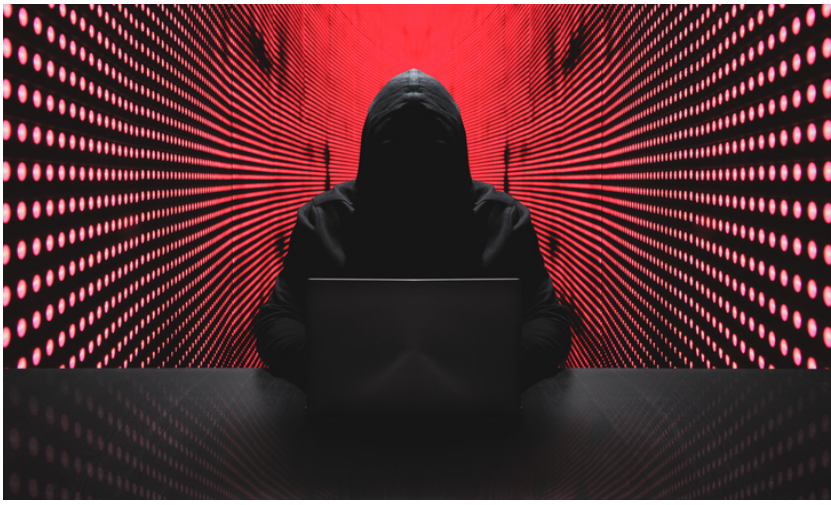
panda
a WatchGuard brand



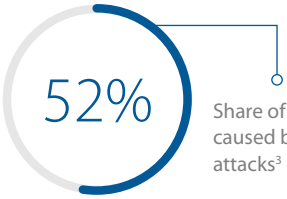
Threat Hunting Service

Cyber Threats and Undercover Malicious Actors Are Multiplying

Cyber crime presents an unrelenting danger to businesses and governments. Data shows a rapid increase in the number (11% more every year[1]) and sophistication of attacks, as well as in the business costs incurred. ($5.52 million is the average total cost of a breach for enterprises with more than 25,000 employees and $2.64 million for organisations with under 500 employees.[2])

Although the increase in cybersecurity investment (+10%, $60.2 billion[3]) has led to a greater level of protection, there is no such thing as absolute security, and organisations cannot afford to wait for an attack and then take action, giving attackers time to gain access to the corporate network.

Once inside, malicious actors hide in the everyday nature and complexity of their target's environment, often using legitimate mechanisms and hiding their activities in normal network traffic to achieve their objectives. Depending on the security sophistication of the target network, an adversary is often presented with ample time to do their work.



Share of breaches caused by malicious attacks[3]

Country with the highest data breach costs[3]

Understanding Cyber Attacks

Threat hunting proactively searches for cyber threats that are lurking undetected in the corporate network. Threat hunting digs deep to find malicious actors in your environment that have been able to bypass traditional defense measures.

After sneaking in, an attacker can stealthily remain in a network for months as they patiently wait for opportunities to steal data, uncover confidential or personal information, or discover key identities and obtain login credentials that will allow them to move laterally across the environment.

Once an adversary is successful in evading detection and the attack has begun, many organisations that lack the necessary budget, technology, processes, and above all a team of experts, are unable to prevent and detect it. This makes it impossible for those companies to build and grow their defenses at the same rate that cyber crime evolves.

-3.58 MILLION

Cost savings of fully deployed automation vs. no security automation[3]

315 DAYS

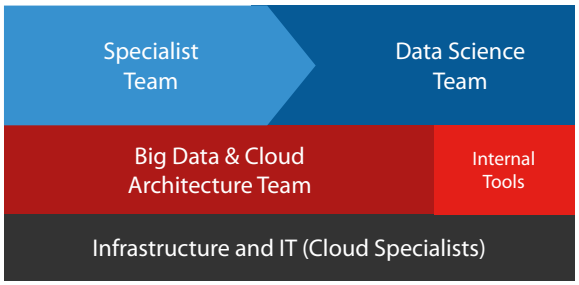
Average time to detect and contain a data breach caused by a malicious attack[3]

As the number of successful cyber attacks soars, it's critically important to take a proactive stance to detect them. You can't simply take a passive approach and hope for an automated alert to let you know you've been breached. You need to actively seek out potentially malicious behaviour on your network, hunting down indicators of attack (IoAs) so you can detect and contain an incident as quickly as possible.

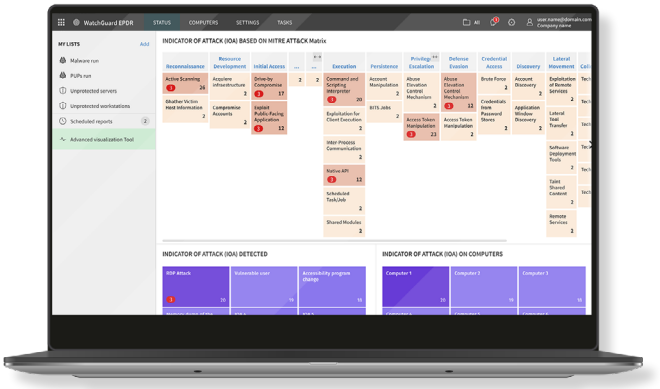
Hunting the Unknown

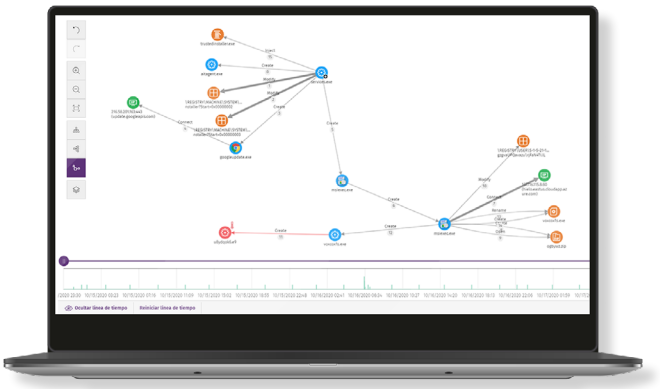
Adaptive Defense's continuous monitoring of endpoint activity allows the agent to act as a sensor and inform the Cloud platform not only about the files being run, but also about their context of execution (what happened right before, which users are trying to run which command or application, what network traffic is generated, which data files accessed, parameters, etc.).

This allows our Threat Hunting Service to identify abnormal behaviour and suspicious activity and their categorisation as indicators of attack with a high degree of confidence and without false positives.

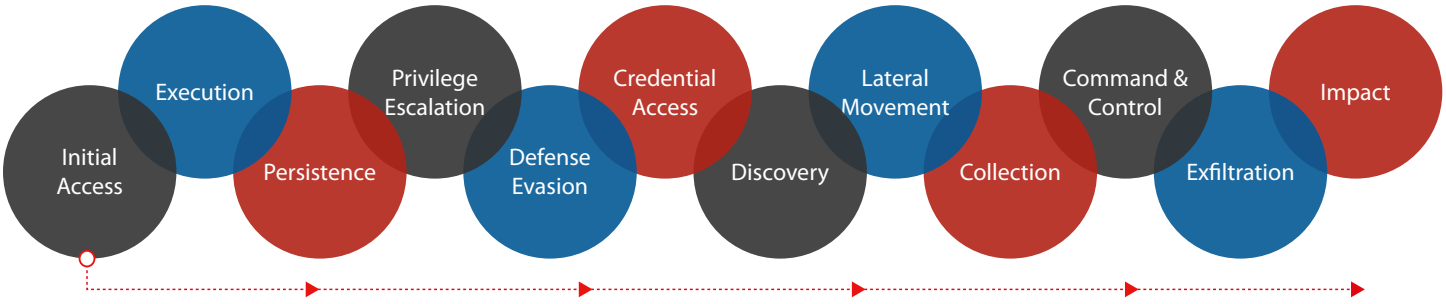


We have implemented the MITRE ATT&CK™ Framework (a globally accessed knowledge base of adversary tactics and techniques based on real-world observations) across multiple Endpoint Security processes and product features to help improve analysts' productivity and prevent breaches. By adopting this framework, we have incorporated the following specific phases of IoAs into Adaptive Defense 360 and Adaptive Defense solutions.





Often IoAs are related to specific phases of the Cyber Kill Chain or to the tactics of the MITRE ATT&CK framework adopted by our advanced Endpoint Security solutions.



Detecting IoAs before data is exfiltrated (or encrypted in the case of a ransomware attack) is a very effective defense mechanism, especially against living-off-the-land (LotL) attacks, even if endpoints may have already been compromised.

Adaptive Defense and Adaptive Defense 360 integrate, within the same protection agent, a complete technology stack to detect IoAs in different attack phases. Far from being static technologies, they are updated continuously with new attack patterns and techniques that are discovered by the Threat Hunting Service.

Hackers are launching **extremely sophisticated cyber attacks**. There are no security measures that can ensure 100% protection. Fileless attacks in particular are a growing concern, being increasingly difficult to detect. **But hackers can still leave traces** that enable us to detect unknown attacks that leverage living-off-the-land techniques.

The automated Threat Hunting Service continuously monitors everything that happens in the endpoints in real time in the form of **event telemetry**. In case of a **validated breach** with a living-off-the-land technique, the indicator of attack is shown and recorded in the web console.

RDP brute force attacks, privilege escalation, fileless attacks, and lateral movements are examples of IoAs detected thanks to the Threat Hunting Service, included at no extra cost in our EDR solutions.

The Automated Threat Hunting Service - Revealing the Undetectable

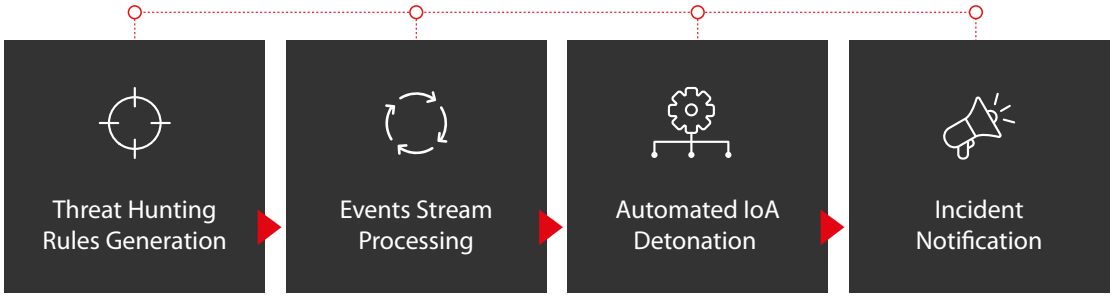
Our Threat Hunting Service, included in Adaptive Defense and Adaptive Defense 360, is based on a set of threat hunting rules created by threat specialists that are automatically processed against all data gathered from telemetry, which triggers IoAs of high confidence and with a low rate of false positives to minimise MTTD and MTTR (Mean Time To Detect and Mean Time To Respond).

These indicators of attack are the result of a continuous process to discover threat actors, using advanced data analytics, our proprietary threat intelligence, and the expertise of our analysts.

This service inherits all the cyber intelligence that we have perfected thanks to our years of experience in threat research and the historical visibility offered by a registry of application behaviors that has received more than 10 billion events per day, user and machine for more than 30 years. We have strategic alliances with international organisations such as the Cyber Threat Alliance, where we exchange indicators of attack (IoAs), indicators of compromise (IoCs), and their corresponding responses.

Should they come across an anomalous situation, the customer is notified via the web console showing details and graphs of the anomaly, providing forensic analysis of the affected systems, the origin of the attack, and the techniques used. They also provide recommendations on how to mitigate the attack and reduce the attack surface to avoid falling victim to future attacks.

How the Threat Hunting Service Works



1. Help Net Security: 2020: The year of increased attack sophistication
2. Canalys: Cybersecurity investments will increase up to 10% in 2021
3. Ponemon Institute and IBM Security: Cost of a Data Breach Report 2020

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.
To learn more, visit WatchGuard.com.