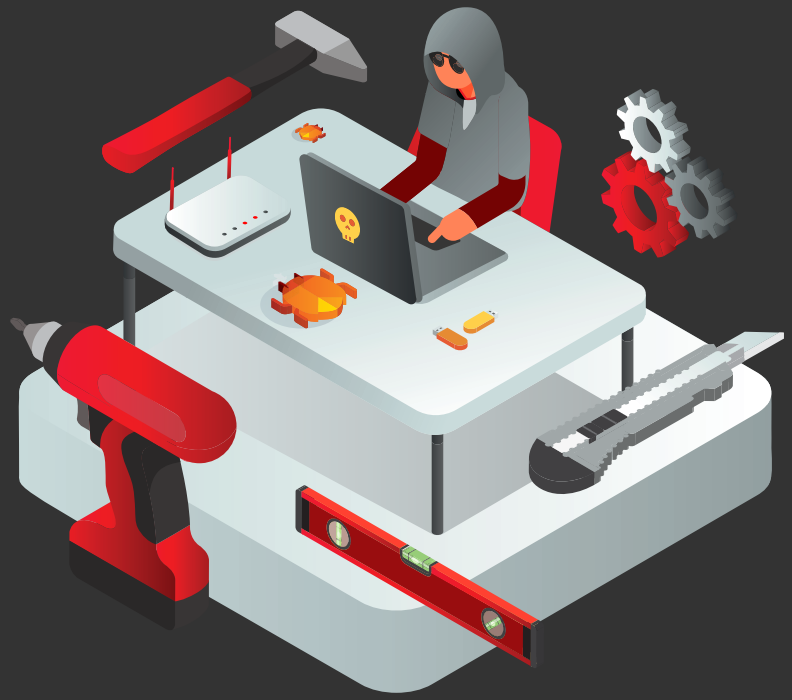
Advanced Endpoint Security

TAKING A PROACTIVE POSITION WITH YOUR CYBERSECURITY

Your Threat Hunting simplified with WatchGuard

Index



WatchGuard

Your Threat Hunting service program simplified with WatchGuard

Propagation

When it comes to security, nothing is a hundred percent.

What we know is that no organization is immune regardless of where they are located, the size, or the vertical in which they operate.

- As adversaries continue to mature their tradecraft, augmenting technology-based controls with human expertise have never before been more important.
- The tempo of adversary activities also increases rapidly, and they're becoming increasingly adept at doing more with less.
- Many intrusions today involve fileless malware leveraging the continuously evolving living-off-the-land techniques in some stages of the attack.

What does this mean for the effectiveness of the security program of the organization?

Today's threat actors are well-organized, highly skilled, motivated, and focused on their targets. These adversaries could be lurking on your network or threatening to break into it, using increasingly sophisticated methods to reach their goal. Simply put, there's often no need for adversaries to deploy malware at the early stages of the attack. They usually have all the tools they need to get into the network and move laterally to instrumentalize the legitimate applications present in the endpoints.

In addition, the attacks can come from many different threat surfaces to exploit the many vulnerabilities that may be present across an organizations' network, endpoints, and people. Worst of all, organizations do not know by whom, when, where or how a well-planned attack will occur. Today, even advanced detection mechanisms struggle to anticipate how attack vectors will evolve.

This trend presents severe challenges for organizations' security programs. It underscores the importance of using a combination of technology-based control with human-led, proactive hunting service to ensure that the organization moves quicker than the speed of the threat, remaining well protected and resilient.

Attackers using **LotL** forage on target systems for tools, such as operating system components, misconfigurations, or installed software, they can use to achieve their goals. LotL attacks are classified as fileless malware because they do not leave any artifacts behind.

A living-off-the-land (LotL) attack describes a cyberattack in which hackers use legitimate software and functions available in the system to perform malicious actions.

WatchGuard

1. The function of Threat Hunting

Threat hunting is a niche function often misunderstood. Therefore, it's essential first to examine what we mean when we use the term threat hunting.

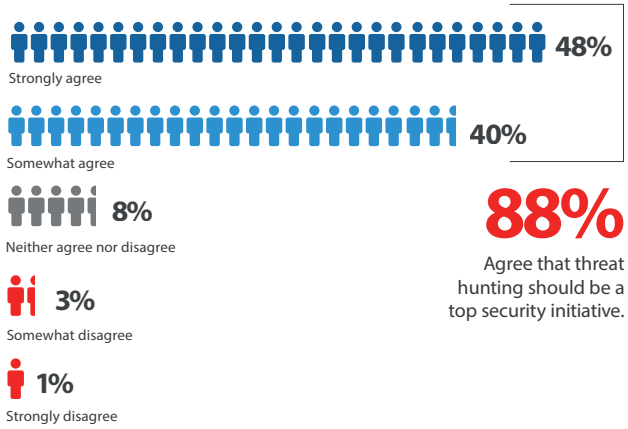
It can be defined as an analyst-centric process that enables organizations to uncover hidden, advanced threats missed by automated preventative and detective controls. In simple terms, the threat hunting mission is to find those unknown threats that manage to bypass technology-based controls.

Threat hunting is for addressing the last 1% of the unknown behaviors. It is not about finding malware and identifying abnormal activity. Technology is just the necessary starting point to proactively spot and stop threats in the cyber kill chain before the damage is done. Although threat hunting is not for finding malware, the hunting provided in the WatchGuard Advanced Endpoint Security solutions benefits the Zero-Trust Application Service by blocking any attacks when a malicious application tries to run, even if the abnormal behavior is not stopped.

Threat Hunting is a top security initiative

Although threat hunting is still an emerging discipline, there is significant interest in it according to the last Cybersecurity Insiders survey on the maturity of the threat hunting security practice.

According to Pulse, **32% of IT leaders say that their organizations plan to reinforce their endpoint security posture by adding a threat hunting program to their overall security strategy.**



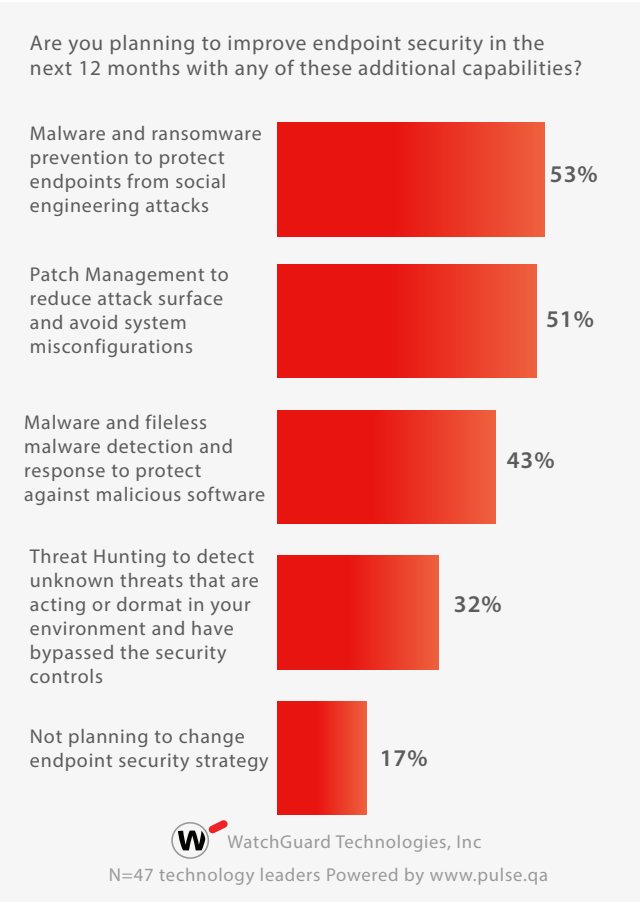


Figure 1. WatchGuard EDR and EPDR, combined with the Threat Hunting Service and Patch, provide you a single solution you can add to your mix of Managed Security Services to cover all additional capabilities planned in the next 12 months.

Threat hunting is a discipline that organizations need to stop thinking of not as a nice-to-have but as a must-have. It should be a continuous function, not a point in time, as it is essential in any robust cybersecurity program.

Where Threat Hunting function fits in your security program

Organizations have always relied on prevention and policy-based security controls. Today, organizations are flooded by advanced and targeted attacks. More advanced threats don't have any problem overpassing those security measures leaving the organizations unprotected with limited or no visibility into threat activity.

In addition to reducing the attack surface and reinforcing their prevention capabilities, security operations teams must adopt a proactive security approach.

They must implement a robust and complete threat protection life cycle, effectively detect threats in the network and endpoints, and respond accordingly to stop the breach before the damage is done and recover normality as soon as possible

This means a **shift in the security mindset from prevention and incident response to proactive and continuous response,** assuming the organizations are compromised and require continuous monitoring and remediation.

Every minute, users and endpoints used by those organizations produce valuable telemetry information about what's happening across the organization. The vast majority of that telemetry is related to legitimate day-to-day activity.

However, after being **analyzed by advanced security technologies like machine learning and behavioral analytics, abnormal behaviors are detected, triggering security signals.** This standard process based on automated abnormal behavior analytics requires specific technologies, processes, and analytics to be executed.

Threat hunting is a function that works in parallel with this workflow. Its core function is to use queries to the data lake and specific tooling to extract insights from the telemetry to automate new deterministic analytics. Additionally, threat hunting also comprises the combined activity of applying these new analytics to the telemetry and contextualizing weak signals to streamline the identification of actual attacks.

The function of threat hunting, when executed in real time, significantly reduces the time to respond to threats.

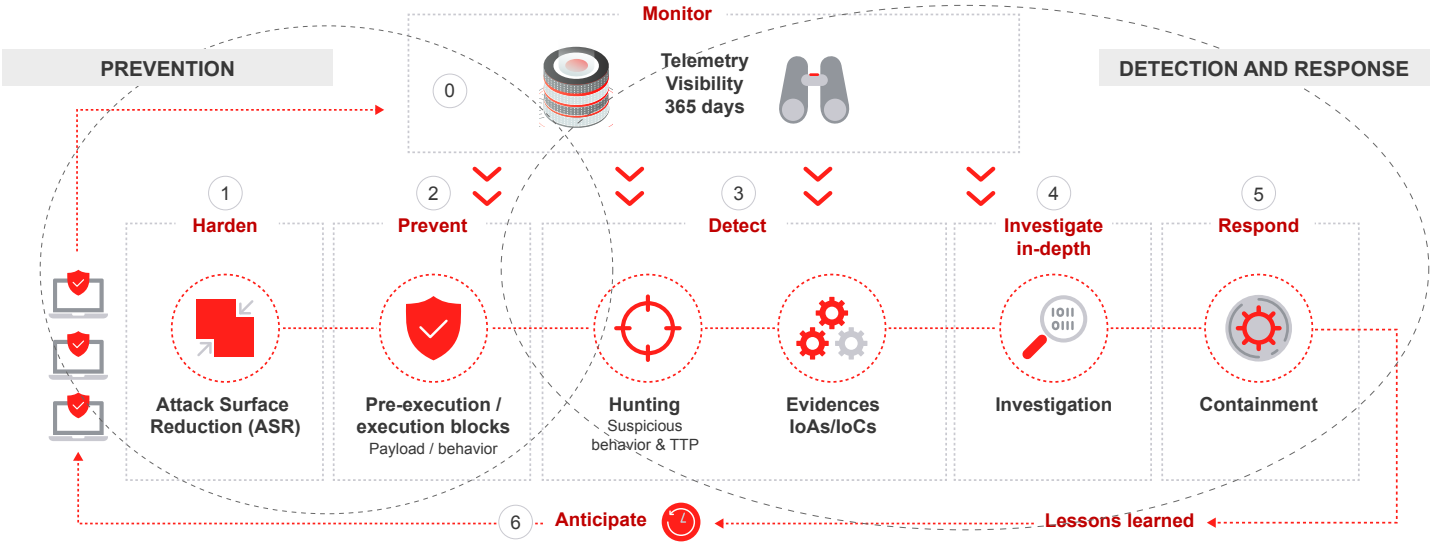


Figure 2. The threat protection life cycle that a robust security program must address

2.The Threat Hunting Operations

When it comes to discussing threat hunting operations, the activities behind them can broadly be grouped into one of three key buckets:

- The analytics-driven approach. Using statistical methods, the actual process of threat hunting often involves examining outliers and performing frequent analysis to detect something that hasn't been seen before or irregularities that might be malicious based on baseline data in the environment.
- The hypothesis-based approach tends to be where elite threat hunters have the opportunity to get creative and think like the adversary. It involves developing and testing theories about where and how a determined attacker might attempt to operate, move in the network, and living off the land, unseen until it decides it's the best time to attack.
- Finally, the intelligence-based approach is the most common operation, and it involves the use of up-to-the-minute threat intelligence to search historical data for signals of intrusions. Today, many organizations tend to integrate this approach by themselves, using a collection of known IoCs, like IP addresses or hashes.

Using threat intelligence for threat hunting should not be limited to IoCs. More critical to threat hunters is a type of threat intelligence called tools, techniques, and procedures (TTP). TTPs can be defined as "patterns of activities or methods associated with a specific threat or group of threats.

TTPs are much more difficult for an attacker to alter when compared to IoCs. Adversaries reuse their TTP across attacks while changing the binaries or command and control (C&C) infrastructure. For example, changing a C&C IP address is trivial. However, changing the communication protocol being used is much more challenging because it requires a lot of programming effort. The MITRE ATT&CK framework attempts to map these TTPs into something usable.

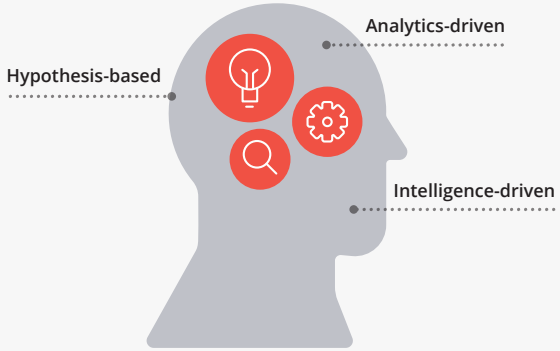


Figure 3. WatchGuard Threat Hunters and Analysts continuously monitor everything that happens in real time and retrospectively (365 days) in all our customers' telemetry. Continuous real time monitoring, technologies, and human-led proactive hunting service enables discovery of hackers and malicious employees, leveraging LotL techniques..

3.Value of the Threat Hunting

Some of the value threat hunting provides to organizations are:

Allows for the timely discovery and disruption of internal and external threats that have bypassed technology-based controls before a breach.

It augments existing technology-based controls with human layer expertise.

Augments security technologies with human expertise to reduce the dwell time.

Hunting leverages that human experience to see and stop advanced attacks that might otherwise linger unseen for days, weeks, or even months. It shortens the dwell time, and it's really the key to reliably stopping breaches.

Arms security teams with insights required to disrupt adversaries at scale

While hunting operations occur at the first stage, finding those unknown threats is still only half the battle. When it is performed effectively, a highly structured threat hunting program arms the security teams with the insights they need to disrupt threats.

Feeds the continuous effort of reducing the attack surface and improving automated detection capabilities.

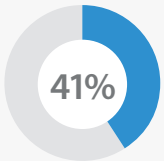
New patterns must be leveraged to improve detection capabilities leaving threats with nowhere to hide.

What are the primary goals of your organization's threat hunting program?[1]

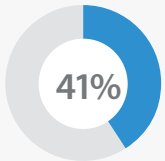
51% Reduce exposure to internal threats

45% Reduce number of breaches and infections

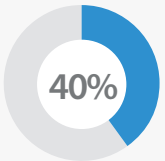
43% Reduce attack surface



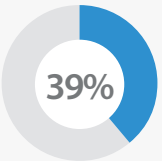
Reduce time to containment (prevent spread)



Reduce exposure to external threats



Improve speed and accuracy of threat response



Reduce dwell time from infection to detection

4. Barriers to a successful threat hunting program

Establishing a threat hunting program in-house comes with its challenges. The issue that appears most clearly prevalent is the challenge of finding skilled staff and the ability to train current staff.

Having skilled and knowledgeable staff allows an organization to better select tools and technology and better define processes required to perform a threat hunting program. The main challenges when attempting to implement their hunting efforts are summarized in the following:

1. Lack of human expertise dedicated to threat hunting

Decisions on what and how to automate analytics for proactively detecting and guiding input and questions can be only led by experienced threat hunters. These questions don't remain static against an ever-changing threat and need to be constantly evolved by expert hunters. This means embedding continuous threat hunting into your daily security workflows.

Many organizations attempt to add this threat hunting task as an additional responsibility of security analysts that are already juggling an expansive collection of daily tasking. Therefore, hunting activities are performed as time allows and often lack the required structure necessary to define, execute and apply the learnings and observations.

WatchGuard's threat hunting service brings elite-level expertise in threat hunting and extend the existing security team capabilities.

2. Lack of structured workflows to speed up the processing

Structured workflows and consistency are fundamental keys to success in the hunting efforts for organizations today.

Taking an ad-hoc or unstructured approach to hunting operations inhibits the chances of success against well-resourced and well-organized threats.

WatchGuard's Threat Hunting process follows a well-structured hunting methodology to make the most of the valuable and long-term telemetry (365 days). It covers the tools and workflows necessary to enrich and search in the telemetry for unseen threats while having the technologies and processes to ensure that hunting discoveries are leveraged to improve automated detection capabilities and provide immediate insights to mitigate threats and reduce the attack surface.

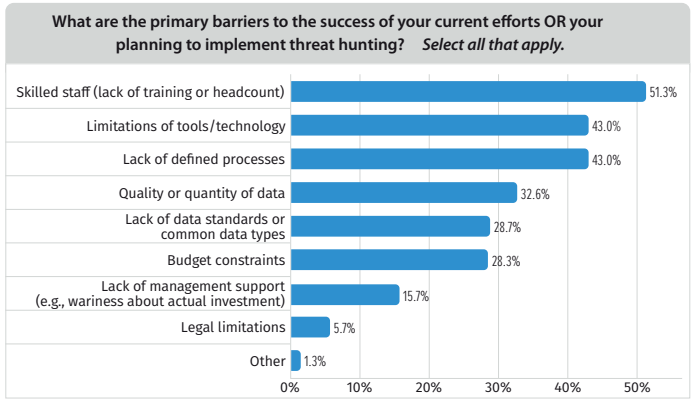
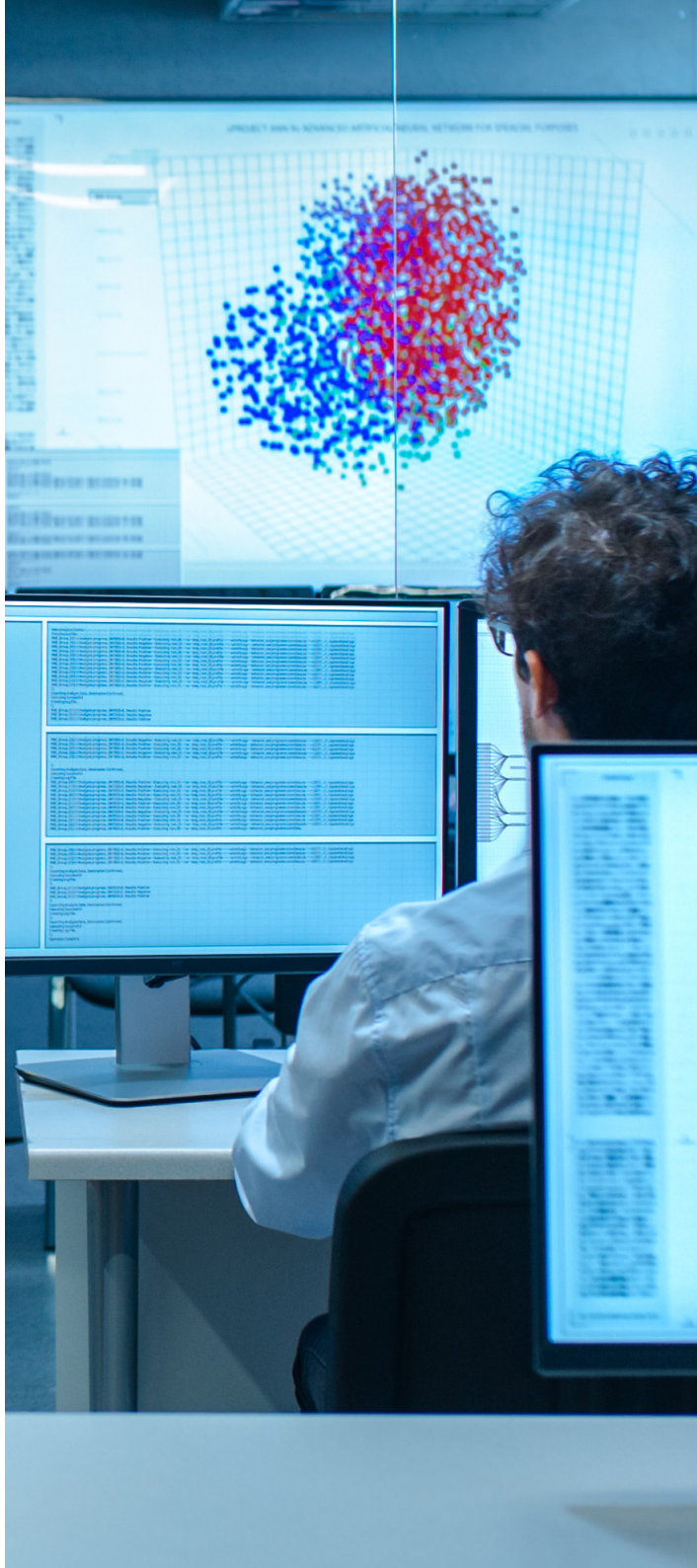


Figure 4. According to the Threat Hunting Survey of Cybersecurity Insight, 2021, lack of expertise, lack of technologies, tools, and intelligence, lack of structured workflows and lack of visibility/data are the primary barriers to implementing a threat hunting program



3. Lack of visibility

You can't stop what you can't see. When it comes to endpoint detection and response, the telemetry available across all endpoints is critical. Lightweight endpoint agents must collect robust telemetry, delivering deep visibility to support faster and more accurate hunting, investigation, and incident response during the threat protection life cycle.

Telemetry must be automatically normalized, stored at scale, and accessible for immediate and consistent analysis. Whether it is for hunting, investigation, or forensics, long-term access to the telemetry is essential.

According to Ponemon Institute, in 2021, the average time to identify a breach is 212 days, and the average time to contain it is another 75 days, totaling a 287-day breach lifetime. Threat hunters and security analysts need to investigate retrospectively for at least 300 days; otherwise, they could get blind-sided in their research and investigations.

WatchGuard believes that 365 days of retention is a must. Our Threat Hunters use the rich telemetry in real time, having complete visibility at their fingertips.

4. Lack of technologies, tools, and updated-in-minutes threat intelligence

An effective EDR solution requires that the massive amounts of telemetry collected from the endpoints are automatically enriched with context and correlated so it can be mined for signs of attack with various analytic techniques. One key attribute is file reputation.

Search and visualization tools that enable quick and easy search in the telemetry for any use cases are fundamental for hunters to speedily and handily pivot entities, events, and parameters to identify attack patterns and examine what's happening on the endpoints to spot threats faster.

Finally, any successful threat hunting program must be informed by intelligence. The vast majority of organizations doing in-house threat hunting today operate at a low level in the hunter maturity model, as their hunting activities are often informed by known IoCs. In contrast, true threat hunting is a proactive exercise, not reactive, and means searching for the unknown behavior to uncover and disrupt threats before any damage is done. As such, in successful continuous threat hunting, hunters must be informed by high-quality real time, in-context Intelligence.

WatchGuard Unified Security Platform™ enriches the telemetry with our unique zero-trust application service and a vast volume of updated-in-minutes, high-quality, contextualized threat intelligence.

5. And finally, cost-prohibitive and complex

Today organizations increasingly realize the need to hunt for ever-evolving threats. However, those that have attempted to establish a mature threat hunting program internally have quickly recognized the complexities, cost, and burden of building a threat hunting program, due to the infrastructure, tools, knowledge, threat intelligence, and workflows needed. Additionally, maintaining the practice consistently for a long time without any external support tends to be out of reach for even the most proficient security teams.

For an organization attempting to do this internally, it is highly challenging to quantify the return on investment on a day-to-day basis. It's also extraordinarily complex as hunting operations need to be highly structured. This means the development of workflows and processes that warrant the result requires elite in-house threat hunting expertise.

5. An efficient hunting program with WatchGuard Advanced Endpoint Security

WatchGuard's continuous monitoring of endpoint activity allows the agent to act as a sensor and inform the Cloud platform about the files running and execution context.

According to Ponemon Institute, in 2021, the average time to identify a breach is 212 days and the average time to contain it is another 75 days, totaling a 287-day breach lifetime. Threat hunters and security analysts need to investigate retrospectively for at least 300 days; otherwise, they could get blind-sided in their research and investigations.

No data, no hunt! Period!

WatchGuard believes that 365 days of retention is a must. Our Threat Hunters use the rich telemetry in real time, having complete visibility at their fingertips.

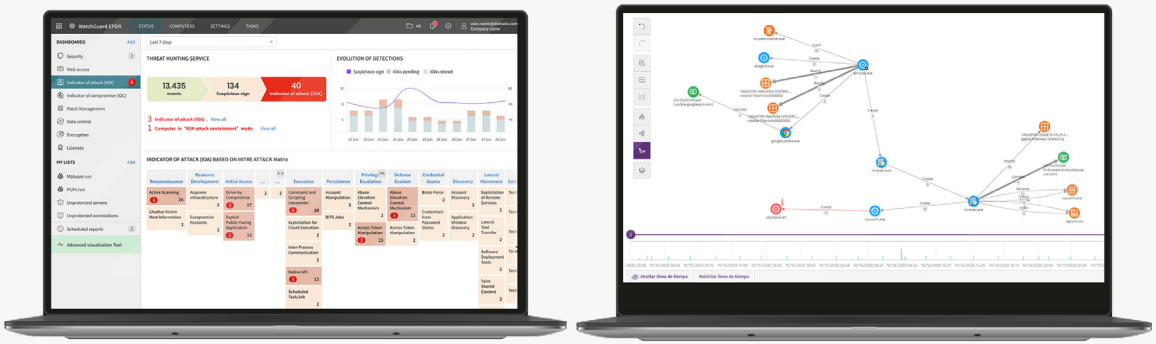
WatchGuard's Threat Hunting service, supported by the 365-day telemetry, the behavioral AI engine, Threat Radar, and our Threat Intelligence – open-source intelligence (OSINT) like MITRE ATT&CK, Cyber Threat Alliance, and proprietary intelligence identify abnormal behaviors and categorizes them as indicators of attacks (IoAs).

WatchGuard hunters sift through these indicators looking for in-the-wild and with-a-high-degree-of-confidence ones, which are then represented on the administrator console as IoAs (indicators of attack).

The IoAs provide valuable information to mitigate the attack and take actions to avoid being a target for threats next time, such as adjustment on system configurations patching endpoints, or revoking users. RDP brute force attacks, privilege escalation, fileless attacks, and lateral movements are examples of IoAs detected by the Threat Hunting Service, included at no extra cost in our WatchGuard Advanced Endpoint Security solutions.

MITRE ATT&CK™ Framework

At WatchGuard, we implement the MITRE ATT&CK™ Framework (a globally accessed knowledge base of adversary tactics and techniques based on real-world observations) across the multiple WatchGuard Security processes and product features to help improve analysts' productivity and prevent breaches.



By adopting this systematic process of hunting, we have incorporated the following specific services into our Advanced Endpoint Security portfolio:

The **Threat Hunting Service** makes hunting for MITRE ATT&CK TTP fast and painless. The service, included by default in all WatchGuard Advanced Endpoint Security solutions, transforms weak signals into solid indicators of in-the-wild fileless malware attacks (IoAs). Contextualized IoAs are delivered in the console with interactive graphs of the course of action.

The Threat Hunting Service is provided at no charge to all WatchGuard Advanced Endpoint Security solutions.

6. The Threat Hunting service as an extension of Your Team

A collaborative and coordinated approach is the key to stopping today's breaches and delivering the highest level of managed security to your customers in a seamless manner.

You or your partner can quickly expand their services leveraging the outcomes of the Threat Hunting service by validating the IoAs and responding to the attack.

WatchGuard EDR and WatchGuardEPDR may notify immediately when a new IoA arises. Each IoA comes with a list of recommended actions to block, remediate, and avoid future attacks using the same TTPs as a starting point for you or your partner.

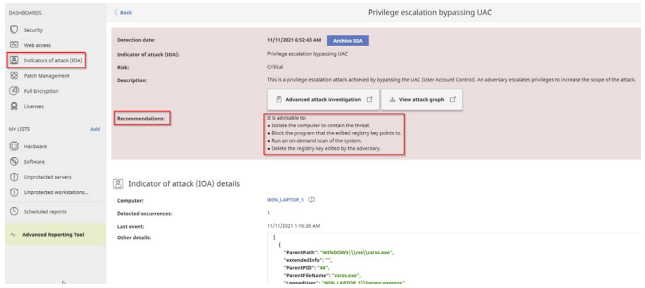


Figure 6. The Threat Hunting Service shows all the details to mitigate and respond to threats when IoAs are detected.

7. Summary

In summary, let's recap some key takeaways for the organizations that are currently performing or considering starting up an internal threat hunting capability:

1. **Threats are moving faster than ever before.** Remember the speed at which threats are operating and evolving.

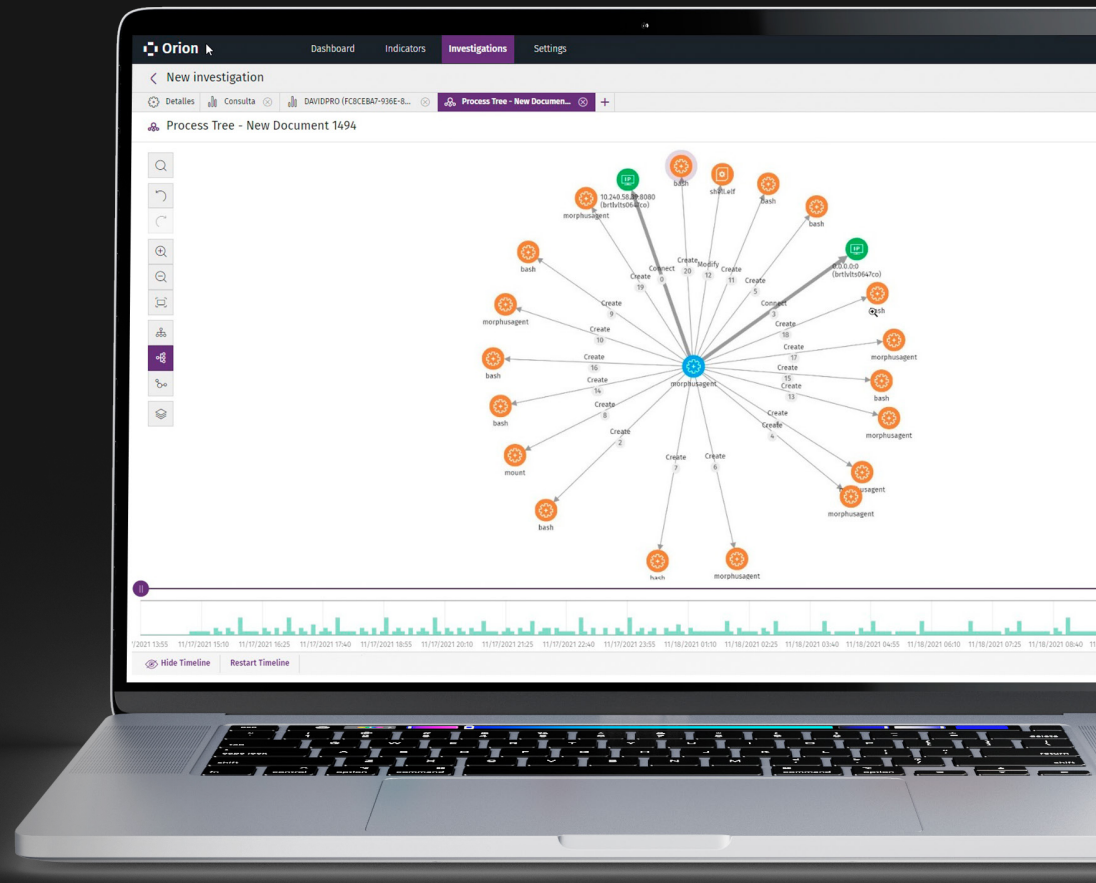
2. **No organization is immune, regardless of size, vertical, or location.** Every organization is a target, regardless of where your organization is located and the vertical you operate in.

3. **Threat hunting is now a must-have for every organization.** Given the speed at which threats are moving, hunting is no longer a nice-to-have; it needs to be viewed as a must-have capability for every organization.

4. **Speed, scale, and consistency are critical.** Threat hunting needs to be able to be conducted with speed and scale. And that requires structured, repeatable processes, mature technologies, long-term visibility, and threat hunters backed by deep expertise, knowledge, and threat intelligence.

5. **Structure your hunts using the MITRE ATT&CK framework.** Advanced Endpoint solutions come fortified with many ATT&CK techniques identified, thus enabling the security team to focus its efforts on dealing with security threats leveraging the well-defined information provided by the framework and extended by our cybersecurity team.

6. **If you cannot do this in-house, partner with a provider that can.**



1. Cybersecurity Insiders conducted the fourth annual threat hunting research project to gain deeper insights into the maturity and evolution of the security practice. This threat hunting report is based on the results of a comprehensive online survey of cybersecurity professionals conducted in February 2021 to gain deep insight into the latest trends, key challenges, and solutions for threat hunting management. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

WatchGuard

THE WATCHGUARD PORTFOLIO

Network Security

WatchGuard Network Security solutions are designed from the ground up to be easy to deploy, use, and manage – in addition to providing the strongest security possible. Our unique approach to network security focuses on bringing best-in-class, enterprise-grade security to any organization, regardless of size or technical expertise.

Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to address the password-driven security gap with multi-factor authentication on an easy-to-use Cloud platform. WatchGuard's unique approach adds the "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Secure Cloud Wi-Fi

WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.

Endpoint Security

WatchGuard Endpoint Security is a Cloud-native, advanced endpoint security portfolio that protects businesses of any kind from present and future cyber attacks. Its flagship solution, WatchGuard EDPR, powered by artificial intelligence, immediately improves the security posture of organizations. It combines endpoint protection (EPP) and detection and response (EDR) capabilities with zero-trust application and threat hunting services.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by more than18,000 security resellers and service providers to protect more than 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

NORTH AMERICA SALES 1.800.734.9905 INTERNATIONAL SALES 1.206.613.0895 WEB www.watchguard.com

Part No. WGCE67539_120721