# THE DUAL DEFENSE OF CYBER SECURITY

**Cyber-attacks are able to take on many forms, but whether malware implemented by technology is the main method or a hacker gains command and control through a social engineering or phishing campaign, the antagonist is still human. Though innovating rapidly, technology alone cannot defend against these attacks. In order to defeat human opponents, a dynamic defense powered by a combination of human intelligence and cutting-edge technology is imperative.**

Pondurance understands the need to capitalize on human performance when it comes to thwarting off cyber threats of all magnitudes. In fact, this method is what sets us apart from the majority of Security Information and Event Management (SIEM) companies and managed security service providers (MSSP). These systems are able to detect early signs of risk, but they are unable to provide the thorough analysis required to see the threat clearly and assess the status. Pondurance's solution to this obstacle is our Threat Hunting and Response (TH+R) service.

Organizations of all sizes and industries need a team of agile cyber security experts who are able to stay one step ahead, safeguarding their data around-the-clock while simultaneously delivering an unparalleled level of personal attention. Through TH+R, our team is not taking over – we simply become an extension of our client's security teams, filtering through incidents ad averting the noise of false positives. We leverage technology combined with human interaction to offer robust dynamic defense, with included incident response. In order to fully augment the detection and response component of the Network and Log services, Pondurance made the decision to partner with Endgame to provide the necessary Host security services.

## TOP NOTCH HOST PROTECTION //

Endgame is a computer and network security company that provides a cyber operations platform for identifying and mitigating cyber threats of all proportions. Pondurance employs Endgame's Managed Endpoint Detection and Response (EDR) service to attain the utmost level of Host security. EDR is deployed prior to an attack to any endpoint and server within a client's network, allowing our team to reveal and remove any existing adversaries. Robust dynamic defense demands the application of the utmost protection within the most vulnerable of locations – the endpoints.

The endpoint uses tested mathematical models on the host in order to uncover and even avert malware. This mathematical approach halts the execution of hazardous codes, without requiring prior knowledge. Endgame's method has the capability to expose and quarantine over 99% of all malware within both open and isolated networks. While a SIEM or MSSP require consistent updates within their respective systems, Endgame's services stay ahead of the game by eliminating the need for continual signature updates. Pondurance remains confident with our choice to use Endgame because no other anti-malware product compares to the accuracy and overall effectiveness of their services. (add transition sentence into APOM incident)

## THE NEED FOR DUAL DEFENSE //

Organizations of all sizes across every industry are susceptible to cyber-attacks. Pondurance was contacted by a certain healthcare organization – who has asked to remain anonymous – that had a data breach occur within their network. After thorough digital forensics were conducted, it was evident that the hackers were able to retrieve access to this organization's internal network directly from the internet. A firewall ruleset was misconfigured upon implementation of a new firewall system a few years back, leaving a port exposed to the internet. This granted them access to every operating system connected to that network's domain, allowing them to execute their attack without any resistance. The attackers were even able to deceive the endpoint protection antivirus program this organization had in place, as this program was unable to recognize the malware that was being used.

Once the antivirus was deceived the actors were able to plant the ransomware on almost 400 internal servers, encrypting all of the server's files as well as deleting the back files. This particular type of ransomware makes it impossible to decrypt infected files without a private key that is held by the attacker and the deletion of the backups made it impossible for this organization to recover and restore the data on their own. While this organization experienced

temporary loss of accessibility to their data, there was no evidence of electronic protected health information (ePHI) exfiltration. After analyzing the digital forensics report, Pondurance was able to provide this organization with many recommendations to help ensure a tragedy such as this will not occur again.

## DUAL DEFENSE IN ACTION //

Since the unfortunate attack on this organization's network, Pondurance has implemented our Threat Hunting and Response service within their network. TH+R will allow them to keep detailed logs that will track all changes to firewall rule sets from this point forward. Recurring firewall audits are also necessary to assess and resolve any vulnerabilities, should they exist. This will prevent ports from exposure to the internet and significantly reduce the chances of a network being breached.

The augmentation of TH+R also entails a centralized logging solution that will greatly reduce the amount of time that is spent on analysis of the network's traffic. This logging solution will also enhance the overarching efficiency of this analysis. 24/7 monitorization of this log will also make it possible to catch similar attacks before or while they are occurring.

In addition to their role within TH+R, Pondurance and this organization were able to leverage Endgame to begin decrypting all of the infected systems. This organization also agreed to the implementation of Endgame's endpoint detection and antivirus solution within all of their infected systems. The execution of this software will make it far more difficult for actors to deceive or surpass these organization's endpoints. Dual defense involving the augmentation of software combined with human intelligence is imperative for maintaining the utmost level of cyber security within any organization's network.