deepwatch

Minimizing Ransomware Impact:

3 STEPS WITH MANAGED DETECTION AND RESPONSE

Introduction

Ransomware has increasingly risen as the top risk for CISOs and organizations around the world, dominating the cybersecurity trends over the last five years and fueling a new ransomware-as-a-service marketplace on the dark web, with crypto-currency used for the extortion.

Ransomware attacks have most recently disrupted serious targets, with devastating results, including loss of life. No target is safe. Organizations of every and any size, including governments, energy, hospitals, software companies, schools, transportation, and food production, have been attacked. According to security researchers, between February 2019 and March 2020, ransomware attacks increased by 148%. In the first half of 2021 alone, ransomware attacks have risen by an additional 93%.

The dangers of ransomware are apparent and repeatedly stressed by cybersecurity researchers, publications, and mainstream media: critical infrastructure is at risk, attacks are persistent, coordinated, and supported by large ransomware gangs and ransomware-a-service (RaaS) programs. Targets like schools, local governments, and hospitals are now considered “low-hanging fruit” by ransomware gangs. There is little doubt that nation states are also culpable, benefitting from the disruption caused by ransomware criminals who live within their borders and share intel.

Ultimately, though, statistics and stories are useless information in the face of the overwhelming threat to businesses. As

governments struggle with policy and solutions and cybercriminals adapt and grow more creative, businesses are simply trying to figure out what they can do to ensure they don’t become the next ransomware headline. **This ongoing business challenge is coupled with an additional bitter pill: there is no single solution or technology that is going to stop a ransomware attack.**

For a business of any size, the clearest path to maximize ransomware readiness is a comprehensive security program that focuses on three primary areas: prevention, detection, and response.

Ransomware **Realities**

The history of ransomware is well documented, dating back to the first attack with a floppy disk, encrypting victims' computers and demanding ransomware, back in the early 1990s. The volume of attacks has continued to increase year over year, demonstrating the desire of threat actors from around the world to extort as many victims as possible behind the veil of the internet. In recent years, however, the scourge of ransomware has taken a dramatic turn, with soft targets, like schools and hospitals, getting hit regularly. This is just one of the ways the ransomware threat is evolving; because the tactics are shifting, it's critical to understanding why and how businesses of every size and variety have suddenly become ground zero for attacks.

THE CRYPTOCURRENCY PROBLEM

Cryptocurrency and ransomware have often been referred to as a 'match made in hell.' Some argue that these fast-money, liquid, and virtually untraceable digital currencies bear a significant portion of the responsibility for the recent ransomware explosion. While some cryptocurrencies, like Bitcoin, can be traced to an extent, others, such as Monero, are anonymous, untraceable, and resist analysis, making them one of the perfect criminal currencies available.

The Vulnerability & Misconfiguration **Issue**

Hundreds of new vulnerabilities are discovered each month, and hundreds (if not thousands) more remain undiscovered. These vulnerabilities pose one of the most significant dangers to businesses since they are most often associated with common and everyday software and hardware applications used by business. To put the threat into perspective, a 2020 study from Forrester Research suggests that software vulnerabilities account for 42% of the most common attack vectors.

Open-source software and code is one of the biggest culprits of software vulnerabilities. While enabling teams to develop programs more quickly, open-source software is typically not written with security in mind. Worse yet, open-source software is sometimes intentionally tainted with malicious code. Additionally, application programming interfaces (APIs) present tremendous security challenges, as threat actors regularly compromise vulnerable APIs through unsecured endpoints.

Vulnerabilities are also presented in the form of misconfigurations. Incorrect permissions, the use of default usernames and passwords, and improperly configured network security all contribute to ransomware attack vectors. Cloud security is also targeted; recent cybersecurity research by Palo Alto Networks revealed that 65% of publicly disclosed cloud security incidents were the result of misconfigurations.

All of this means that no software, application, or endpoint is going to be vulnerability free, increasing the likelihood of attack.

Ransomware: **Data Loss and Death**

When it comes to ransomware, businesses tend to think of only the hassle of encryption and paying a hefty ransom. Unfortunately, the problems with ransomware go much deeper and are beginning to cost people their lives.

Hospitals and health centers are considered low-hanging fruit for most cybercriminals because they provide critical services 24/7. These services may be also protected by disparate or out-of-date cybersecurity technologies. Unfortunately, despite what they may publicly proclaim – it's clear that cybercriminals care nothing for the literal life and death issues at stake during a ransomware attack on a hospital or health center. Recent attacks on major health centers have resulted in the postponement of surgeries, the redirection of emergency vehicles carrying critically ill patients to other, less-convenient hospital locations, and even death.

A 2020 ransomware attack on a hospital in Germany resulted in the death of a woman with an aortic aneurysm, since the emergency vehicle that was carrying her was forced to reroute to a hospital 20 miles further away; this delayed the patient's treatment by at least an hour. The intended hospital, located much closer, had to shut emergency services down due to a ransomware attack.

Sophisticated Threat Actors & Malware Make it **Difficult for Security to Keep Up**

The days of significant threats originating with script kiddies are long gone. Most threats today originate with highly trained, experienced, and sophisticated threat actors, often operating with the support of nation states or skilled crime gangs.

It would also be incorrect to portray threat actors as lacking business acumen. Today's big cybercriminals stay up to date on the latest cybersecurity research. They track vulnerability announcements (also known as Common Vulnerability and Exposures or CVEs), and often have exploits ready within hours or days of the CVE publication. These sophisticated threat actors also market their wares through ransomware-as-a-service (RaaS) models, offering ransomware in a software-as-a-service (SaaS) format via monthly subscription, affiliate programs that include a percent of the profits, one-time licensing fee, or a full profit-sharing scenario.

In addition to displaying a shrewdness for business, ransomware operators also possess expertise in developing malware that is good at evading security products. Threat actors obfuscate code, sign the ransomware with a legitimate authentication certificate, elevate privileges, and abuse stolen admin credentials to enable them to install the ransomware and move laterally within infiltrated networks and systems. When it comes to phishing email attacks, the requirements are more sophisticated. Typically, ransomware crime gangs are operating outside of the U.S., so they must hire a group of native-speaking experts to effectively phish. A successful phishing campaign that has the final objective of a ransomware attack includes a team of experts in InfoSec, IT, email security, graphic design, and writing to create something convincing enough for victims to click.

This combination of expertise, tenacity, and business acumen means that cybersecurity is always playing catch-up to the latest creative criminal trends. Organizations that rely on traditional signature-based tools and antivirus (AV) solutions are at particular risk since these tools are designed to identify known threats based on the threat's signature. Unknown threats or malware that has been designed to evade detection will easily get passed any signature-based AV system. In a recent Ponemon study, IT security professionals reported their current AV solutions missed 60% of attacks, while producing a high volume of false positives and alert overload. And while it is important for businesses to continually enhance and improve security, simply adding more security tools to the technology stack won't solve the problem.

RANSOMWARE-AS-A-SERVICE

Ransomware as a Service is the name of the affiliate model that is widely used to distribute ransomware and then extort large sums of money from victims. The criminal operation involves a few parties, including the Initial Access Broker, who works with an Affiliate, who then works with the RansomwareOperator.

- Initial Access Brokers look for companies that are vulnerable to a variety of things. Often they use similar techniques across a large number of companies, such as on-premise exchange servers, RDP, etc.
- The Initial Access Brokers then sell the access to an Affiliate, who then proceeds to compromisethe company.
- The Affiliate works closely with the Ransomware Operator. Upon compromising a company and detonating the ransomware, the Affiliate then passes the data and description key to the Ransomware Operator.
- The Ransomware Operator then works to extort the victim/exploited company. Double- and triple-ransomware threats may be used to get the victim to pay the ransom.

Double- and Triple-Extortion Ransomware
Cybercriminals engaged in ransomware attacks want to maximize the likelihood that the victim pays the ransom, so they've recently taken to engaging in what is known as double- and triple-extortion attacks.

Double-Extortion Ransomware
In a double-extortion attempt, in addition to locking or encrypting the data, threat actors will also steal the data and threaten to post it on the dark web, sell it to other criminals, or market it to the victim's competitors, unless the ransom is paid.

Triple-Extortion Ransomware
In a triple-extortion attack, the criminals engage in all the behaviors described above, but also use the information stolen in the attack to contact the victim's customers or clients and try to extort money out of them, under threat of sensitive data release.

Ransomware Costs Businesses **Millions**

The cost to remediate an attack has also risen dramatically, doubling between 2020 and 2021. The 2021 Verizon Data Breach Investigations (DBIR) report suggests that the average cost to business in 2021 for a ransomware attack can be as much as $1.16 million per attack. And while cyber insurance certainly offers a meaningful benefit to companies, cyber insurance premiums are skyrocketing (currently up 40% in 2021 on top of an estimated 46% increase in 2020). According to the credit rating agency AM Best, ransomware accounts for 75% of all cyber insurance claims within the United States, causing insurance professionals to warn that claims are outpacing premiums, and recent price increases don't reflect the significant risk posed by a catastrophic cyberattack event. Moreover, threat actors engaged in ransomware attacks openly tout their attraction to businesses that use cyber insurance, considering them "the tastiest morsels," to quote one REvil ransomware gang member. These issues have led some experts to argue that cyber insurance actually incentivizes cybercrime activity.

By comparison, the return on investment (ROI) for ransomware prevention can be substantial and far outweighs the cost of an attack. For example, according to research conducted by deepwatch, investing in a comprehensive security program that includes cyber resilience and preventative tools such as threat analysis, security orchestration, automation, and response (SOAR), logging and alerting data, and data breach avoidance solutions can save a business millions in breach costs.

The Three Key Components of **a Comprehensive Security Program**

While ransomware attacks may be inevitable, this doesn't mean that every organization will be attacked. Ransomware attackers will exploit any type of security hole—from vulnerabilities and misconfigurations to poorly trained users and inadequate security planning and management. Those organizations best able to remediate attack will be the ones that understand the risk and invest in three primary security areas: prevention, detection, and response.

Reduce the Risk of Ransomware with these Strategies and Approaches

#1 Prevention Strategies

Despite the countless news articles and headlines about ransomware, attacks still seem to take some companies by surprise. Often organizations that suffer a ransomware attack become easy victims because they lack some basic preventative security hygiene measures. Preventative security involves the following strategies, techniques, and policies to protect the integrity of an organization's data, the enterprise, the cloud, and assets.

Data Governance & **Backups**

Data Governance — Data governance is all about the planning, monitoring, oversight, and control of data as it moves through the data lifecycle, from capture to storage to disposal. It involves using a framework to define who may access the data, who has control over the data, and how the data may be used. Essentially, data governance is about access, accountability, and actions. As a line of defense, data governance plays a critical role in minimizing ransomware risk. By making data governance a priority in a security program, businesses can help better understand what data needs to be protected and how to protect it. Data governance policies help to:

- Define which data may be at risk
- Document the location of sensitive data
- Identify individuals that have access to sensitive data
- Ensure data is accessed in a consistent and appropriate manner

Backups — Organizations need to engage in regular data and system backups and ensure backups are stored on a system that is separate from other network systems to prevent an attacker from moving laterally and encrypting or stealing backup files. Should a ransomware attack happen, having safely stored and recent backup files available can potentially save organizations from having to pay the ransom.

Training & Assessments

Security Training — Organizations that require mandatory security awareness training for all employees can significantly reduce ransomware attack risk by making staff aware of the types of threats that come through email and the importance of credentials and access privileges. Training ensures that individuals that have access to organizational systems and assets understand and apply cybersecurity best practices to their daily work environment.

Security Assessments — Security assessments involve reviewing and analyzing an organization's cybersecurity controls and their ability to manage and remediate vulnerabilities. Assessment processes include identifying vulnerabilities and misconfigurations, examining controls, scrutinizing compliance, scanning assets, looking at dependencies, measuring potential attack impact, and recommending solutions to close any security gaps. Security assessments can help an organization determine the extent to which they are prepared to defend against an attack. Assessments are often based on cybersecurity frameworks, such as NIST.

Email Security & Other Security Technologies

Email Security — Email security has been around for a while, but its premise – to scan emails and attachments and block anything that appears to be malicious – still serves an extremely important role in the fight against ransomware. In fact, according to 2020 research, spam and phishing emails are the most common delivery method for ransomware infections worldwide, accounting for more than half (54%) of all attacks. Email security is an absolute necessity for any business. Solutions may include such things as threat intelligence, sandboxing, a secure email gateway, machine learning, data loss prevention, encrypted email, and protection from malicious attached links.

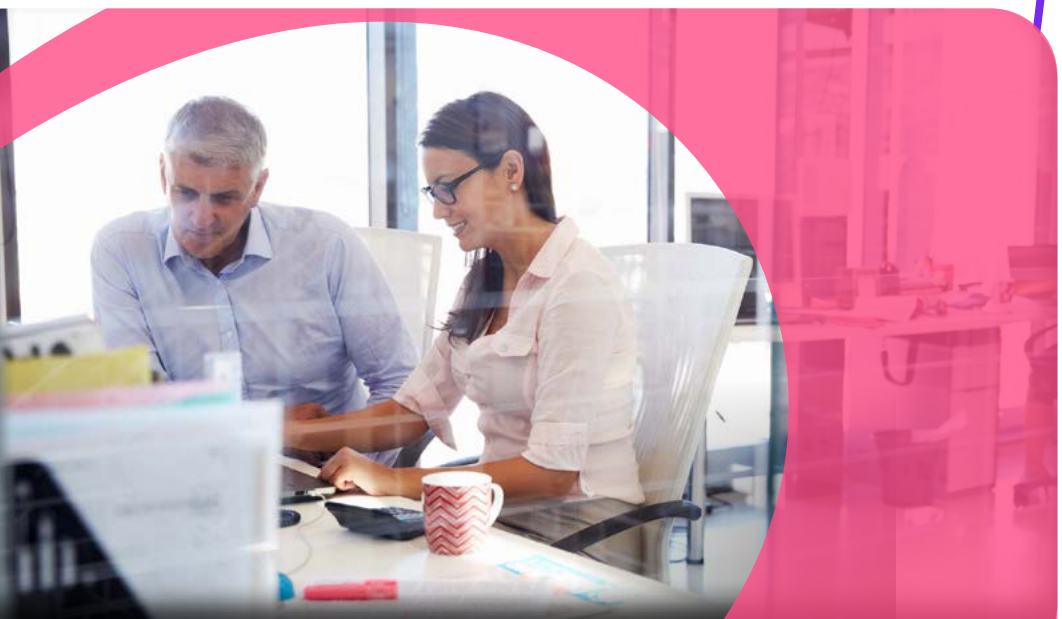
Network Segmentation — Network segmentation separates the network's architecture into individual and isolated sections to prevent lateral movement should the network be breached.

Intrusion Protection System (IPS) — IPS technology responds to a potential threat by blocking malicious network traffic or the user or intruder from accessing systems.

Firewalls — Firewalls shield networks and devices from malicious or extraneous internet activity.

Vulnerability Management

The management of vulnerabilities through ongoing identification, reporting, management, and remediation helps to prioritize threats and minimize the attack risk associated with weaknesses affecting endpoints, software, workloads, and systems. Because managing threats is a reactive process, in which a threat must be actively present, vulnerability management aids the detection process by identifying and mitigating vulnerabilities and closing security gaps before threat actors can leverage them.



Identity and Access Management Methods

Identity and access management (IAM) encompasses the technologies, processes, strategies, and policies associated with determining which users should be given access to corporate assets (identity management) and managing the level and circumstances of access (access management). IAM includes strategies and technologies such as identity governance, IAM solutions, and identity management systems. Identity and access management solutions enable organizations to:

- Corroborate a user's identity
- Delineate a user's role
- Determine the user access level
- Manage access conditions
- Observe, track, and report on user activities
- Enforce corporate policies and government regulations
- Protect assets from threats and attackers.

Multi-factor Authentication (MFA) — Multi-factor authentication requires a user to login to a system, device, network, or application using one two or more different identity components, such as something the user knows (e.g., username and password) and something the user is or has (e.g., token, fingerprint, facial recognition). MFA provides protection from ransomware attacks by reducing the risk that an unauthorized individual could gain access.

Least Privilege — Least privilege limits user access based on the minimum needed to conduct business operations. Least privilege helps to prevent lateral movement between systems and networks should a user's credentials become compromised.

Reduce the Risk of Ransomware with these Strategies and Approaches

#2 Dectection Strategies

Threat detection is about understanding and analyzing the types of threats that are targeting business systems, networks, and devices. Detection technologies and methods are designed to operate quickly and efficiently before a threat can infiltrate and do significant damage. Threat detection helps to prevent delivery of a ransomware payload, by looking for both known and unknown threats using the following tools:

Endpoint Detection and Security

Endpoint detection and security offers benefits such as continuous alert monitoring, validation, automation, containment, escalation, dashboards, and reporting.

Threat Hunting

Threat hunting involves proactively searching networks, systems, devices, and endpoints to identify unusual or suspicious activities using manual and software-assisted techniques and determining if there are any threats within the environment that may have evaded detection with standard cybersecurity tools.

THE VALUE OF HUMAN EXPERTS FOR ML & AI INNOVATION

Machine learning (ML), artificial intelligence (AI), and automation are critical components of any comprehensive cybersecurity program. However, advanced technology still can't fully compensate for the skills and expertise that an experienced cybersecurity professional can bring to detection and response activities.

For all the benefits of AI and automation, it still requires human knowledge and experience to build the data systems and populate key data elements such as ransomware codes and malware anomalies. In addition, should a cybercriminal breach a system, AI is still susceptible to manipulation, making human intervention critical and necessary.

Security Information **and Event Management (SIEM)**

A SIEM combines information and event management to provide real-time alerts and indicators of compromise.

Threat **Hunting**

ML and AI play a critical role in cybersecurity by providing automated solutions to threat intelligence, data monitoring, big data analysis, anomalous behavior and fraud detection, incident response and forensics, and as an enhancement to human analysis.

Reduce the Risk of Ransomware with these Strategies and Approaches

#3 Response Strategies

A comprehensive ransomware readiness approach also includes response and remediation strategies, which address security incidents as they are underway to help significantly minimize an attack's operational and cost impact and gather critical attack information.

Incident Response

Endpoint detection and security offers benefits such as continuous alert monitoring, validation, automation, containment, escalation, dashboards, and reporting.

Attack Planning and Tabletop Exercises

Attack planning and tabletop exercises facilitate a hypothetical discussion of an attack scenario using the organization's current policies, strategies, plans, and technologies. These exercises are designed to provide an organization with an improved understanding of their strengths and weaknesses. Planning and exercises also help businesses make needed changes to policies and response plans.

EBOOK

5 PHASES OF COORDINATED
INCIDENT RESPONSE TO RANSOMWARE

Recovering from ransomware is a process that is heavily dependent on the preparation an organization does prior to an attack, and often long before the attack has happened. In addition, should a cybercriminal breach a system, AI is still susceptible to manipulation, making human intervention critical and necessary.

Download Now

Response Technologies and Services

Two key response approaches are managed detection and response (MDR) and endpoint detection and response (EDR) services. When combined, they extend the organization's overall detection and response capabilities.

Remediation

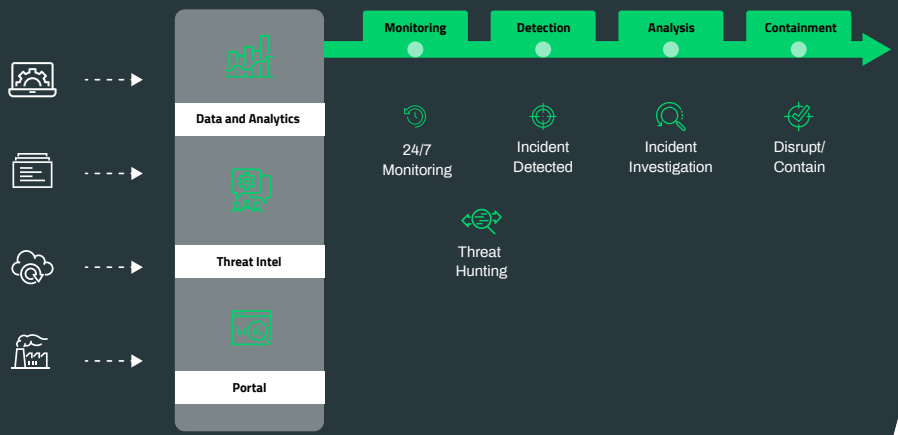
Remediation solutions isolate impacted devices and systems, remediate unauthorized changes, and mitigate the tactics, techniques, and procedures (TTPs) used by the threat actors. Remediation also serves as a roadmap to improve current and future security gaps.

Using Managed Detection and Response (MDR) to Implement the **Three Key Components of a Comprehensive Security Program**

Managed Detection and Response helps organizations:

- Gain greater visibility and active detection and response. MDR partners can correlate and detect attacks across millions of transactions along with active threat hunting to identify sophisticated attacks.
- Augment the in-house team with security experts and expertise to help fully staff & retain security operations center (SOC) resources faster.
- Do more with existing solutions to improve ROI by maximizing the value of your existing tools.
- Integrate seamlessly with enterprise SEIM, vulnerability management, and active response.
- Optimize security investments and gain network effects from wider customer base & threat research.

SCOPE OF MDR SERVICES



Why Managed Detection and Response **Matters Now**

THE MDR EVOLUTION

Managed detection and response solutions provide businesses with all the comprehensive security tools and processes described earlier, without the businesses having to invest in extensive technologies or expensive and hard-to-find staff.

MDR is the next step in cybersecurity managed services, since it not only includes security monitoring and management, but also critical investigation and remediation services. MDR services include comprehensive technology stacks that protect endpoints, networks, cloud services, operational technology (OT)/Internet of Things (IoT) and other resources. MDR also offers monitoring, data collection and analysis, threat intelligence, automation, and deep manual analysis by experts experienced and skilled in detection and response.

The benefit of the more-comprehensive MDR approach is that already overburdened internal IT staff do not have to worry about managing the often-tedious process of identifying threats and engaging in incident response activities. Managed detection and response services include critical threat discovery and mitigation and remediation functions that necessitate expertise from professionals who can investigate threat alerts, see network anomalies, detect privilege escalation, and identify lateral movement toward the domain controller.

Ultimately, a managed detection and response provider offers significantly lower-cost cybersecurity services and all the benefits of a security operations center (SOC) without having to worry about the cost, time, and staff having to build a SOC on premise.

With the threat landscape evolving rapidly, MDR matters more than ever, offering an immediate and comprehensive solution to threat challenges.

How the Right MDR Provider **Can Minimize Ransomware Impact**

No cybersecurity preventative measure is going to be full proof. Threats will slip through, so managed detection and response takes up where prevention leaves off, offering rapid, coordinated, and automated services to stop attacks from achieving their final objective or to minimize the overall impact an attack has on an organization.

- An experienced and customer focused MDR partner can help diminish the impact of ransomware by providing:
- 27x7x365 monitoring of the environment by experts.
- The right SIEM technology is deployed to collect massive volumes of data in real-time, detect advanced attacks, and raise alerts about anomalies such as insider threats and other hard-to-detect use cases.
- An integrated endpoint detection and response (EDR) solution that identifies malicious files and activity based on the attributes of known malware.
- Detection of ransomware behaviors with indicators of attack and prevent rapid encryption of files before it takes hold.
- Risk management by proactively hunting for indicators of compromise to identify attackers and files with ransomware payload.
- Capabilities to notify stakeholders and isolate affected endpoints to contain threats and roll back any unauthorized changes with expert guidance.
- Risk management strategies to help improve the security posture on a continuous basis.

deepwatch

ABOUT DEEPWATCH

Deepwatch helps secure the digital economy by protecting and defending enterprise networks, everywhere, every day. Deepwatch leverages its highly automated cloud-based SOC platform backed by a world class team of experts who monitor, detect, and respond to threats on customers' digital assets 24/7/365. Deepwatch extends security teams and proactively improves cybersecurity posture via its Squad delivery and patented Security Maturity Model. Many of the world's leading brands rely on Deepwatch's managed detection and response security.

Visit www.deepwatch.com or reach out to us at sales@deepwatch.com.

Conclusion

Increasing ransomware attacks and their evolving sophistication make MDR services more critical than ever. The technology and staffing requirements needed to run in-house cybersecurity operations make it infeasible for most businesses, rendering MDR services necessary to successfully securing any business environment. According to a Ponemon study in 2020, one of the best ways to minimize the impact of ransomware is to use a managed security service provider (MSSP) to help close the security skills gap. However, not all MDRs and MSSP providers are created equal. Selecting the right MDR partner like deepwatch who can not only detect and respond to ransomware threats but also help improve security posture to mitigate future risk is critical to improving cybersecurity operations.

About Deepwatch's Managed Detection & Response Services

Deepwatch is a trusted security leader, offering professional and innovative managed security to help stop breaches and attacks. Deepwatch's managed detection and response services include 24/7/365 threat monitoring, alerting, validation, and proactive threat hunting, with accelerated detection of malware, botnets, and ransomware behavior aided by industry's most comprehensive and fastest platform built with machine learning and content libraries. At Deepwatch, organizations work with a named squad—an assigned team of experts that includes detection and response analysts and threat hunters who take time to understand a business's unique environment.

From economies of scale, network effect and technology, and personnel savings, with Deepwatch's MDR solution, customers have realized greater than 450% ROI per year on average. Moreover, through real-time squad collaboration and engineering refinements, customers on average see 40%+ improvements in security maturity every year.