deepwatch™

3 Steps to Improve Cyber Resilience Against Ransomware

How Managed Detection and Response Partnerships Can Reduce the Impact of Attacks

www.deepwatch.com

Table of Contents

Introduction

Ransomware attacks are a top risk for CISOs in virtually every industry. While this type of malware attack has been around for a while, its nature changed in 2019 when threat actors moved beyond merely holding computers and networks hostage and started stealing the sensitive data they contained to sell on the dark web, often infecting and compromising backups in the process.

Today a ransomware-as-a-service (RaaS) ecosystem exists to make it easier for hackers to successfully execute attacks. According to Verizon's 2023 data breach report, ransomware is still considered a top 3 threat concern for businesses, and it is present today in more than 62% of incidents, with 59% having financial motivation. The annual global cost to ransomware victims is expected to rise to $265 billion by 2031.

The damage a ransomware attack can inflict on an organization goes far beyond lost or stolen data. Lost revenue, damaged reputations, and remediation costs often tally up to $2 million or more in damages for victims of an attack. To minimize the impact of a ransomware attack, organizations must increase their visibility into networked environments, harden defenses through vulnerability management, and create coordinated plans for recovery–all as part of a program to improve cyber resilience.

Cryptocurrency's Role

Ransomware would not be possible without the existence of cryptocurrency.
While some cryptocurrencies, such as Bitcoin, can be traced to an extent, others, such as Monero, offer additional anonymity features, making them nearly impossible to trace. Organizations must understand the role of cryptocurrencies in ransomware, and may even choose to acquire Bitcoin as part of their recovery strategy.

While many victims pay ransoms, the number of victims that pay is declining.
According to Covenware, a ransomware response company, just 41% of ransomware victims in 2022 paid a ransom, compared with 50% in 2021, 70% in 2020, and 76% in 2019.1

The **Vulnerability and Misconfiguration** Issue

Hundreds of new vulnerabilities are discovered each month, and hundreds (if not thousands) more remain undiscovered. These vulnerabilities pose the most significant dangers to businesses since they are most often associated with common, everyday software and hardware applications utilized across the enterprise.

Open-source software and code is another 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 can also manifest 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.

Ransomware **Realities**

Catastrophic Consequences

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 and are therefore more likely to pay a ransom. In an ironic twist given their vital importance, healthcare organizations routinely rely on disparate or out-of-date cybersecurity technologies. 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.

According to a 2022 report from Sophos, successful ransomware attacks can take up to a month or longer to fully remediate, with remediation costs averaging at $1.4 million.

SOPHOS, 'THE STATE OF RANSOMWARE 2022'

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

Most threats today originate from highly trained, experienced, and sophisticated threat actors, often operating with the support of nation states or skilled criminal gangs.

It would also be inaccurate 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 easily install ransomware and move laterally within infiltrated networks and systems.

When it comes to phishing email attacks, the requirements are more sophisticated. Ransomware crime gangs typically operate 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.

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. RaaS criminal operations typically involve a few parties, including the Initial Access Broker, who works with an Affiliate, who then works with the Ransomware Operator.

The Ransomware-as-a-Service 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 even greater 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 bypass 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 improve their existing security posture, simply adding more security tools to the technology stack won't solve the problem.

Ransomware **Costs Businesses Millions**
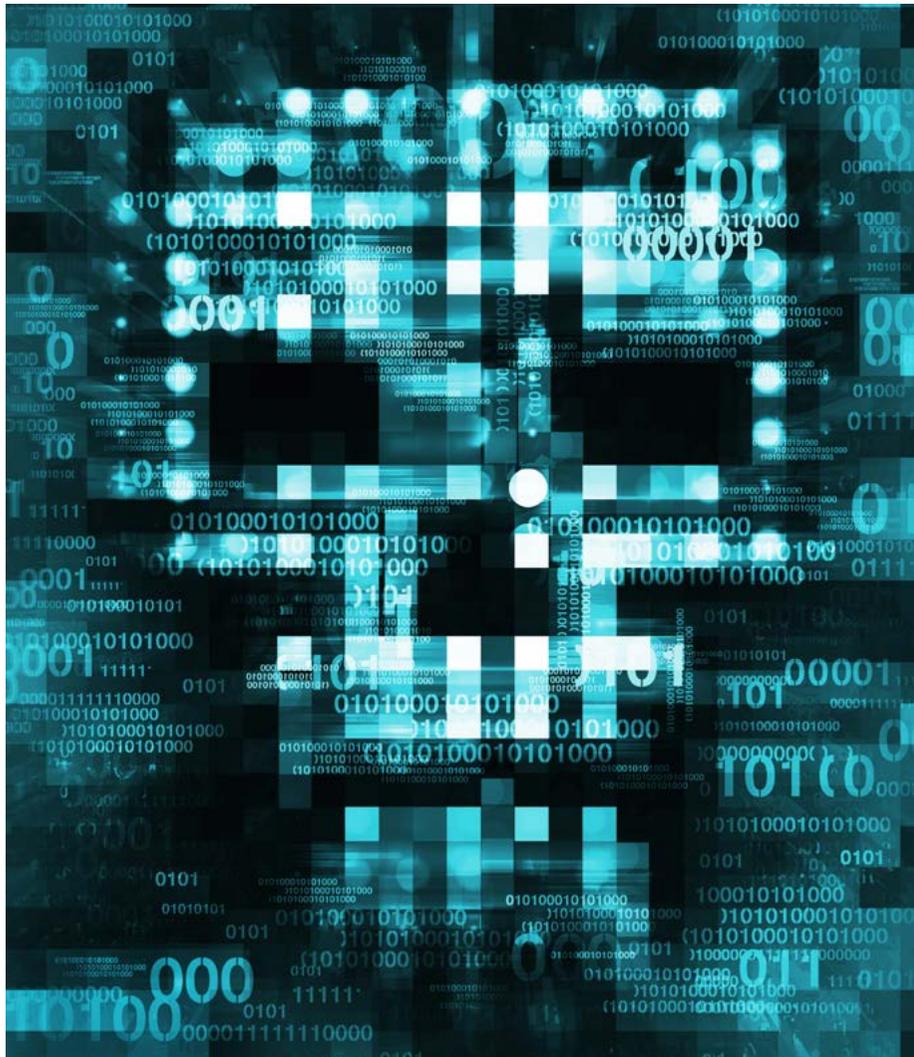
Cryptocurrency tracing firm Chainalysis reported that victims have paid ransomware groups $449.1 million in the first six months of 2023. The total victims paid in 2022 was just below $500 million. If the trend continues, 2023 would be the second biggest year for ransomware revenue since 2021, in which Chainalysis estimates $939.9 million was paid by victims.[2]

According to the IBM Cost of a Data Breach Report 2023, the global average cost of a data breach is $4.45 million. While a large majority of ransomware victims involved law enforcement (63%), those that did not paid 9.6% more, an average of $470,000, and experienced a 33-daylonger breach lifecycle.[3]

Three Key Components to Minimizing Ransomware Impact 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.

The average cost of a ransomware attack in 2022 —not including the cost of the ransom itself — was usd 5.13 Million, an increase of 13%.

$5.13M

-IBM, COST OF A DATA BREACH REPORT

# Three Key Components to Minimizing Ransomware Impact

Reduce the risk of ransomware with these strategies and approaches.

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.

01.

Prevention Strategies
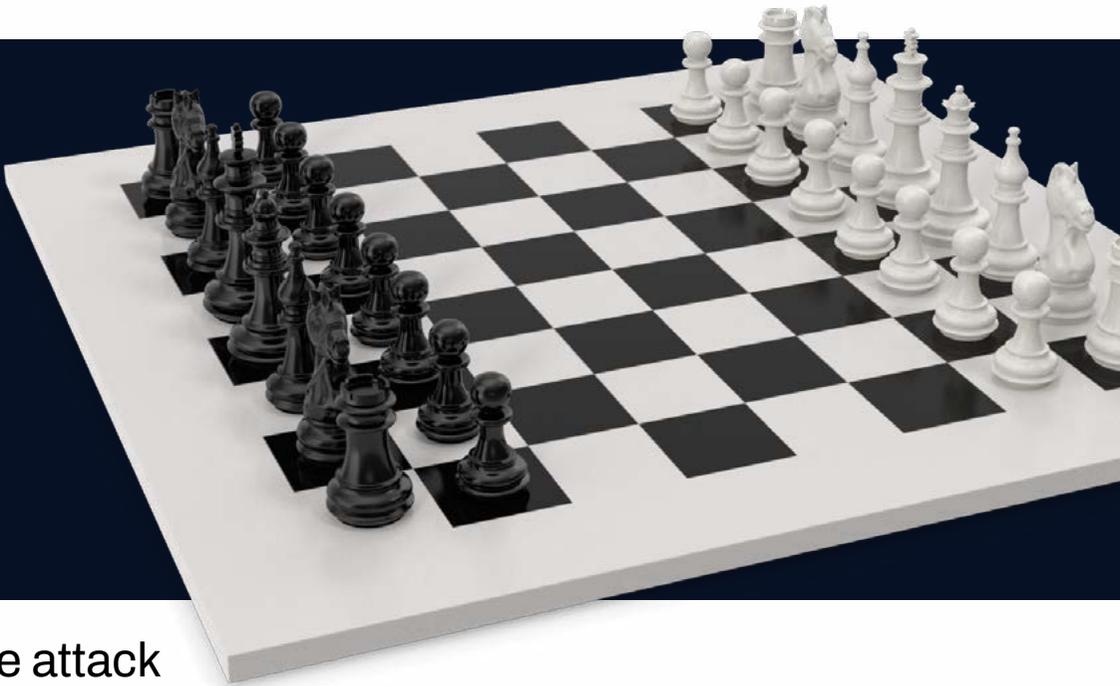
Often organizations that suffered a ransomware attack became easy victims because they lacked some basic preventative security hygiene measures. Preventative security involves the following strategies, techniques, and policies to protect the integrity of an organization's enterprise systems, user data, and cloud 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 how data may be at risk
- Determine where sensitive data is stored
- Identify individuals who 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 in a location 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 implement 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 along with the importance of credential verification and access privileges. Training ensures that individuals who 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 detect and remediate vulnerabilities. Assessment processes include identifying vulnerabilities and misconfigurations, examining controls, scrutinizing compliance, scanning assets, checking 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.

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, compromised users, or intruders 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 risks 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 a users 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 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.

02.

Detection Strategies

Strategies Threat detection is about understanding and analyzing the types of threats that are targeting your 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:
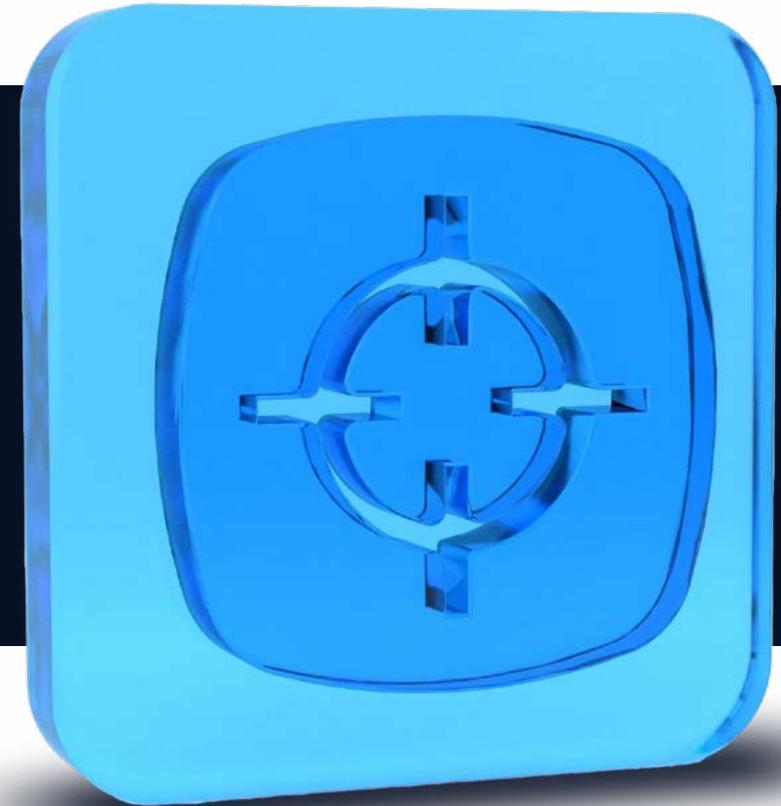
Endpoint Detection and Security

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 a critical necessity

Security Information and Event Management (SIEM)

A SIEM solution 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.

03.

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.
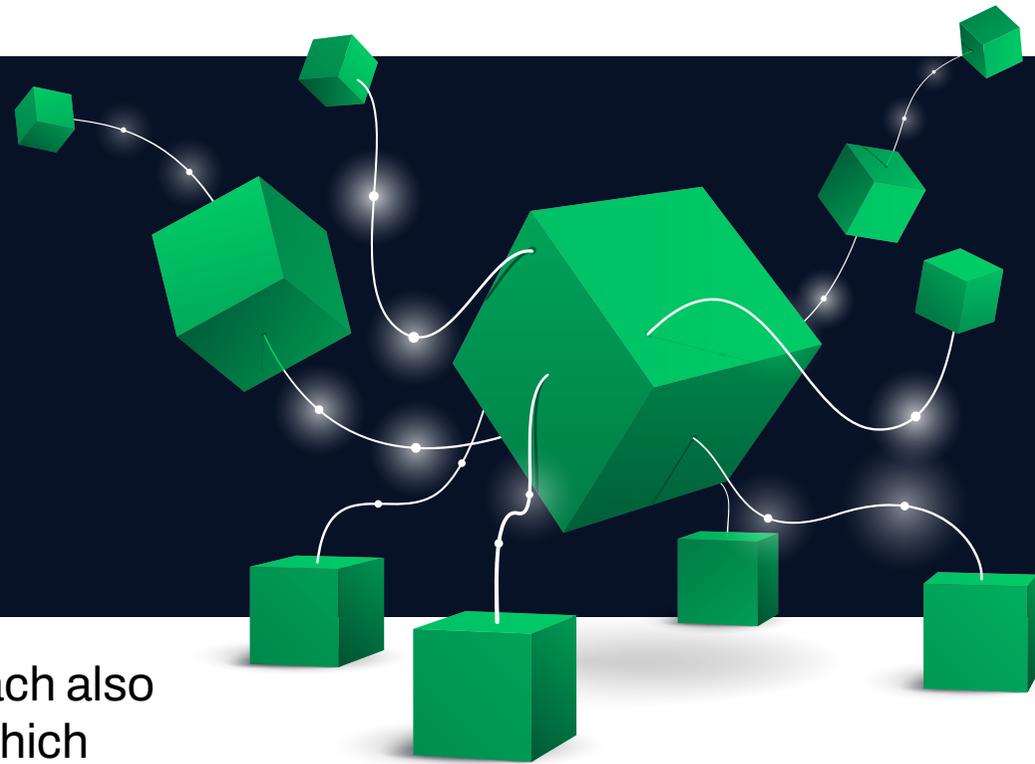
Incident Response

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.

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, roll back 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.

Data extortion techniques are expected to become even more sophisticated in 2023 as malicious actors develop and deploy "cloud-aware" ransomware that can compromise data even when it's moved off-premises into the cloud.

Trend Micro, 'Future/Tense: Security Predictions for 2023

How MDR Helps Implement the **Three Key Components of a Comprehensive Security Program**

Managed Detection and Response helps organizations:

- **Gain greater visibility into potential system vulnerabilities.** MDR partners can correlate and detect potential attack vectors across millions of transactions along with active threat hunting to identify sophisticated attacks.

- **Augment the in-house team with trained security experts** to help staff and deploy SOC resources as needed.

- **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 boost network performance** through a wider customer base & threat research.

Why Managed Detection and Response **Improves Cyber Resilience**

Managed Security Improves Resilience to Ransomware

Managed detection and response solutions provide businesses with all the comprehensive security tools and processes described earlier, without 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 capabilities. MDR services include comprehensive technology stacks that protect endpoints, networks, cloud data, 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 specifically trained in detection and response techniques.

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 SOC without having to worry about the cost, time, and staffing investments associated with building a SOC on premises. With the threat landscape evolving rapidly, MDR matters more than ever, offering an immediate and comprehensive solution to threat challenges.

How the Right Security Partner Can
Minimize the Impact of Ransomware

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:

- 24/7/365 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 that 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 payloads.

- 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.

The Deepwatch **Managed Security Platform**

We have engineered the most advanced threat detection platform available today. We offer advanced security technology, human-led security expertise, and operational processes to provide the fastest, most comprehensive managed detection and response service. Our 24/7/365 monitoring and response, advanced threat detection, and proactive threat hunting allow you to quickly react and contain security threats.

Conclusion

The frequency and complexity of today's ransomware attacks require more time and resources than most security teams have to fight them. Managed detection and response can help fill cybersecurity skills gaps, and provide faster response to ransomware incidents. As the leading managed security platform for the cyber resilient enterprise, Deepwatch helps teams identify risk, withstand and recover from successful attacks, and helps teams adapt their security programs to better prepare for novel or complex threats in the future.

Sources

- **"Ransomware Profits Decline as Victims Dig In, Refuse to Pay,"** Dark Reading, January 20, 2023

- **"Ransomware Attacks Are on the Rise, Again,"** Wired, July 12, 2023

- IBM Cost of a Data Breach 2023