panda
a WatchGuard brand

Know Your Security Model: Traditional vs. Contextual Protection

Introduction

Traditional Security Protection

Contextual (Next-Gen) Protection

Panda's Protection Model

Table of Contents

Introduction

03

The Generation Gap

In technology, buzzwords come and go, but one of the more common terms in security these days is "next-generation (or next-gen) endpoint protection." But what does that really mean? Solutions from all origins are now deemed "next-gen" with seemingly little basis for comparison. Is it nothing more than spin, or is there something fundamentally different about these solutions that separate them from the pack?

In this case, where there's smoke, there is fire as well. Next-generation endpoint protection represents a fundamental shift in the underlying protection model that the solution relies upon. It's more technically advanced, more adaptive and more capable of detecting threats, no matter the shape they take. It's not only capable of stopping known threats, but also new attacks that have never been seen before.

That's a stark contrast to a traditional protection model, which can only block files that it has seen before. Some traditional protection is very effective at this function, but in today's threat landscape, it's just too narrow a field of view to effectively protect against the evolved malware, ransomware, fileless attacks, living-off-the-land attacks and more that plague systems.

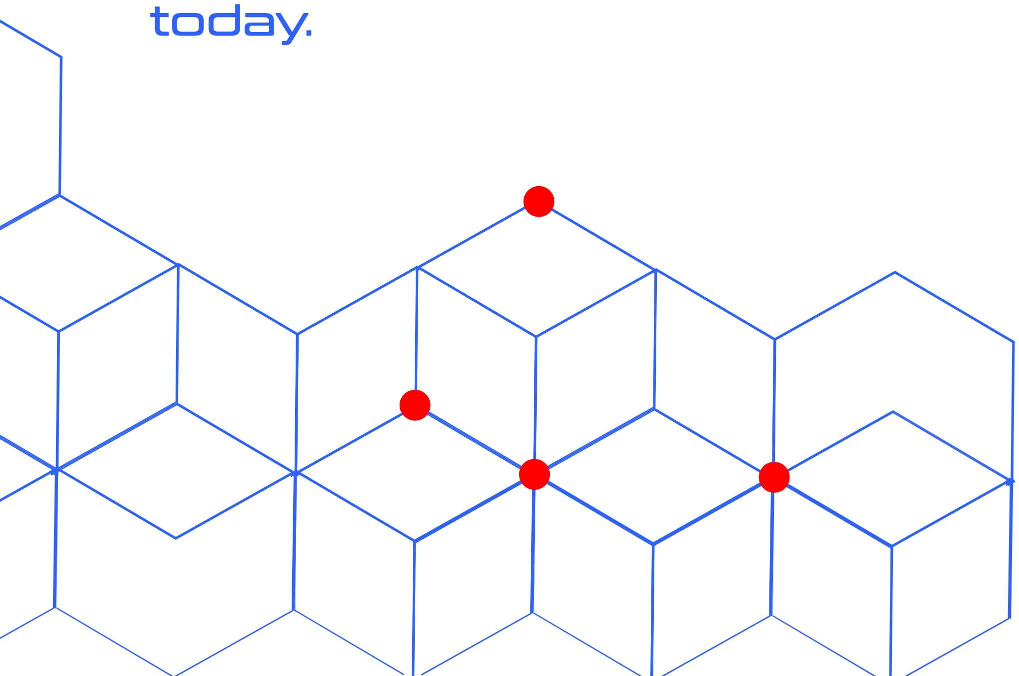
When it comes down to it, "next-gen" is a misnomer. Next-generation endpoint security is more like **now-gen**: the right technology and tools to face the threats of today. Traditional protection alone is no longer enough to be considered comprehensive security, even for small- to medium-sized businesses. This has created a dynamic scenario; instead of tradition protection being replaced, it has has come to stand side-by-side with next-gen technology, which has become the new standard for endpoint cybersecurity. This amalgam has become an effective partnership, a merging of old and new technologies to provide greater security. The sum is indeed greater than its respective parts in this case.

However, not all next-generation endpoint security is created equal; while the missions may be similar, the technology, methodology and execution of these solutions can differ wildly, creating plenty of confusion in the market as to the efficacy and validity of the solutions.

This eBook will cut through the fog that surrounds the term "next-gen endpoint security," exploring the differences between traditional and next-generation cybersecurity protection models, and how Panda's unique protection model employs the best of both to be an industry leading solution.

Next-generation endpoint security is more like now-gen: the right technology and tools to face the threats of today.

04



Traditional Endpoint Security

By definition, security is defensive; a method to defend and protect something of value, a preventative measure to repel attacks that are anticipated in the future. It's something that lies in wait, prepared for what may or may not come.

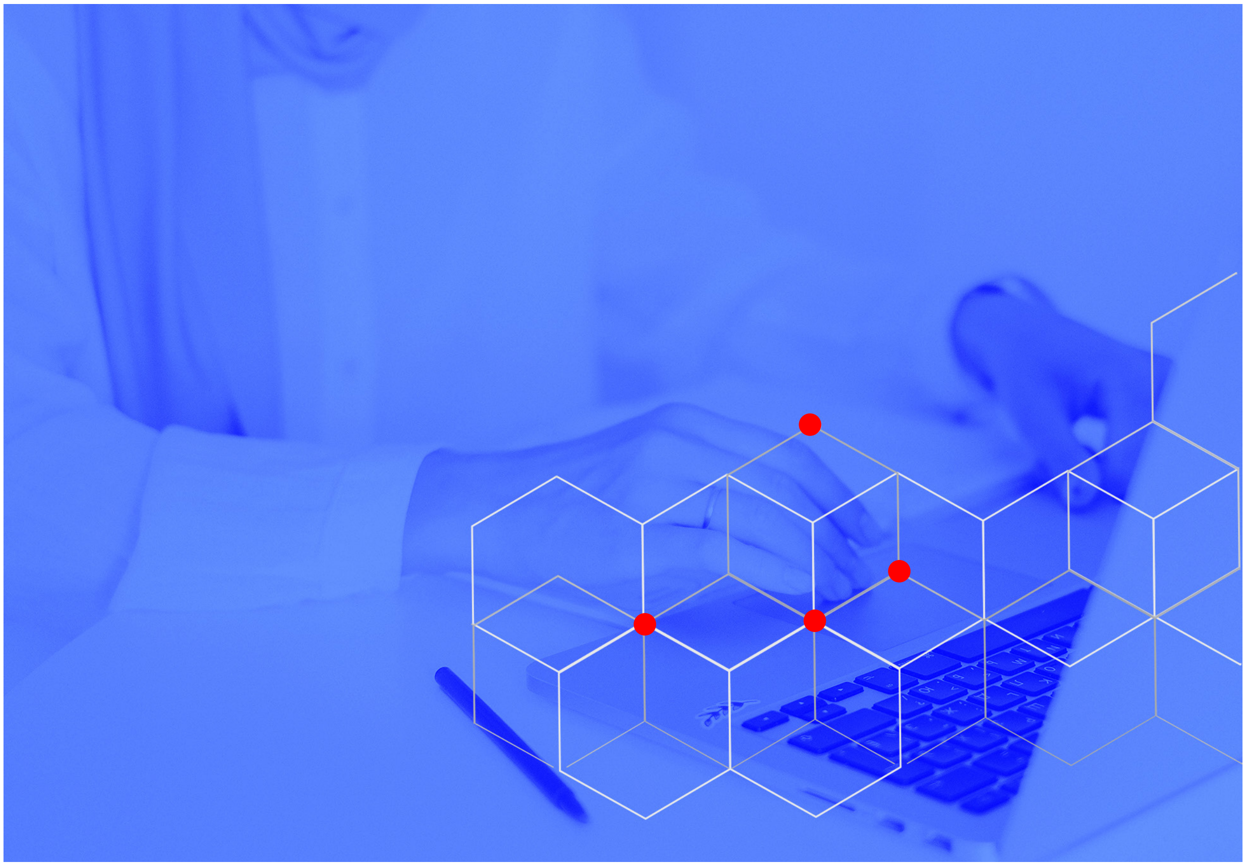
Security, therefore, is a reactive process. It's triggered only when there's a known threat that needs to be defended against, and it's only effective if it has prepared for the specific threat that it's facing. So-called sneak attacks can easily slip past undetected.

Traditional endpoint security is based on this framework. It was created to repel viruses and other threats that were transmitted via specific code. Threats were discovered based on previous successful attacks and were forensically analyzed to create a signature file that can recognize that code to stop future attacks. It was a method that worked well for a long time (well, except for the first people to encounter a new attack), and it became very efficient and effective.

Even today, traditional file-based protection has its place in stopping known attacks or slight variations of those attacks. But the threat landscape has evolved considerably since the inception of traditional endpoint security. Today, traditional protection can be defeated in numerous ways:

- A new malicious file never seen by a traditional security solution.
- An adversary that's determined enough, employing tactics consistent with an advanced persistent threat.
- A file not classified as malware that runs despite any of the malicious actions it carries out.
- A fileless attack that uses exploits in "safe" running processes to inject malicious code and carry out malicious behavior.
- And more.

05



06

Clearly, since the inception of traditional endpoint security, there has been an escalating arms race in cybersecurity. On one side are the cybersecurity experts, constantly improving technologies to detect, respond and hunt for threats, taking the fight to the criminals in a much more proactive way than ever before. On the other side are the cyber criminals, who don't sit on their laurels; they are constantly researching new protections and security solutions, understanding them on a fundamental level so as to subvert them. And, while they gain more knowledge through every successful incursion into an endpoint, IT professionals using traditional protection gain no insight into the nature of the attack nor the state of applications or processes running on the system.

Hacking is no longer the domain of the single bad actor in a hooded sweatshirt seeking to cause chaos; it is professionalized, sophisticated and organized, capable of extending its reach past traditional endpoint security with ease and able to inflict greater damage than ever before. Without a doubt, and by no flaw in its design, traditional endpoint protection is no longer sufficient to withstand the onslaught of today's advanced threats—threats that demand security just as modern, adaptive and sophisticated as they are.

Contextual (Next-Gen) Endpoint Security

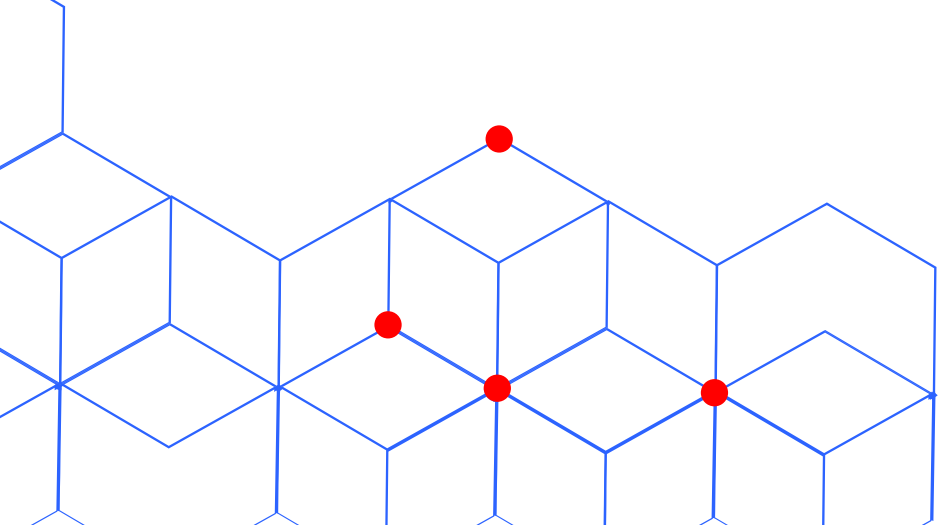
If traditional endpoint security is a straight road, then next-gen, or contextual, endpoint security is a multi-lane highway. Far from the signature-file approach, next-gen protection employs numerous technologies to detect and respond to threats of all kinds, based on analyses of contextual, behavior-based events.

Unlike traditional protection, which only reacts when a known malicious file is detected, a next-generation solution provides continuous protection against all types of attacks. This amounts to nonstop prevention, detection at runtime, visibility into every action taken, and intelligence to block malicious actions such as lateral movements. Effectively, next-gen solutions are designed to protect systems before, during and after any attack.

Along with this evolution in technology is a shift in methodology: a turn to what's known as zero-trust security—a philosophy in cybersecurity that, instead of only searching for specific malicious activity, assumes all files, applications and processes are vulnerable until they can be vetted. Unlike traditional protection, which blocks nothing but what it knows to be malicious, next-gen protection blocks all applications and processes that are unknown from running, while also monitoring the behavior of all known and classified applications to ensure nothing is acting suspiciously. It's a more holistic and complete view of what is actually occurring on every endpoint, and, through the use of AI-based techniques, can lead to new insights and understandings of how threats are attempting to attack and gain control of systems.

Next-gen protection employs numerous technologies to detect and respond to threats of all kinds, based on analyses of contextual, behavior-based events.

07



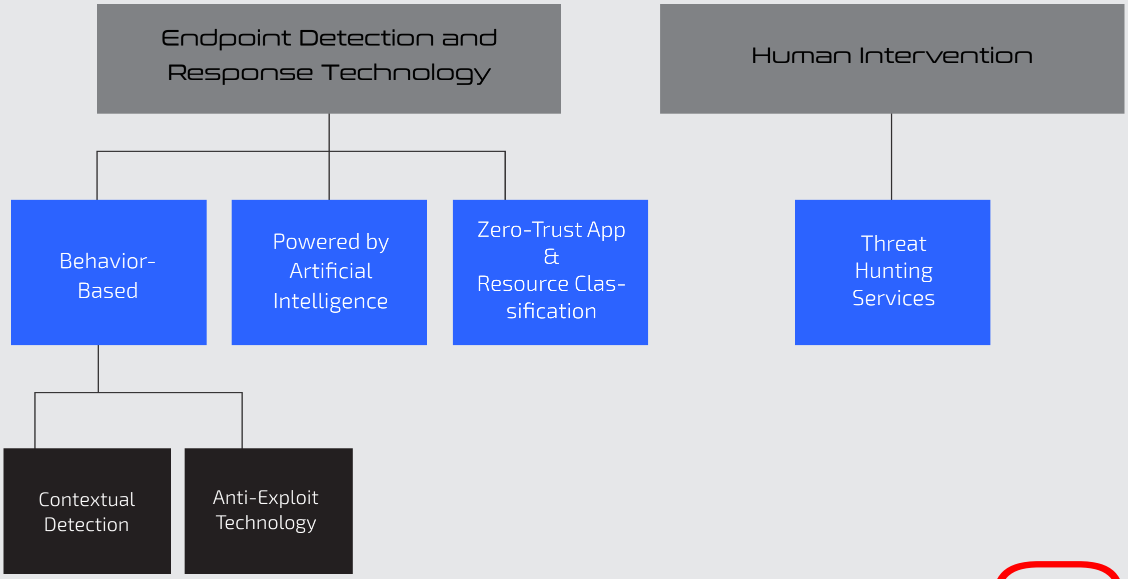
Market Confusion

While next-gen endpoint security is the next evolution in cybersecurity protection, it is also a term that has not coalesced around a specific standard or requirement. Many solutions are now dubbing themselves as "next-gen" in the cybersecurity space, with little uniformity surrounding their products.

Some are bloated with settings and features that don't make much of an impact. Others are overly complicated, demanding dedicated resources to manage them despite the fact that many IT departments don't have those resources available, due to an ever-widening cybersecurity skills gap, high labor costs, and a lack of qualified candidates and operations that rely on 100% staff utilization to be profitable. Still others use buzz words to sound current and trendy, leaving out the specifics on how they use concepts like AI, deep learning, etc.

When evaluating next-gen endpoint security, it's important to thoroughly review the underlying technology that's powering the solution. A strong next-gen solution will utilize multiple technology layers that work in tandem with one another, designed to not only to block existing threats, but to anticipate new ones, monitor suspicious behaviors, and hunt threats before they attack. There should be a strong focus on automation, typically powered by AI-backed technology, which makes detection lightning fast and removes the need for manual classification of threats, applications, processes and more.

Next-Gen Endpoint Security—The Basics


Endpoint Detection and Response Technology
Human Intervention
Behavior-Based
Powered by Artificial Intelligence
Zero-Trust App & Resource Classification
Threat Hunting Services
Contextual Detection
Anti-Exploit Technology

Side By Side

At this point, it might seem like the choice between traditional protection and next-gen protection is a clean-cut, either/or decision. Next-gen endpoint security clearly offers advanced protections for advanced threats, so it may seem that traditional protection is obsolete.

That couldn't be farther from the truth. Next-generation endpoint protection relies on multiple layers of technology rolled into one solution to be as comprehensive as possible, and traditional protection is typically folded in as one of these layers. Because traditional endpoint protection is mature and effective technology, it is still viable—as part of a larger strategic solution. It cannot be relied upon on its own but will commonly be found as a component of next-gen endpoint security.

Evaluating Next-Gen Endpoint Protection— Common Questions

“How long has your EDR technology been on the market?”

“How does it learn and adapt to new threats?”

“Is malicious code allowed to execute before it is detected?”

“To what extent are signature files and heuristic scanners part of your solution?”

“How is artificial intelligence applied to your solution, specifically, and how does it enhance the overall security posture of an endpoint?”

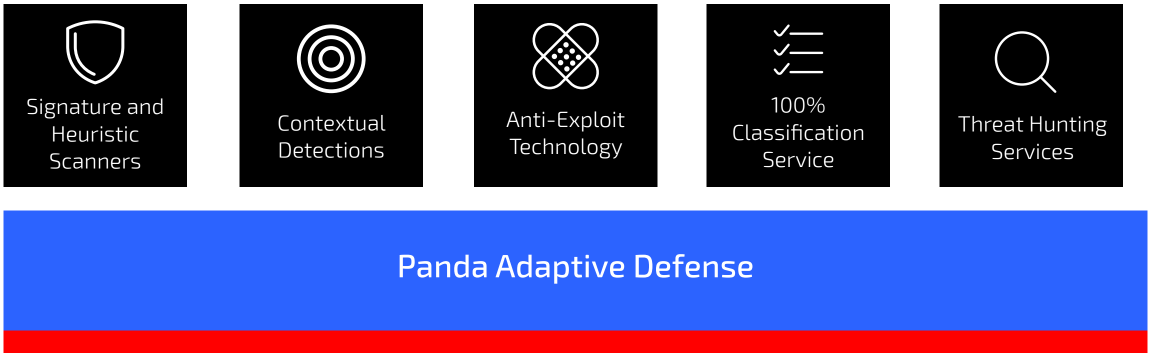
“Do you have a service validating all running applications as part of your solution?”

“Is Threat Hunting a core component of your solution?”

How is the management of the platform delegated? Does it require dedicated resources?”

Panda's Protection Model

Panda Adaptive Defense is an industry leading, next-generation endpoint security solution, comprised of multiple layers of endpoint protection (EPP) and endpoint detect and response (EDR) technology that work concurrently to defend against and remediate cyberattacks. Using the most effective traditional endpoint protection technology combined with multiple next-gen endpoint detection and response technologies, it offers comprehensive protection for all endpoints, along with complete visibility into the entire network and an easy-to-use dashboard that minimizes labor-intensive tasks.



Adaptive Defense Technology Layers

Signature Files and Heuristic Scanners

Known as traditional endpoint protection, this antivirus (AV) technology layer is proven effective against many common, low-level threats. It's optimized to detect known attacks, based on specific signatures, generic and heuristic detection and malicious URL blocking.

Contextual Detection

Essential for detecting malware-less and fileless attacks, contextual detection looks for abnormal or unusual resource and application utilization. And, with the complete visibility that Adaptive Defense provides, Panda's contextual detection technology is constantly learning, improving and adapting to new threats and techniques. It is very effective against script-based attacks; attacks using goodware operating system tools such as PowerShell, WMI, etc.; web browser vulnerabilities and other commonly targeted applications such as Java, Adobe Reader, Adobe Flash, Microsoft Office and more.

Anti-Exploit Technology

Complementing Panda's contextual detection technology, anti-exploit technology specifically detects fileless attacks that are designed to exploit vulnerabilities. It searches for and detects anomalous behavior—a surefire signal of exploited processes. Anti-exploit technology is important on all endpoints, but mission-critical on unpatched/waiting-to-be-patched endpoints, and on endpoints with operating systems that are no longer supported.

100% Classification Service

Some endpoint detection and response solutions identify malware, but offer nothing else, which introduces risk. With the addition of a unique 100% classification service as a core component of Panda Adaptive Defense, it monitors all processes and applications before, during and after execution. The only technology of its kind available, this mature EDR technology (more than five years in operation) means that there are no "suspicious" items to investigate—only processes that are known and classified as trusted by Panda are allowed to run. Panda's 100% classification service is unique managed service that provides maximum protection without having to delegate important cybersecurity decisions to end users. And, it offers superior protection should a previous layer be breached, because it stops attacks on already-infected computers and lateral-movement attacks inside a network. The AI-based approach of this service ensures 99.98% of applications are automatically classified, leaving only the remaining 0.02% to be reviewed and classified by experts at Panda's laboratory.

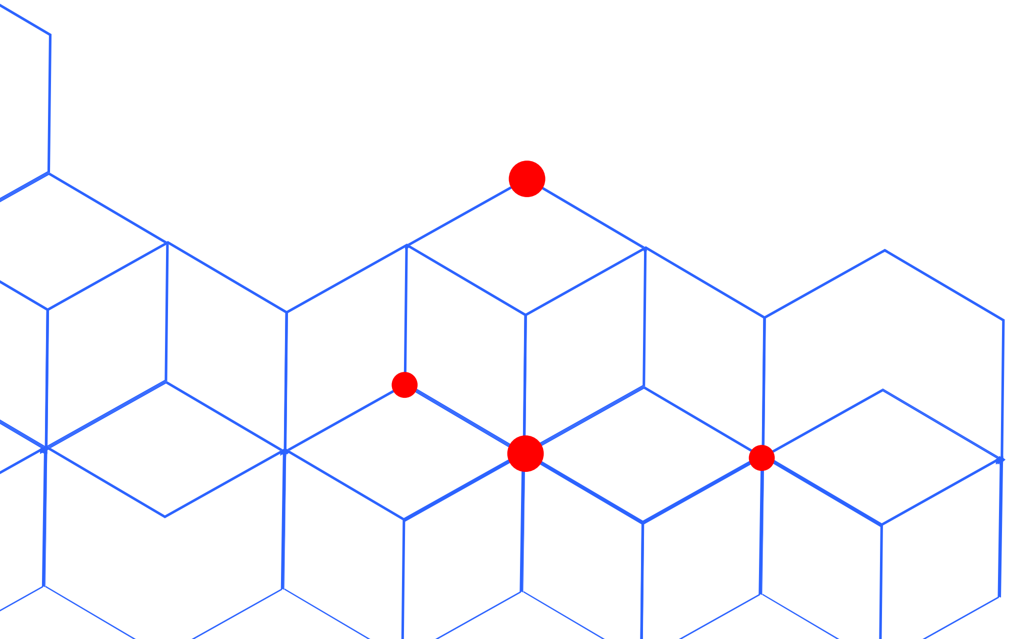
Threat Hunting & Investigation Service

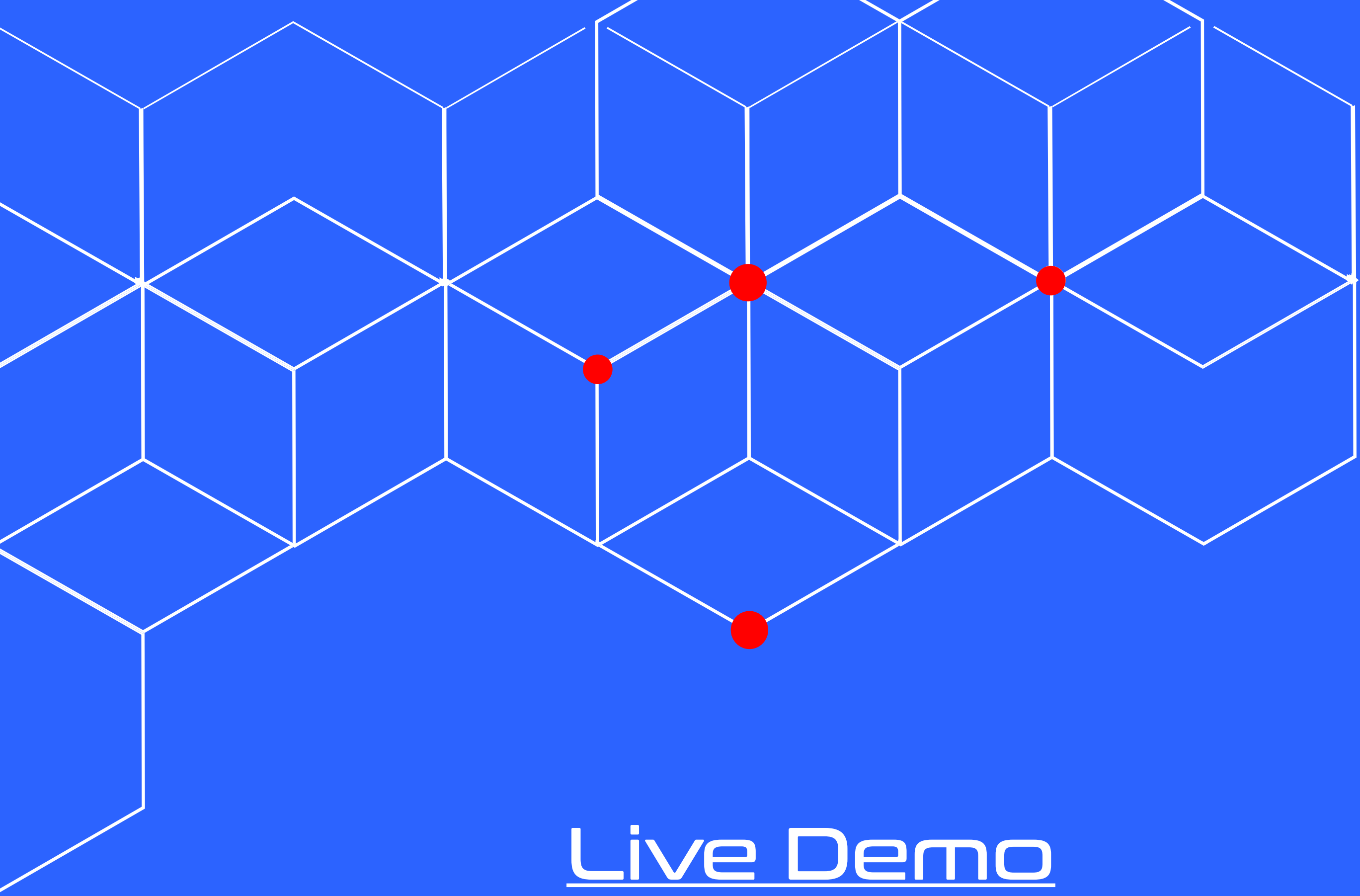
The only technology of its kind that's included as a core component of an EDR solution, Panda's Threat Hunting & Investigation Service (THIS) is an advanced, proactive service that detects compromised machines, early-stage attacks, and suspicious activities. When all else fails against extremely sophisticated attacks—ones that often can go undetected for months—threat hunting roots them out using a set of proactive procedures. Managed by Panda's global cybersecurity experts experts, the Threat Hunting & Investigative Service can find even the slightest of traces left by hackers that are attempting to take control of endpoints through living-off-the-land (LOTL) techniques. It's a massive value not only in terms of technology, but also for the bottom line of IT professionals. This managed service frees admins from the time consuming and difficult task of searching for threats, leaving the daily management and decision-making in the capable and trusted hands of Panda's expert threat hunting team.

Conclusion

The future of cybersecurity lies not in a magic bullet, one-size fits all approach to technology. As cyber threats have evolved in complexity and severity over the last decade, the security solutions that fight them have responded by rising to the challenge of keeping endpoints safe across the globe. This escalation, which has given rise to next-generation endpoint security, continues to this day, with the tools currently in place to meet the needs of years to come.

But just as every fortress needs its foundation, effective cybersecurity technology is not easily discarded, which is why traditional protection has not gone extinct, but merely folded into the larger perimeter of next-generation endpoint security. And, as threats and security technology continue to advance, that perimeter will only grow larger to encompass further generations of cybersecurity technology to keep IT systems safe. However, more technology and larger solutions often mean more unwieldy and complicated dashboards, configurations and deployments. It's important to seek out only those solutions that are capable of seamlessly and simply integrating multiple technologies into one next-gen solution, while simultaneously alleviating the pressures of staffing and labor resources for every team that uses it. Only then will IT professionals be fully prepared for the threats to come.





Live Demo

Contact Us

More info at:

pandasecurity.com/usa/business

Let's talk:

63.2.8352.8250

sales@ph.pandasecurity.com

www.watchguard.com | pandasecurity.com/business

WatchGuard®