ENDGAME.

AN ADVERSARY-FOCUSED APPROACH TO ENDPOINT PROTECTION

IAN MCSHANE, VP PRODUCT MARKETING

INTRODUCTION

Most organizations still focus all of their endpoint security controls in one area: Execution. Trying to stop bad files from running, trying to stop unwanted applications, trying to prevent malware from gaining unauthorized access to a machine or a network.

ATT&CK has become the buzz word du jour for the information security industry, so there's a good chance you have already heard vendors gushing about their ATT&CK alignment. To level set, let's just say that the ATT&CK matrix describes many of the attacker techniques that make up the tactics, and we'll be getting familiar with this later on.

In the MITRE ATT&CK matrix, Execution is just one of the 13 columns of adversarial tactics. There can be no doubt that adversaries have the advantage over organizations that are purely focusing on Execution. And that's not to say that those organizations are doing anything wrong. They have been let down by their security vendors.

The traditional endpoint security vendors decided that rather than give customers the best possible protection, they would add new products and new SKUs and make second-class citizens of those that could not afford to upgrade to the best protection available. Worst of all, some vendors even encouraged blaming end-users for incidents.

Then there was a period of time when vendors, old and new, claimed to be able to reduce total cost of ownership (TCO) and to maximize return on investment (ROI) by throwing in machine learning, cloud-services, and managed-services.

My friends, I'm here to tell you that **there is no one-size fits all**, and if you are blaming your end-users you need to take a look at why you and your vendors are allowing that end-user activity to occur.

WORK SMARTER, NOT HARDER

Twenty-odd years ago, I was a practitioner. I spent a lot of time going through installation and configuration, hitting next, checking the EULA box, hitting next, next, finish – and almost never coming back to it again. The default AV would detect and block things, anti-spam would block and quarantine things, and I would seldom have to go back and make policy changes or do anything at all with the alerts that were raised.

Times have changed, and for all of the talk of TCO, ROI, machine learning, AI, automation and so on, one of the dirty secrets of the information security industry is that you and your IT and security teams are still going to have to do some work. Your security team is not being replaced. In fact, as you move from an Execution-only focus to what we call an Adversary focus, you'll actually have MORE work to do.

So, you have to look for the tools that help you work smarter, and help you make faster, accurate, confident decisions. InfoSec is all about decision making around risk mitigation, but I'm getting ahead of myself.

"THERE'S NO ONE-SIZE-FITS-ALL FOR SECURITY, THE ERA OF SET AND FORGET IS ALL BUT FORGOTTEN."

– IAN MCSHANE, RESEARCH DIRECTOR ANALYST, GARTNER

THE EVOLVING THREAT LANDSCAPE

The best-case scenario is the status quo you have now:

- SECURITY IS EXPENSIVE.
- HIRING PEOPLE IS EXPENSIVE,
- FIRING PEOPLE IS EXPENSIVE,
- KEEPING PEOPLE IS EXPENSIVE,
- GIVING PEOPLE THE TOOLS THEY NEED IS EXPENSIVE,
- GIVING PEOPLE THE TIME IS EXPENSIVE.

It's all expensive. And that's the best-case scenario.

Worst case – all that expensive human capital and tool expenditure PLUS productivity loss, reputation damage, and breach disclosure.

Yet with all the anecdotal talk and the freely available evidence, you still have a tough job to justify budget to invest in a stronger security posture. Especially when vendors mask the true cost of security and demonstrate that renewing a legacy, file-based antivirus product is usually less expensive than selecting, deploying, and maintaining a modern solution. No matter how much the vendor talks about artificial intelligence, a file-based approach is NOT enough.

Whether it's hard to justify budget or not, the fact is that execution-based protection – where everything is based on deciding if a file is good or bad – is already out of date. Ten years ago, the big, traditional vendors used to dominate this market with products that were good enough to detect commodity malware, but their biggest selling point (or renewal point) was that they were familiar and comfortable for organizations to use. Unfortunately, they still lack the threat intelligence and prevention capabilities necessary to even recognize modern attacks today, much less the capabilities to remove threats from an enterprise network.

PONEMON INSTITUTE, 2017

55% OF ATTACKS **ARE NOT CAUGHT BY ANTIVIRUS**

$5M THE AVERAGE COST OF **A SINGLE ATTACK**

Even two years ago, file-based AV was preventing less than half of the most common attacks. Traditional vendors, and even some of the so-called "Next-Gen" vendors just couldn't keep pace with adversary evolution.

Almost all victims of the biggest known breaches were doing their best with the products at their disposal. Still, Ponemon reports that more than 50 percent of businesses have had a security incident that exposed data or compromised infrastructure. Focusing on files – or execution-based protection – led to over 75 percent of those attacks being successful.

And in the last couple of years, we've seen a rapid drop in the delta – the time gap – between nation state tools being leaked and then being used to breach enterprises. It's never been easier to bypass the simple security controls that organizations have relied on for a long time.

More than that, adversaries are able to completely avoid file-based detection by operating entirely in system memory, using built-in OS features like PowerShell or WMI. There is also a black-market that sells the difficult and expensive to develop techniques as a service, so they can be adopted without the need for much technical ability.

ENDPOINT SECURITY WILL ALWAYS CONSUME YOU

Two decades ago, AV signatures could keep up with the number of bad files. Then a new market emerged, focused on "personal firewalls," sometimes known as host intrusion detection (HIDS). You might remember products like Zone Alarm that ended up being bought by one of the network vendors. That type of capability ended up combining with AV and creating what we now call Endpoint Protection Platforms (EPP).

Sandboxing and process isolation used to be a big deal, but then adversaries found out how to escape from them, or to detect that they were being monitored, and simply stopped doing anything suspicious, leaving the sandbox to decide that the file was benign, or at the very least, not a bad file. Then when the file was run by a user outside of the sandbox, surprise, their endpoint was popped.

Then comes NGAV - a phrase that does more to confuse organizations and end-users than it does to describe anything useful. It takes longer to try and understand what people mean when they say "Next-Gen," and more often than not it does not mean what anyone thinks it means. What it originally described was AV that didn't rely on signature distribution.

Which brings us to a worthwhile deflection point.

I'm sure you have heard talk about how terrible signatures are for detecting bad things. Well, that's nonsense. Signatures are the most accurate detection mechanism. Because signatures look for things that are definitely known to be bad. If a signature says something is bad, it almost always is.

Accuracy and effectiveness of signatures was never the problem. The problem was the distribution and scale of signatures. There were too many unique bad files, and by the time a vendor pushed out the new signature package, it was already out of date.

So machine learning solves the distribution problem, not the accuracy problem. And, as the pioneers of ML in endpoint protection will tell you, it's really hard to be accurate. Many early adopters suffered with huge numbers of false positives – where legitimate files or applications were accidentally blocked.

Now back to the timeline of buzzword bingo.

After machine learning comes the era of endpoint detection and response (EDR). We all know that prevention can never reach 100 percent. No matter how many decimal

places come after the 99.x, something will always get through. And, let's not be naive here, there are malicious insiders that are trusted by their organization that do bad things. So EDR was born to bring the ability to find endpoints, applications, and processes that exhibit suspicious behavior, to detect anomalies in the environment, and to respond to them. Contain the threat, isolate the device from the rest of the network, perform an investigation, and clean up after an incident.

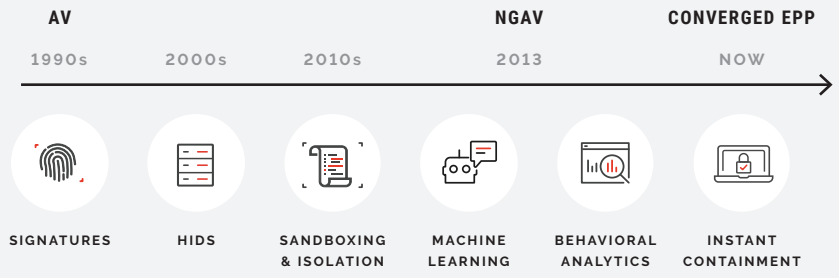
And here we are today, talking about adversaries. Endpoint protection has consumed all of these threat protection capabilities – and even more than this, actually – so the skills required to operate and maintain them effectively have evolved too.

KEYS TO PLANNING A STRONGER ENDPOINT SECURITY PROGRAM

1. MODERN ATTACKS ARE ADAPTIVE
   Adversaries will often try multiple methods to attack specific targets, and even the opportunistic attacks will make use of more than one technique. Even well-known vulnerabilities can work, because, after all, there are many organizations that simply don't have the ability to meet 100% patching targets. And that's okay. They just need to mitigate risks.
2. MODERN ATTACKS ARE DYNAMIC
   Attackers will change. They will look for specific behavior to decide if they are likely to be detected or not. The type of user, the type of device, the type of security controls, can all play a part in deciding how a malicious payload behaves.
3. MODERN ATTACKS ARE EXTENDED
   Often, the adversary will just wait and watch. They don't want to burn themselves by acting too quickly. It is much more beneficial to hold multiple machines to ransom, rather than just one

Modern attacks are not just malware, they are not just file-based, and there is no single silver bullet. The issue is also compounded by the fact that so many organizations have no controls in place to restrict end-user administrative privileges. In many cases, restricting Local Admin rights, or putting in place privilege access management (PAM) controls, would go a long way to improving risk mitigation.

SECURITY TIMELINE



EVOLVING FROM A FILE-BASED APPROACH TO AN ADVERSARY-BASED APPROACH

File-based approaches are always inherently Windows-based and focus on the Portable Executable file type. Few vendors have true support for macOS and it's Mach-O file format, and even fewer for Linux, much less any specific protections that align to the threat models of those operating systems.

By moving from an execution- or file-based focus, to an **adversary-focused** approach, your organization can future-proof your security plans and help mitigate risks that you aren't yet exposed to and maybe don't yet know about. And the most effective way to do that right now is by familiarizing yourself with the MITRE ATT&CK matrix that I mentioned early on.

ATT&CK stands for Adversary Tools, Techniques, and Common Knowledge. Real-time prevention is critical and always the preferred solution, but often it's not feasible to detect attacks at the first step, and ATT&CK is a way to describe the **post-compromise** activities that attackers take.

It covers over 200 different behaviors, with coverage over multiple operating systems. And more than being just a list of things, it is a wonderful learning tool. For example, if you don't know how an adversary can gain access to accounts with domain admin access, check out the techniques under the Privilege Escalation column.

The ATT&CK framework is an excellent learning tool for new security professionals and growing security teams to familiarize themselves with attacker techniques and

ATT&CK

/əˈtak/

Adversary Tools, Techniques, and Common Knowledge

understand the full breadth of attacker behavior.

ATT&CK emphasizes a layered approach to attack mitigation that goes beyond simple "hit or miss" detections. By mapping known adversary profiles and red team simulations to the framework, you are able to have specific and intelligent conversations with business leaders about the state of your organization's cybersecurity posture. Developing a baseline also gives you a way to evaluate how a change to a process or workflow can improve coverage.

That next security vendor presentation? How does that product move the needle for YOUR organization? Remember, there is no one-size fits all.

Use it to look at your renewals and reduce spending on too much redundancy.

EVALUATING MITRE ATT&CK CLAIMS

Sadly, ATT&CK claims made by vendors do not always mean what you think they do. In the Forrester MITRE ATT&CK™ Evaluation Guide – where seven vendors were tested by MITRE themselves – Forrester points out that buyers should be wary of claims around ATT&CK.

Especially as some vendors didn't seem to understand what they were being tested against. At least two vendors published

"ENDGAME LEADS THE PACK IN REAL-TIME ALERT GENERATION ACROSS THE KILL CHAIN. FROM A DETECTION PERSPECTIVE, THIS PRODUCT DOES ALMOST EVERYTHING WELL."

– FORRESTER MITRE ATT&CK™ EVALUATION GUIDE, 2019

press releases with information that was factually inaccurate and indicated that they didn't realize that the data – which is freely available on the MITRE website – showed that they performed terribly.

You should also be skeptical of any vendor that tries to cover the entirety of the ATT&CK matrix because there are some things that can and should be done outside of endpoint protection, like DLP or denial of service protection.

How can you navigate the marketing claims made by vendors, then? Well, check out Endgame's coverage against the ATT&CK framework at *www.endgame.com/blog/technical-blog/heres-how-we-do-numbers*.

As you can see, we point out where we have complete coverage, where we think we might have to do more in the future, and even where it doesn't make sense to mitigate on the endpoint.

Importantly, you should ask vendors when they will have coverage and visibility for non-Windows devices. Most organizations have at least one macOS device and at least one device running Linux. Without full containment and visibility for all devices, you're giving up ground to the adversary.

But even if you are giving up ground, or not covering everything, that's okay. Don't let the toxic sales element of InfoSec tell you that you are failing if you aren't doing everything.

Information Security is mostly about risk mitigation. Investments in InfoSec – whether endpoint tools, network devices, or moving from spreadsheets to business intelligence analytics – should come down to making informed, fast, and accurate decisions, such as:

- DOES THIS LOOK MALICIOUS?
- SHOULD I CONTAIN THIS ENDPOINT AND INVESTIGATE MORE?
- SHOULD I IGNORE THIS ALERT?
- HOW DO I PRIORITIZE ALL OF THESE RISKS?

Making an active choice to prioritize decisions, balance the risks, and decide what needs immediate attention is your job as a security leader. Deciding not to do something today – and understanding why you chose not to – is just as important as the tasks or changes that you do execute.

THE ROLE OF PEOPLE, PROCESS AND TECHNOLOGY

Let's say you want to focus on how your organization responds to the detection of a post-compromise activity. You want to understand how the change – whether that is a new tool, a new process, or a new hire – affects the metrics.

Yes, people and process are how you can make a real difference.

And you already have people and process involved. It might be that your detection system is actually based on a user calling the helpdesk. It might be that your response action is to re-image every device. But you have these systems in place today; you just need to bring it all together in a way that can operationalize your security.

It's not just about throwing money into technology that claims to solve these problems faster. You have to focus technology, process and people improvements in the right places.

Moving away from the traditional and so-called "Next-Gen" technologies into a platform built to deliver protection against adversaries, as well as bad files, means that you aren't double-dipping into resources on the endpoints.

A modern protection platform should be able to block not only malware but the sources of infection.

Proofpoint, Symantec, MimeCast, and Microsoft all have email security businesses. I'm sure you use one of them, but they still fail to protect against phishing scams – the number one infection point. They're busy talking about business email compromise, but they aren't able to solve the biggest security risk.

You need to identify an endpoint solution that can give you the best prevention coverage, and it needs to be across more than just Windows. Every vendor will claim to have some macOS or some Linux coverage, but the visibility and control usually pales in comparison.

Lastly, you also need to be able to work through investigations swiftly, which means having the right data in the right place.

Managing multiple consoles and admin interfaces just slows things down.

ADVANCED PROTECTION AS SIMPLE AS AV

Endgame's focus is on delivering the strongest protection to organizations of all sizes. We aim to reduce the skills gap by providing customers with a way to make use of advanced capabilities like threat hunting, anomaly detection, and incident response without having to be experts.

Our chatbot, Artemis, allows you to ask questions of your security data in plain English, such as, "find X file hash," or, "show me what X process did."

Our visualization engine, Resolver, helps customers solve incidents faster because you can see what happened and when, making it quicker to come to a decision about what to do next. And, if need be, isolate an endpoint in real-time to investigate without leaving the organization at risk.

Endgame is the only platform that makes advanced endpoint capabilities as simple to use as legacy AV. With a single agent – not two, three, or five like other vendors – Endgame brings an industry-leading combination of prevention and detection, no matter if your infrastructure is running on a submarine or on an endpoint in Starbucks.

Unlike vendors who rely on cloud-services, Endgame believes that the delay caused by sending things to be analyzed outside of the endpoint is unacceptable. We do it all on the endpoint itself, and we're the only vendor that can do this without bringing your endpoint device to its knees.

INDEPENDENT VALIDATION

Endgame is proven to deliver the best endpoint protection by leading independent testing organizations.

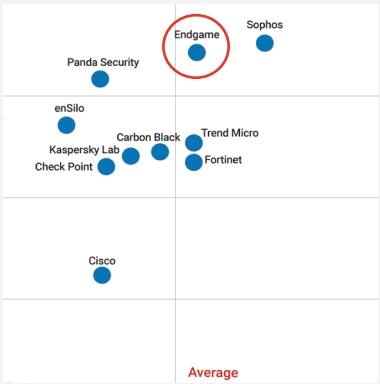
We are the only vendor that provides both leading prevention and detection in one product, with one agent.

We don't up-sell you on the next tier of protection. We believe in getting the job done and bringing the best protection to our customers EVERY time, not just when they pay extra for it.

NSS LABS

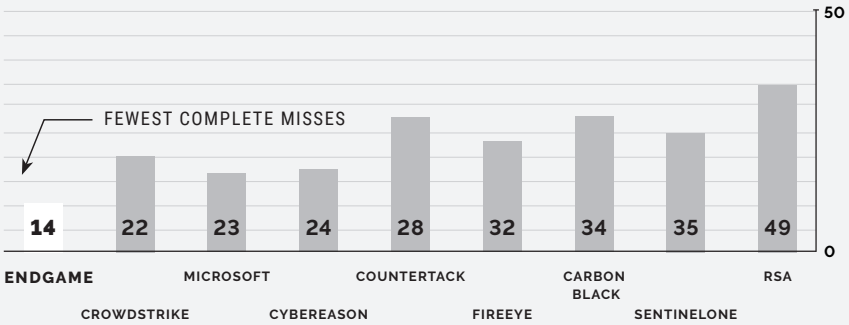
2019 NSS LABS ADVANCED ENDPOINT PROTECTION REPORT

- HIGHEST CONVERGED ENDPOINT EFFICACY **(98.9%)**
- **VERY LOW** TOTAL COST OF OWNERSHIP (TCO)
- **100% BLOCK RATE** ACROSS OFFLINE THREATS, UNKNOWN THREATS, BLENDED THREATS, EVASIONS



MITRE ATT&CK™ EVALUATION

MITRE ATT&CK™ EDR PRODUCT EVALUATION, 2018



ABOUT ENDGAME

Endgame makes military-grade endpoint protection as simple as anti-virus. Leveraging the industry's most advanced machine learning technology, Endgame enables security operators of any skill level to deliver full-force protection, stopping everything from ransomware, to phishing, and targeted attacks. Endgame is the only endpoint security platform to offer a unique hybrid architecture that delivers both cloud administration and data localization that meets all industry, regulatory, and global compliance requirements.

For more information, visit **www.endgame.com.**

@ENDGAME

ENDGAME