COMODO

WHITE PAPER

The State of Endpoint Protection: Promises, Promises

The cybersecurity industry is in crisis. It seems like every week another new player appears, claiming they've come up with the elusive magic bullet to stop malware and breaches, finally making us immune to ransomware, phishing and APT attacks. "We're different," they claim, "because we use whitelisting, or sandboxing, or machine learning, or virtualization." Quite often, it's a combination of these approaches and strategies. Unfortunately, the stark and unforgiving truth is that despite a landscape saturated with promises and crowded with cybersecurity solution providers, there are roughly five times more breaches occurring today than there were ten years ago[1]. Put simply, cybercriminals are winning a decades-old arms race. Today's malware producers are more sophisticated and well funded than ever, but so too are the cybersecurity "innovators" and the defensive solutions they've developed, ostensibly to counter and nullify them. The money being spent on cybersecurity protection is staggering -- $75 billion in 2015 alone with projections reaching $170 billion by 2020[2]. Yet, despite the increased investment and effort to thwart them, cybercriminals still have the upper hand. More companies are being breached today, many of them repeatedly, than at any time in history.

> While many providers still make bold claims to stop malware and ransomware in their tracks, an increasing number have basically conceded defeat and have pivoted from 'protection and prevention' straight to 'detection and remediation.

According to the most recent Verizon Data Breach Incident Report, last year, 39% of successful crimeware incidents involved ransomware. 93% of data breaches took place in minutes, while 83% of those breaches' victims took more than a week, usually several, to detect those breaches – and, to add insult to injury, they were usually discovered by sources outside of the organization[3]. Meanwhile, the Ponemon 2016 Cost of a Data Breach Report, sponsored by IBM, pegs the *average* cost of a breach right around $4 million, not counting the considerable damage to brand and consumer trust[4].

On balance, traditional endpoint protection as we know it today is a failure, and expensive and new, so-called advanced products are only providing incremental value. Gartner reports that, "44% of reference customers for EPP solutions have been successfully compromised[5]." Think about this for a moment: that's almost half of all cybersecurity customers, despite collectively spending billions of dollars to protect themselves, who are still getting breached. If your home security system failed you roughly 50% of the time a burglar tried to break into your house, your security company would be out of business in less than a New York Minute.

Clearly, what this tells us is that the conventional wisdom – organizations deploying conventional solutions – simply isn't working. Why? The main problem stems from the fact that, despite all the promises and fancy terms, historically there have really only been two basic cybersecurity postures to choose from: **Default Allow** and **Default Deny**.

Default Allow

In a **Default Allow** approach, known bad files (those on the blacklist) are blocked while known good files (those on the whitelist) are allowed to run on your endpoints. While this is good for productivity and usability (until your network gets infected, anyway) it's generally disastrous for security. Why? Because in Default Allow, *all unknown files are assumed to be good files and thus are also allowed through to run on the endpoint.* In a simpler, more innocent time, this made a fair amount of sense, as there weren't nearly as many malicious files being created, and there was far more time to respond to each attack. The problem is that it's now 2016, and there are literally **almost a million malware variants being created EACH DAY**, and all of them start out as an *unknown file*, and as such, they won't initially be found on any vendor lists – until they make some organization Patient Zero. Gartner estimates that "signature based malware engines are only 30% accurate at detecting new threats[6]," so if you're still operating a Default Allow model – and most businesses still are – you're allowing a huge number of unknown files, including malware, to enter your environment every day. Worse, the malware is essentially invisible and free to do whatever damage it's been designed to do until detected. This is such a fundamental point that it bears repeating:

With Default Allow platforms, and with all malware starting out as an unknown file, you're not only asking, *you're practically begging to become Patient Zero* and compromise your business, your brand, your reputation and your bottom line.

Somehow, Default Allow continues to be the industry norm. But in point of fact, no one really wants a Default Allow system protecting their environment. Who would? It's simply no longer able to do the job it's supposed to do, which is to protect you from malware, both new and old, known and unknown.

Clearly, this is an untenable solution.

We've solved the malware problem, once and for all. Comodo's award-winning **Advanced Endpoint Protection (AEP)** is the perfect solution in a world where everything is an endpoint.

Traditional Default Deny

Over the years, a few companies have bucked the **Default Allow** trend and introduced **Default Deny** platforms, also known as whitelisting.

These solutions take a sharply restrictive approach, *allowing ONLY known good applications and executables into the environment, while DENYING or blocking EVERYTHING else.*

And while this approach will generally keep you safe, doing a reasonably good job of blocking the known bad, *it also blocks all of the unknown good as well!* This will cause your productivity to all but stop, as your employees won't be able to download any new unknown files or software. In traditional Default Deny models, usability is reduced to dismal levels. Again, if you can **only** use known good files, that generally rules out all new types of software and/or new iterations of known software being released. This works quite well if you're in a nuclear sub on a machine that has one job and that isn't being used for anything else – to launch the missiles in case of nuclear war, for example. But in virtually every other business environment, with traditional Default Deny, the hit to productivity is simply too large.

The UNKNOWN problem

In each of the security postures discussed above, we understand which are the known good files and which are the known bad files. It's always the unknown files that continue to haunt the industry. Whatever the method: blacklisting, signature generation, machine learning, dynamic analysis, remarkably, they all still allow for infection by unknown malicious files. When you take a hard look at all of the complex methods used to identify malicious files, the sad result is that in the end, despite all of the fancy technology, these malicious unknown files will still slip past these expensive but ineffective defenses. The only way to provide a true malware free environment is to prevent all unknown files file from running unfettered.

True Default Deny – Default Deny Without Compromise

This is where **Comodo's True Default Deny** shines.

Like Default Allow and traditional Default Deny, *all known good* files and executables are automatically allowed to run unfettered on your organization's endpoints, while *all known bad* files and executables are denied from entering your environment and thus from running on your endpoints.

The big difference from **the rest of the industry** is in how Comodo's **True Default Deny Platform** handles *all unknown* files, processes and executables.

Comodo automatically wraps all unknowns in a protective 'wrapper' and allows them to run in what is essentially a very modern jail -- a very lightweight but very robust container where they're allowed to run safely, without any risk of infecting your endpoints or environment. This keeps workers happy and productivity high. And, if the contained unknown *does* turn out to be malware, it can't infect your endpoint, or compromise your environment in any way.

> With **Default Allow** platforms, and with all malware starting out as an unknown file, you're not only asking, you're practically begging to become **Patient Zero** and compromise your business, your brand, your reputation and your bottom line.

And how does Comodo ascertain whether the unknown is good or bad?

The answer is exceptionally efficiently. While the unknown file or executable is jailed in Automatic Containment, Comodo's VirusScope (on the local level) and Valkyrie (in the cloud), using a combination of static, dynamic and human analysis (if needed), will render a blisteringly fast verdict on whether the contained unknown is good or bad, 100% of the time. If judged good, the file or executable is added to the whitelist and allowed out of containment. If bad, it's added to Comodo's blacklist and deleted from the environment. Typically, Comodo delivers a verdict in only 45 seconds – roughly 5-10 times faster than our closest competitors.

And what of Sandboxing and Virtual machines? Isn't Comodo doing basically the same thing?

The answer is no.

Sandboxing is designed for research and analysis, not protection. Most Sandboxing is too resource-intensive and inefficient to actually use on a regular basis, as each environment needs to have a copy of the operating system running as part of its environment, and spinning up a number of virtual machines simply siphons off too much CPU compute power. By offloading sandboxing to a supporting role in the cloud, and

using a container on the endpoint, Comodo's Automated Containment can be exceptionally lightweight, phenomenally fast, and provide much better protection than traditional sandboxing approaches. In contrast to heavy 'micro-visors' and sandboxes needing gigs of RAM, the Comodo Client takes up just 10 megs of RAM and costs you virtually nothing from a CPU perspective.

A Prevention Solution That Actually…Prevents Infection

While many providers still make bold claims to stop malware and ransomware in their tracks, an increasing number have basically conceded defeat and have pivoted from 'protection and prevention' straight to 'detection and remediation.' Things have gotten so bad that many of the industry's key players, despite their stated claims to the contrary, have given up even the *pretense* of protection and prevention. This has spawned an entire 'endpoint detect and response,' or 'EDR' sub-industry. Having failed initially to protect you, they instead have come up with several new talking points detailing how they'll clean up the mess that they've allowed to happen in your environment. Their focus increasingly is on more of a reactionary role -- detecting, reporting and responding to breaches that they failed to prevent, instead of doing the job of protecting you against such attacks**.** It's important to have both prevention and detection of course, as many breaches will continue to be caused by human error, or successful phishing scams, for at least the time being, but with prevention rates so low, today's remediation teams are having a difficult time responding to and managing so many "EDR" events. Why not block the attacks like you're supposed to be doing in the first place rather than throwing in the proverbial towel and defaulting to "cleanup mode?"

How Comodo Enables True Default Deny

At Comodo, we're tacking hard in the other direction. Far from throwing in the towel, we're confident that we've done what others just promise: we've solved the malware problem, once and for all. Comodo's award-winning Advanced Endpoint Protection (AEP) is the perfect solution in a world where everything is an endpoint – laptops, desktops, servers, tablets, phablets and, of course, smartphones. Comodo's AEP tightly integrates IT and security management and unifies compliance and security policies across all the OS platforms you are charged with protecting. The IT and Security Management (ITSM) console features seamless integration between your IT and security management buckets. ITSM has many outstanding features including remote employee endpoint monitoring and management, malware hunting, and global visibility of an employee's entire digital footprint. If an employee's device is infected, it's very likely that one of their others will be too. If a breach does happen to occur on an individual's laptop, for example, ITSM automatically correlates their other devices so remediation efforts are comprehensive.

Comodo AEP provides unified management, including:

- Mobile Device and Application Management (MDM, MAM)
- Remote Monitoring and Management (RMM)
- OS and Application patches and updates
- Security Management

The Comodo Client combines advanced and traditional security by delivering Default Deny security with Default Allow productivity using a combination of:

- Application Control for known good intelligence
- Integrated Threat Intelligence to block locally and globally known bad
- Automated Containment of all unknowns so they can't infect you if they are malware

- Closing the threat exposure window – no exposure, no infections
- Completely preventing all 'Patient Zero' scenarios
- Delivering 100% of verdicts to convert all unknowns into either known good or bad
- Not just another layered-on tool but a complete solution for full AV compliance

Other providers talk about it, but Comodo actually secures you by incorporating best of breed technologies into one highly integrated solution featuring:

- Application Control
- Integrated Threat Intelligence
- Automated Containment
- Machine Learning (VirusScope)
- Cloud Integrated Sandboxing (Valkyrie)
- Host Intrusion Prevention System (HIPS)
- Host Firewall
- URL Filtering

Comodo's cybersecurity solutions combine a host of interlocking technologies including our unique, patent-pending secure but lightweight automatic containment solution. And Comodo doesn't perpetually contain unknown files and executables, but assesses them exceptionally quickly and releases them from containment (and adds them to the whitelist) if judged good and deletes them from the system (and adds them to the blacklist) if judged bad. In addition, Comodo's unique containment system:

- Only contains unknown portable executable ('PE'), not your office files, increasing usability and productivity
- Restricts sandboxing analysis to the PE, so unlike other vendors' solutions, your sensitive data is never at risk
- Utilizes Comodo's proprietary Valkyrie File Analysis Platform which:
    - Accelerates the verdict process
    - Uses static, dynamic and expert human analysis (if needed)
    - Detects zero day, unknown and APT threats
    - Delivers a verdict in roughly 45 seconds. This reduces containment time, further increasing endpoint performance and usability

Comodo Advanced Endpoint Protection is integrated seamlessly into the Comodo 360 Security Platform featuring:

- **Comodo Dome** – Providing unparalleled protection at the boundary
- **Comodo cWatch** – Providing advanced breach detection and prevention
- **Comodo AEP** – Providing unmatched protection at the endpoint

Unlike our competitors, Comodo is actually doing what we say we'll do – protecting you, your network and your endpoints from malware and ransomware by blocking all known bad files and all unknown files from entering your environment and running unfettered on your endpoints. We don't just talk about it, we prevent breaches and infections, 24x7x365.

COMODO

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals, to mid-sized companies, to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in New Jersey and branch offices in Silicon Valley, Comodo has 12 international offices across Europe and Asia.

[1] Digital Guardian, "The History of Data Breaches," June 27, 2016
[2] Forbes.com, "Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020," December 20, 2015
[3] Verizon 2016 Data Breach Investigations Report Executive Summary
[4] Ponemon 2016 Cost of Data Breach Report, sponsored by IBM Security
[5] Gartner Research Inc., TRUE Default Deny and the end of Patient Zero
[6] Gartner Research Inc., TRUE Default Deny and the end of Patient Zero