guardDog

Active Incident Response White Paper

by Peter Bookman

Between a mass convergence of intelligent devices and the devised chaos that has infiltrated our everyday lives, technological warfare of our “human rights” is being stripped away second by second by a faceless enemy of predators paraded as a Superpower of Communication preying on our vulnerabilities and tracking our every move- inflicted with the sickness of exploitation, manipulation, and violation. It has become appallingly clear that the invasion of a disenfranchised “network” is highly frangible against criminal factions of nefarious activities from online tactics to propagated interrogation that compromise our safety and put us gravely at risk. At guardDog.ai, we believe that the blueprint that drives the cybersecurity lane to success is to deter, apprehend, and disarm attacks without interference to our daily practices.

guardDog

Passive & Active Cyber Defenses

Active Cyber Defense Introduction

Historically cybersecurity has taken an approach similar to what the US Department of Defense categorizes as passive defense, considerably defined as "Measures taken to reduce the probability and minimize the effects of damage caused by hostile action without the intention of taking the initiative." Whether firewalls, virtual private networks (VPN), mobile device management, or a host of other available technologies and products, they seek to react and create barriers and walls that mitigate risks without taking initiatives or offering a proactive approach to countermeasure against breached threats and attacks. You can identify these types of defenses in cybersecurity solutions by their use of the verbiage "Zero Day" or "Zero +1 Day".

In contrast to belief, with what the Department of Defense defines as active defense: "The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy." which not only takes initiatives but anticipates profiles and takes action against connective collusion, falls short of proactive cyber defenses with technologies such as "Asymmetric Defenses," Moving Target Defenses (MTD), or a method that's been used for a long time referred to as "Honey Potting." While these methods indeed begin to change the marketplace and prelude tactical efforts from being passive to active, the financial models associated with protection versus the costs of the attack don't add up. It all boils down to human cost versus automated cost. GDS deploys autonomous incident response (AIR) that responds in real-time and has the magnitude to afford the most effective concierge solution than any other current offering in the cybersecurity arena. In turn, this allows people to have better protection and avoid vulnerability than the scant few substantial companies that can afford the human cost of full-time cybersecurity professionals.

Cyber defense focuses on sensing, detecting, orienting, and engaging adversaries to assure success and to out-maneuver the rival. This shift from security to defense requires a strong emphasis on intelligence, surveillance, and reconnaissance, integrated with staff activities to include intelligence, operations, communications, and planning. Proactive Cyber Defense means acting in anticipation to oppose an attack involving computers and networks. It represents the machine learning between purely offensive and defensive action, interdicting and disrupting an attack or a threat’s preparation to attack, either preemptively or in self-defense. The mission of the preemptive proactive operations is to conduct aggressive interdiction and disruption activities against the assailant.

guardDog

Passive & Active Cyber Defenses

Active Cyber Defense Introduction

Proactive cyber defense operations engage preemptively with the adversary.

Cyber threat hunting is the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions. Offensive, proactive cyber activities and active cyber defense facilitate anticipatory threat reduction while informing protection, detection, and incident response, given its ability to engage the adversary at a distance and time.

- Has greater efficacy than reactive systems.
- Drastically reduces the volume and severity of attacks, leading to fewer alerts, incidents, and costs. Thus, passing these savings to cybersecurity.
- It provides early warning and indicators to zero-day model signatures to incident response mechanisms and enumerates attack networks through cyber threat intelligence.
- Is not subject to scalability issues around performance and cost like reactive systems.
- Uniquely has the capability to shape contested space.

guardDog

Definitions of Exploit, Vulnerability, Threat, Attack, and Defense

While there are many viewpoints and overlapping concepts of cybersecurity-based words, it is helpful to identify what we mean by the terms exploit, vulnerability, threat, attack, and defense. For example, although used interchangeably historically, an attack such as a “man in the middle” attack first utilized exploits and threats to successfully implement the attack.

Vulnerability -

This is a weakness that can be exploited by a threat, such as an attacker, to perform unauthorized actions within a computer system.

Exploit -

The sequence of commands takes advantage of a vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.

Threat -

This combination of exploits, toolkits, and know-how intelligence that someone executes is conceived as a “threat actor” to achieve a successful attack.

Attack -

This is the execution of exploits and threats in an aggressive manner intended to cause hurt upon a device, network, or system when combined.

Defense -

Regardless of passive or active, these are methods intended to mitigate threats and attacks that respond accordingly towards protecting hacked or breached resources.

guardDog

How Exploits, Threats, & Attacks are Used Against Passive and Proactive Security

In a Passive Cyber Defense system, attacks or breaches are only identifiable to the network or device they monitor and typically don't have a critical visibility reaction time. Although we see numerous products and solutions in this arena utilizing automation, they are considered passive due to the response needed to remediate the vulnerabilities before damage and havoc are identifiable. By the time an invasion is successfully redeemed, the attack's objectives have escalated into other territories where the threat and exploit have taken a stranglehold of the network. Even without a successful attack, it's likely that many systems are compromised due to threats and exploits, allowing for footholds and engagement outside of the prescribed use of the system.

In proactive cyber defense, although methods might vary, the idea is to restrict an exploit or threat from getting into your system at all times. In the case of AIR technology, we utilize the vulnerability of the exploits and the exploiting systems themselves to stop attacks before they're able to formalize. Like their passive counterparts, the AI methodology is used in the same setting with different intentions to gain results. Instead of focusing on the time of reaction, automation's trained to learn new profiles and optimize efficiencies of attack prevention before it organizes and spreads.

guardDog

Exploits and Threats are Common on Networks Before Becoming Attacks

Although there are many passive cyber defense methods that, when combined, can help mitigate threats and attacks or the damage they can do, ultimately, there are far more exploits and vulnerabilities that are used towards successful attacks when executed.

Whether VPN, Firewall, Intrusion detection, and prevention, or even threat intelligence adding to these technologies to make them more ADAPTIVE, the vulnerabilities of the devices themselves as well as the network make it easy to do recon as well as initiate attacks whether from a simple toolkit or using generally available network commands. One example of how easy it is to gather information on a network without even sending any traffic or connecting to it is by looking at your device list. It sends the universal commands to everything it operates and monitors by using the following command: “arp-a,” and it will list the devices your network router will report it sees and how the network configures to get out. So by using this example, without crossing over a firewall or even if using a VPN technology, the network itself and the devices we all use leaves ourselves exposed to the vulnerabilities inherent to the network and devices themselves.

guardDog

What is Meant by Wireless Network Security Today & Common Methods

Two types - encryption usage for privacy and network usage privileges

Commonly deployed on wireless networks are some form of encryption, though there can be some vulnerabilities with these encryption methods if the networks are subject to exploitation. Commonly used protocols are WEP (an old standard that should not be in use today and regularly found) and WPA, where each of these is designed much like a VPN within the network to offer privacy within the wireless network. While these encryption methods offer privacy when deployed correctly, they provide no device-level protection or even protection for and from the network itself.

Network usage privileges are far more common and hard to measure just how exploited these types of hacks and engagements are. Most if not all wireless networks, due to not knowing who and what devices are on the grid, offer no levels of protection at a device level, leaving that to the users on the network, which are often the weakest link because of the need for each device to maintain itself and ensure its maintenance with the latest updates without known exploits. Even, when an internal network might be attached to a shared or public WIFI offering there are commonly shared radios between them. The network itself offers no protection for itself, much like the devices that are on them.

Often WIFI networks are managed and connected to gateways or firewalls that can protect against attacks known and that pass through the gateway or firewall using packet inspection and searching for known attack signatures and threats with them. Because this is limited to passing through a wall, this only is effective in environments where the systems under the protection are known and understood to what the intended attacks might be.

Building on these concepts with proactive defense and being able to profile attacks before organized into a threat from the exploits that start them, we can thwart attacks from being able to start in the first place. If a system gets compromised with methods outside of exploitive network behavior such as a traditional virus that might use a network to spread, a proactive defense would not see the attack until the infected device or machine attempts to proliferate or compromise something off of the machine infected. Yet when that happens, a proactive defense can then take action to go beyond traditional threat mitigation and thwart the exploit off the virus might attempt to spread.

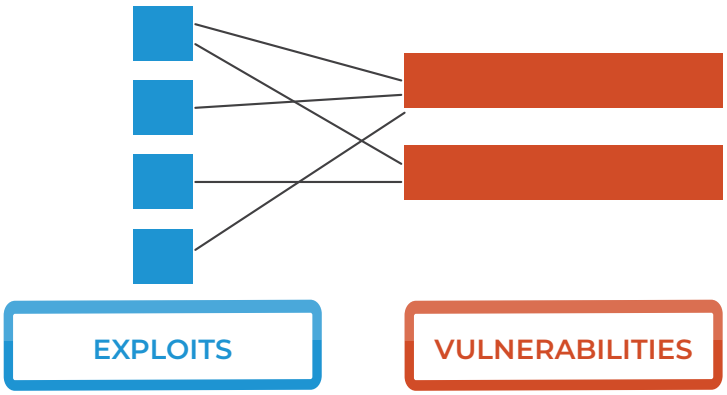
guardDog

Cyber Attack Orchestration & Countermeasures

Exploits and their relation to vulnerabilities of systems

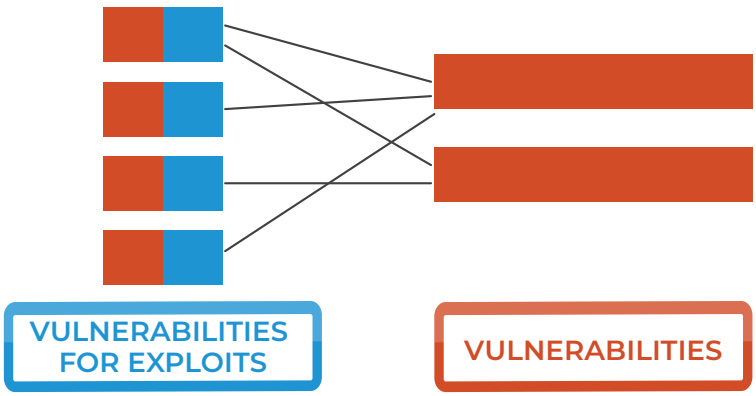
In the passage of this writing, there were 156,355 entries, up from 125,012 entries since last year, describing exploits from the CVE database available by Mitre. While this is a vast and daunting list, there are a growing number of others that are undocumented and utilized.

While there are names and hacks, these exploits do not necessarily follow the same concepts and instead tend to form more of a map of exploits to known vulnerabilities.



Turning Exploits into Vulnerabilities

Like any system, an attacking device or machine has its vulnerabilities allowing for exploiting systems to be targeted in such a way as to halt the attack. Combining the available exploits and vulnerabilities and then focusing on the components, using the exploits associated with the given attack or exploit can effectively thwart attacks before they can implement them.

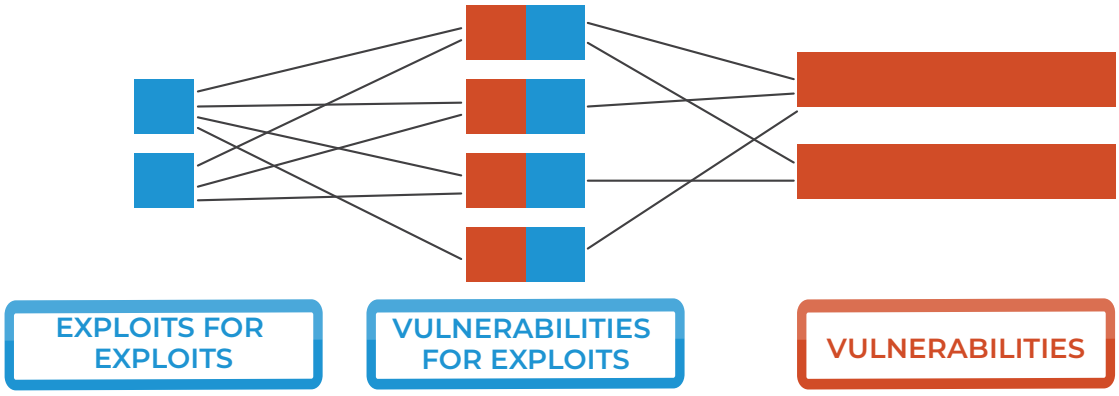


guardDog

A Catalog of Exploit Countermeasures

A Catalog of Exploit Countermeasures

One way to look at a proactive cyber defense methodology would be to catalog counter measuring exploits and their usage patterns against the exploits now being used to create threats by exploiting vulnerabilities. A catalog such as this could then be automated using artificial intelligence (AI) to successfully thwart attacks and threats before they can become such, starting from the exploit stage.



Anatomy of a Traditional Hack

No matter whether attacking devices or networks, attacks begin and rely on recon to achieve any form of success throughout the irruption.

There are numerous cybersecurity toolkits available meant to exploit devices and networks in a nearly automated way. Recon and each step are guided and simplified to easily allow for the hacking of various types and signatures.

guardDog

Advanced Persistent Threats

One example of the types of situations for which current passive cyber defense technologies have difficulty recognizing or stopping that active cyber defense cannot only do better but in the case of utilizing Active Threat Elimination on top of Threat Intelligence can thwart an attempted threat through eliminating the exploits that are used to make up a threat or attack.

Definitions of precisely what an Advanced Persistent Threat (APT) can vary and summarized by their named requirements below:

• Advanced – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include commercial and open-source computer intrusion technologies and techniques but may also extend to include the state's intelligence apparatus. While individual components of the attack may not be well designated or particularly "advanced" (e.g., malware components generated from commonly available do-it-yourself malware construction kits or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques to reach and compromise their target and maintain access to it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from "less advanced" threats.

• Persistent – Operators prioritize a specific task rather than opportunistically seeking information for financial or other gains. This distinction implies that external entities guide the attackers, and targeting is conducted through continuous monitoring and interaction to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. A "low-and-slow" approach is opportune. If the operator loses access to their target, they usually will successfully reattempt access. One of the operator's goals is to maintain long-term access to the target, in contrast to threats which only need access to execute a specific task.

• Threat – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized, and well funded. Note that actors are not limited to state-sponsored groups.

guardDog

Advanced Persistent Threats

Specific to WIFI and a prolific example of Advance Persistent Threats is the Dark Hotel hack.

DarkHotel (or Darkhotel) is a targeted spear-phishing spyware and malware spreading campaign that appears to be selectively attacking business hotel visitors through the hotel's in-house WIFI network. Kaspersky Lab characterizes it as an advanced persistent threat.

The attacks are targeted explicitly at senior company executives, using forged digital certificates generated by factoring in the underlying weak public keys of genuine certificates to convince victims that prompted software downloads are valid.

By uploading malicious code to hotel servers, attackers can target specific guests at luxury hotels, primarily in Asia and the United States. Zetter (2014) explains that the group, dubbed DarkHotel or 'Tapaoux', has been actively infecting users through spear-phishing and Peer-to-Peer networks since 2007 through key-logging and reverse engineering. "Man in the middle" was also a technique used for this attack.

Utilizing a method called SSLsplit allows hackers to display fake phishing login pages to sites of interest with a forged SSL certificate. This is one of the many attacks guardDog detects, eliminates the attacker, and raises the alarm.

Targets are aimed primarily at executives in investments and development, government agencies, defense industries, electronic manufacturers, and energy policymakers. Many victims are earmarked in Korea, China, Russia, and Japan.

Once attackers are in the victim's computer(s), sensitive information such as passwords and intellectual property is quickly stolen before attackers erase their tools in hopes of not getting caught.

guardDog

Recon Allows for Knowledge of Initial Exploits Towards Threats and Attacks

Because the network itself will report on what devices are interconnected, simple interrogation can return what known or unknown vulnerabilities might be on that particular device or network. Recon is a simple beginning to any exploit used to create a threat or attack when combining those elements. Recon can take on many forms but are generally executed. Using toolkits makes turning recon into targeted exploits and threats towards an objective that every cybersecurity environment would recognize as an attack.

Recon compromising and lateral movement are the keys to initiating and engaging in any attack. Recon is when a system sits alongside other systems, and is close to looking and “snoop" for known exploits or vulnerabilities.

Compromising is when a vulnerability or exploit is used for prepense to engage in hacking a device.

Lateral movement is working within the compromised environment freely to further surveillance or move on to the next level of escalation.

What these key factors have in common is that they require probing to take place to complete the initial compromise following either recon or a lateral move. This makes identifying and stopping recon the primary objective of a proactive system. There are few legitimate reasons to engage in vigilante activities, much less engage in stakeouts that rely on these to compromise a network or device on it.

guardDog

Recon and Initial Compromise Engagements can be Profile

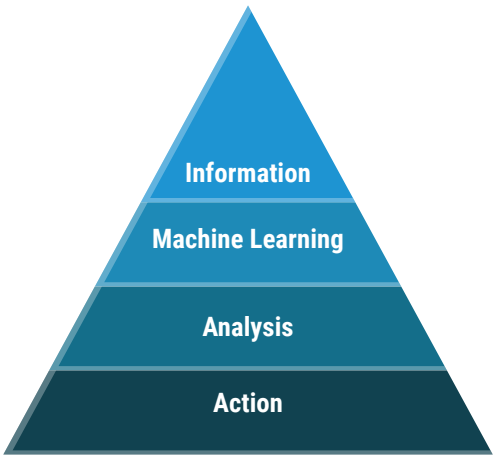
Recon and Initial Compromise Engagements can be Profiled

Due to common elements and overlapping usages, exploits can be profiled effectively, just like potential threats or attacks. Because of the ability to profile exploits as well as a knowledge of common ways to exploit vulnerabilities from devices themselves, a network is an ideal place from which to protect by not allowing recon or initial compromises to take place regardless of where within an attack, threat, or the exploit is taking place. AUTONOMOUS INCIDENT RESPONSE Technology begins with this concept and builds on it to offer protection.

guardDog Autonomous Incident Response Technology

guardDog AIR technologies can quickly implement onto existing networks through a hybrid cloud SaaS offering where guardDog services constantly learn and proactively respond to digital terrorist threats as appropriate based on escalation.

As an overlay working solution to traditional networks, the technology monitors WIFI, wired networks, and reports on found threats and vulnerabilities across networks, attached devices, IoT, and many other potential vulnerable access points. Employment of artificial intelligence, guardDog.ai technology keeps up on the latest threats and can learn new behaviors to apply automated countermeasures to a constantly adapting and expanding attack surface. Found incidents are color-coded and ranked by threat level. Multiple Fido devices can be manageable in a distributed environment, where different privacy and other settings may be required. PCS creates a situational awareness across networks, devices, and other technology that transmit across traditional network environments.



guardDog

Automated A.I. Incident Response (AIR)

Automated A.I. Incident Response (AIR)

guardDog.ai employs a machine learning training methodology called Automated A.I. Incident Response (AIR) to determine the appropriate response to known and unknown threats across the spectrum of evolving and novel attacks on an ever-expanding attack surface. This method guides our A.I. to a proper and measured response based on best practices, rules, policies, and ongoing machine learning. Information from many sensor inputs such as networks, devices, IoT, etc., enters the top of the triangle. Then this information is put through Analysis and matched against known threats for resolution response. Unknown threats are flagged and recorded for further understanding and machine learning. Comprehensive knowledge from the informed Analysis is derived and put into Action, processed into machine learning algorithms to teach and evolve incident response in a repeating cycle.

AUTONOMOUS INCIDENT RESPONSE Technology can be deployed as either passive or active cyber defense.

guardDog.ai employs a machine learning training methodology called Automated A.I. Incident Response (AIR) to determine the appropriate response to known and unknown threats across the spectrum of evolving and novel attacks on an ever-expanding attack surface. This method guides our A.I. to a proper and measured response based on best practices, rules, policies, and ongoing machine learning. Information from many sensor inputs such as networks, devices, IoT, etc., enters the top of the triangle. Then this information is put through Analysis and matched against known threats for resolution response. Unknown threats are flagged and recorded for further understanding and machine learning. Comprehensive knowledge from the informed Analysis is derived and put into Action, processed into machine learning algorithms to teach and evolve incident response in a repeating cycle.

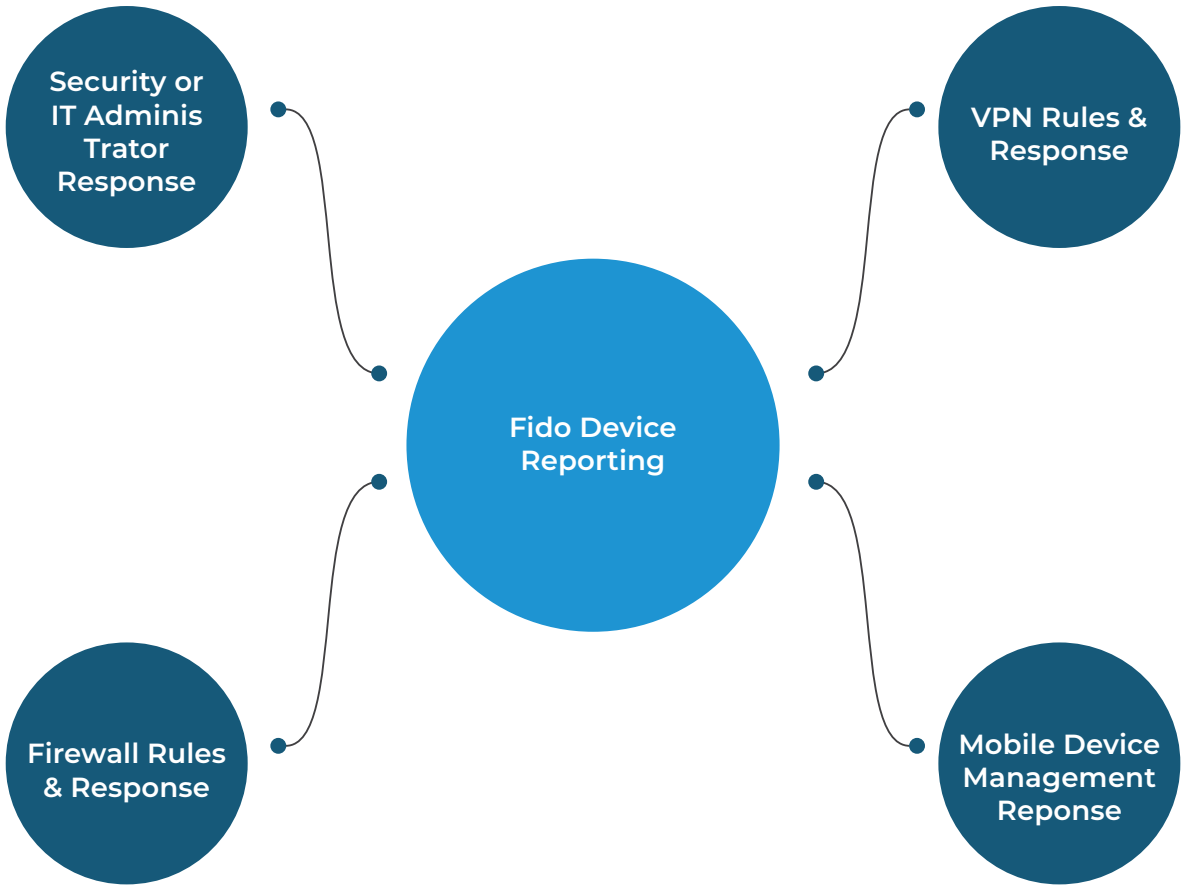
AIR Classification Modes

guardDog.ai has three classification modes of response within the AIR framework. Each of them is customizable and follows the operating rules of the law of engagements it abides. The following matrix explains these classifications.

guardDog

Fido is Passive & Works with Professional Services and other Technologies to Provide Threat Intelligence

When our novel Fido product deploys to a security professional or other administrator, guardDog.ai takes action and gives both a passive and autonomous incident response that acts as an active defense offering. We can integrate into other passive defense measures such as firewalls, VPN, or mobile device management solutions which extend early detection and provide an interactive resolution to potential issues faster and more efficiently than ever before. The results are a much smaller attack surface by which hackers can exploit. guardDog recognizes the threat through means of an ML engine that's quickly trained and works on blocking and attacking the wielders.



guardDog

guardDog is Active & Proactively Exposes and Exploits Threats

guardDog is Active & Proactively Exposes and Exploits Threats

guardDog layers on different reactions and offerings beyond the response of exploitation, threat, and attacks through the industry's first Active Threat Elimination Technology. By responding to exploits early and often while the exploits have not yet evolved to threats or attacks, guardDog.ai can thwart potential threats or attacks before they fully form and cause intentional and irreparable damage.

Combining Passive & Active Cyber Defense for Best Practices

Utilizing threat intelligence to up-level cybersecurity

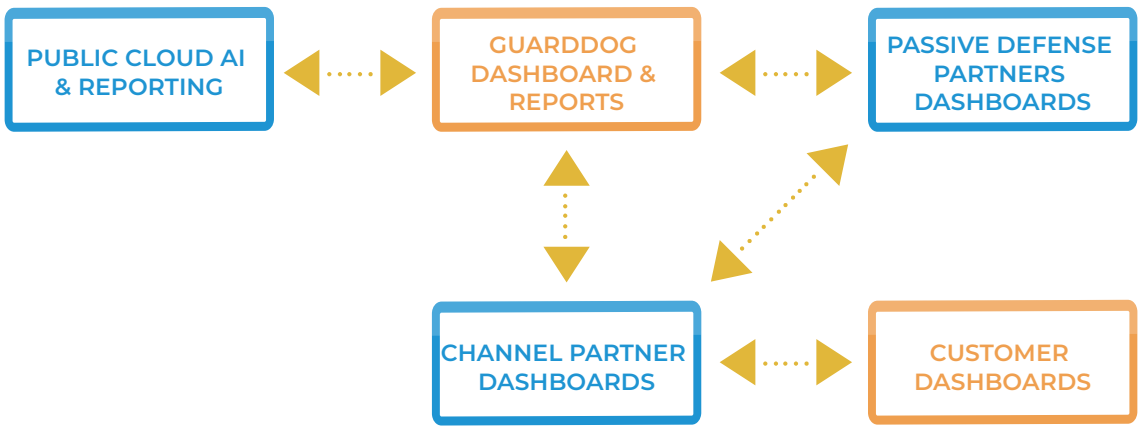
When a Fido's deployed, it will immediately begin to penetrate and test the network it's part of and near. In addition, it will start to watch for known and unknown exploits and provide reporting along the way to partners and customers alike to take action.

Immediately after deployment Fido can perform the following to allow for faster reactions to threats and attacks while they are still at an exploit level:

- Fido can notify a channel partner or customer who can then adjust or create firewall rules.

- Fido will secure its partnerships and tell the firewall directly to adjust and adapt to its rules or create new ones.

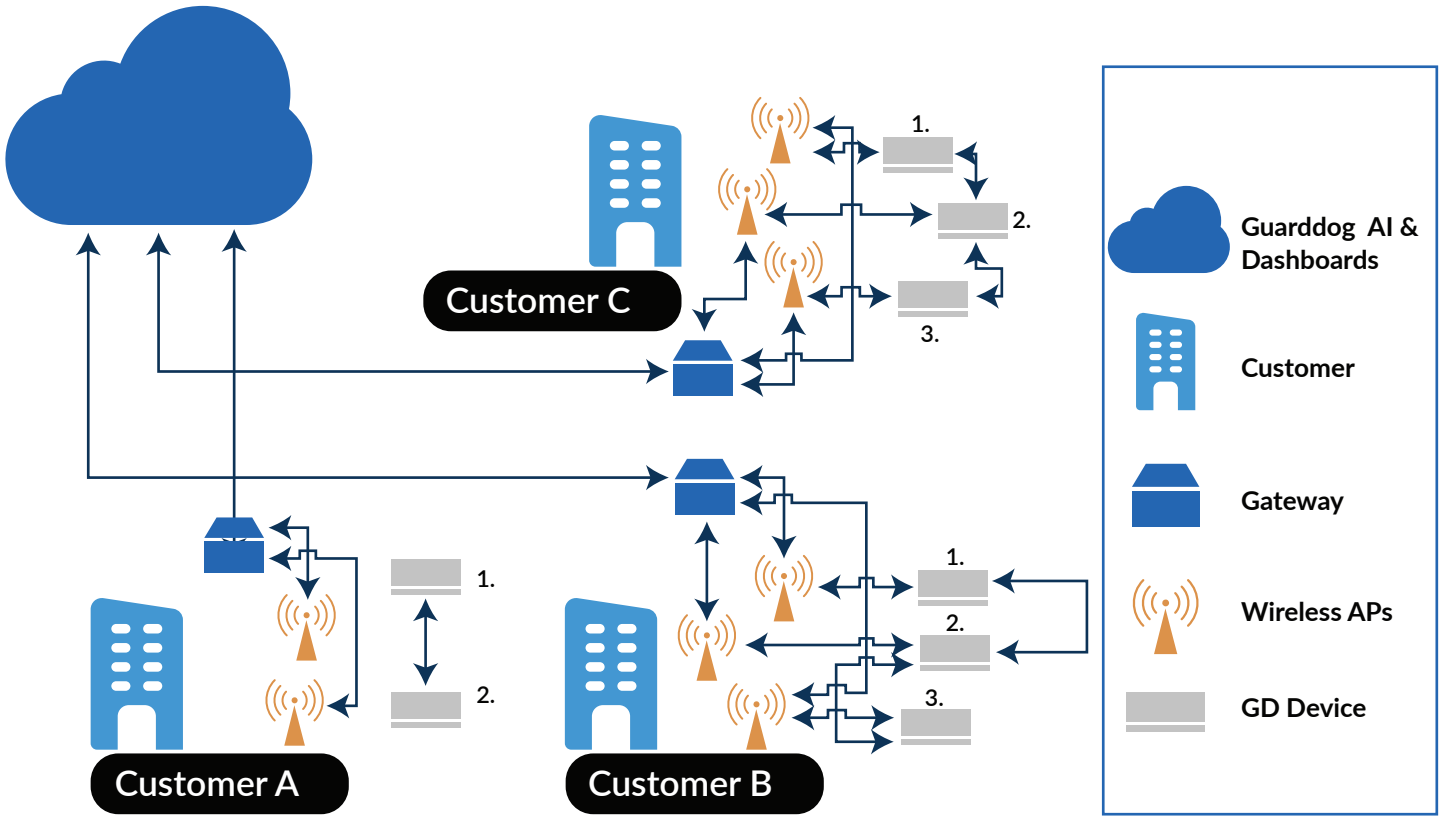
- By simply adding Fido to existing passive solutions, they can become more active and then add the proactive component of threat elimination.



guardDog

Threat Intelligence can lead to Threat Elimination

Once Fidos are expanded upon to have a 1:1 ratio with the wireless radios on a customer's site and are converted to guardDog configurations, they're easily used to not only do threat intelligence but offer threat elimination. For each site location and customer, the reports and dashboard configure to allow for that site to manage itself and enforce policies on the kinds of exploits it is seeing and what responses to automatically deploy for exploits, threats, or attacks as they come up. Within each site, guardDog devices will communicate with each other and utilize the specialized AI that they share between them to identify, disarm, disable, and destroy as needed based on escalation, as well as notify all systems involved of what steps might be best suited to arbitrate future exploits that might come up. Each guardDog device also communicates back to the AI and cloud-hosted node that ensures all guardDog devices worldwide are aware of the latest seen exploits and adequately trained to create algorithms that proactively eliminate the threats as they evolve.



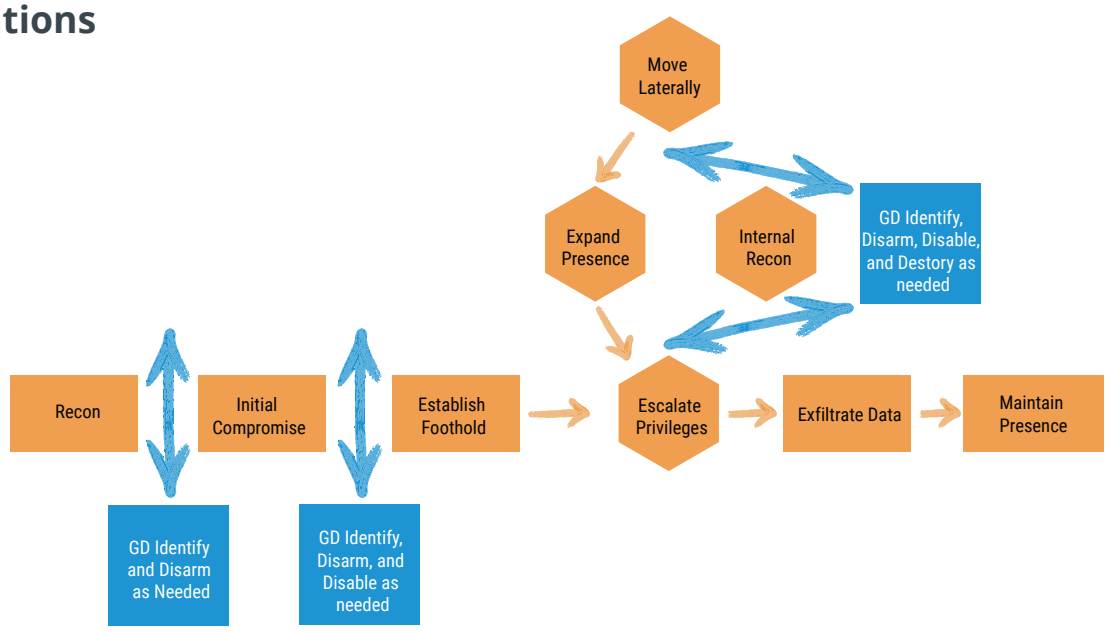
guardDog

Proactive versus Reactive

Artificial intelligence in passive defense methodologies has increased response times and efficiencies of currently existing methods. While this is an excellent start to react in near real-time automation, it is only once an exploit has escalated to a threat or an attack that these tools can appropriately respond. Methods vary for profiling threats or attacks, yet these threats and attacks indicate a host of other exploits that may be preempted in addition to the known and measured threats or attacks.

Compare this with proactive threat elimination and the ability to address and respond to threats or attacks before they even become threats through countermeasures designed for managing exploits by using exploits written specifically for exploits known and unknown to come. Through a proactive threat elimination type approach, we can eliminate the idea of responses in the first place.

AUTONOMOUS INCIDENT RESPONSE Technology Interrupts Recon and Escalations



AUTONOMOUS INCIDENT RESPONSE Technology interrupts at crucial stages of the attack and shuts down the attacker from impacting the network or devices on it. Through various IP techniques, AIR technology offers proactive response where attacks cannot be initiated by being identified as recon methods, initial compromises, and lateral movements stopped through strategic countermeasures that shut down attacks and attackers as needed. By interrupting automated systems, identifying and responding to all threats based on policy, AUTONOMOUS INCIDENT RESPONSE can mitigate threats before they can even assess any potential vulnerability available.