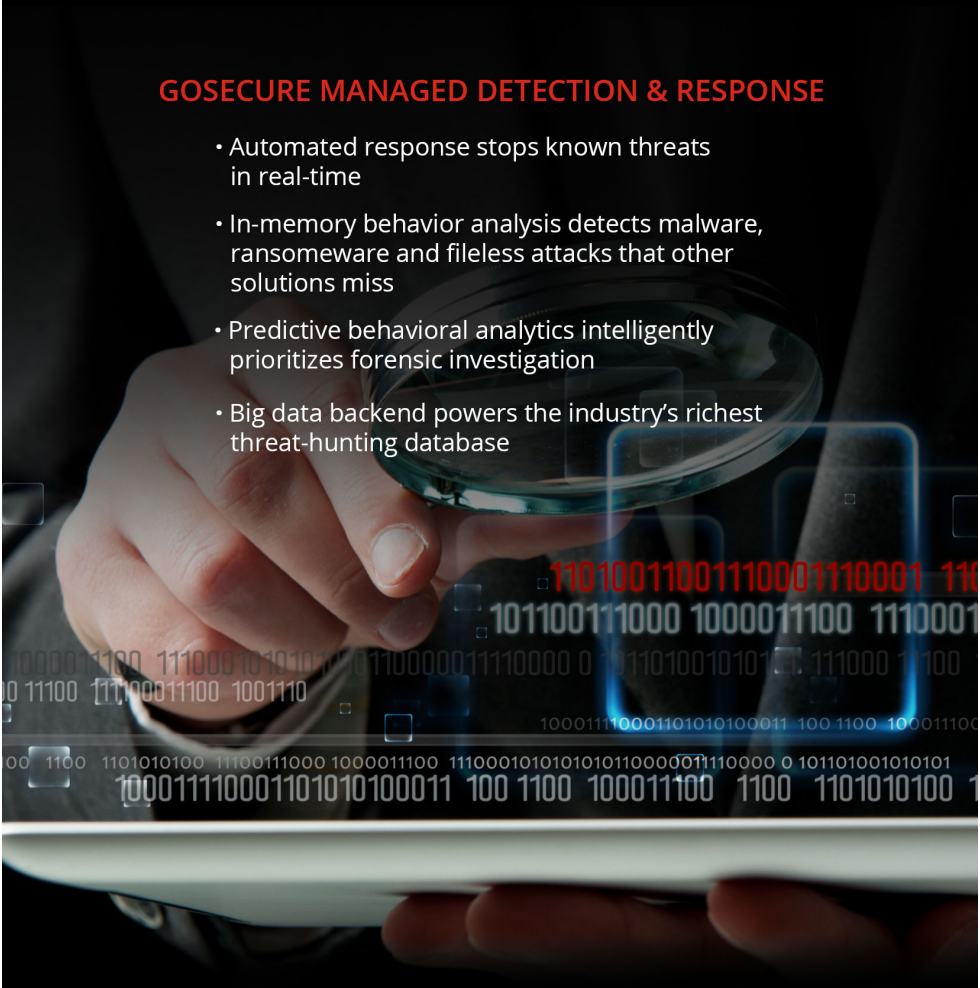
# NOTES

# DETECT | PREVENT | RESPOND

## TO MALICIOUS THREATS AND BEHAVIORS IN REAL-TIME ACROSS THE ENTERPRISE

### GOSECURE MANAGED DETECTION & RESPONSE

- Automated response stops known threats in real-time
- In-memory behavior analysis detects malware, ransomeware and fileless attacks that other solutions miss
- Predictive behavioral analytics intelligently prioritizes forensic investigation
- Big data backend powers the industry's richest threat-hunting database



GoSecure

To learn more, visit www.gosecure.net

# Easily “converse” about endpoint detection and response in any setting.

Within today’s technology landscape hides a diverse array of security threats and weaknesses; from fileless malware, to ransomware, to zero-day vulnerabilities. Malicious actors use these to strike at sensitive data, often with little resistance. Security teams must arm themselves with the tools and knowledge necessary to understand their adversaries’ tactics and stop an attack before it occurs. This book explores a necessary shift in defensive strategies to take a proactive approach to endpoint security.

## About George Finney

George Finney, J.D. is the Chief Security Officer for Southern Methodist University and a licensed attorney, CIPP, CISM, and CISSP. George is a frequent speaker on the topic of Cybersecurity across the country, with a focus on improving Cybersecurity through a combination of neuroscience, psychology, and wellness.

ConversationalGeek®

Visit conversationalgeek.com for more books on topics geeks love.