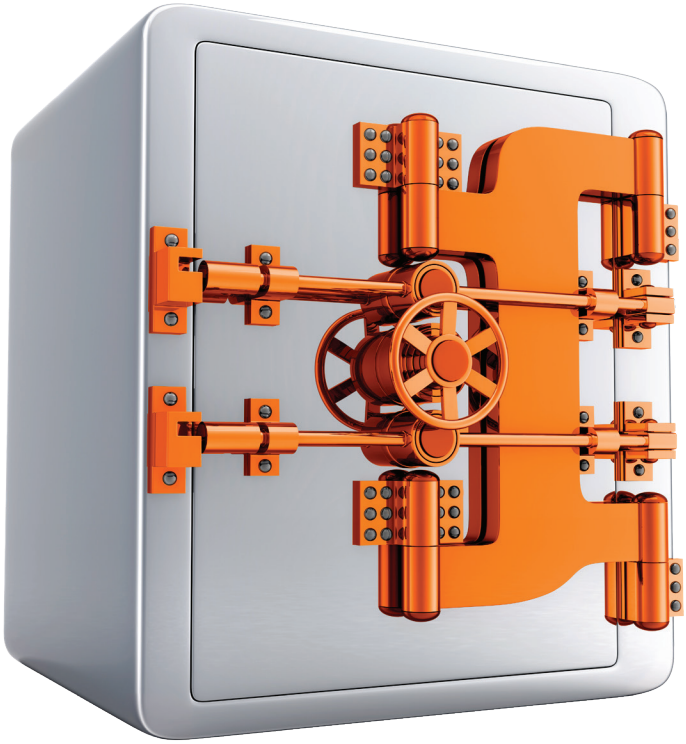

ARMOR

WHITE PAPER

MDR: BEYOND DETECTION AND RESPONSE

TABLE OF CONTENTS

INTRODUCTION

Organizations are finding it difficult to hire and retain security talent. At the same time, they face pressure to continuously upgrade their security infrastructure to stay abreast of the dynamic threat landscape. Managed detection and response (MDR) solves both problems by providing an external team of skilled security professionals and technologies to effectively and efficiently identify threats and help customers address these threats.

KEY TAKEAWAYS

- An increasing number of organizations are utilizing MDR solutions and this is forecasted to continue to grow rapidly.
- Organizations are leaning on MDR providers to help them navigate a complex cybersecurity space with increasing threats, high cybersecurity skills shortage, and countless security tools and vendors to manage.
- MDR providers vary in their expertise of different types of IT environments and their approach to addressing cyber threats.
- Armor not only detects threats, but also protects customer environments from threats whether they are on-premises or in public, private or hybrid cloud environments.

WHY IT AND SECURITY LEADERS NEED MDR

The spiraling advancements in both cyber threats and defenses has led to massive headaches for leaders responsible for protecting their organizations. Companies must continuously ramp up their investment in security functionality, but limited budgets mean that for each area of the infrastructure, they must select the technology that will best address the growing number of threats.

CISOs must also staff a security operations center (SOC) with expertise that is in high demand. Recent research indicates that the skills gap is worsening quickly, growing by 350% in eight years, from 1 million unfilled cybersecurity jobs in 2013 to 3.5 million in 2021[1]. The competition for talent has become a "full-on war," which inevitably ratchets up salaries and the total cost of running a SOC[2].

1 Cybercrime Magazine, "Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally by 2021," Steve Morgan, October 24, 2019.

2 The Los Angeles Times, "Cybersecurity pros name their price as data hacking attacks swell," Anders Mellin, August 7, 2019.

These challenges are exacerbated in organizations with significant compliance requirements. For example, retailers must abide by Payment Card Industry Data Security Standard (PCI DSS) rules, and healthcare organizations must comply with the Health Insurance Portability and Accountability Act (HIPAA). Other industries face their own security-related regulations. In addition, all businesses have data privacy compliance requirements, such as Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Every IT leader must determine how to effectively secure their environments with the resources available. Then they and their compliance teams must prove to internal auditors and external regulators that they have done so.

As a result, many short-staffed SOC teams struggle to secure their organization's cyber assets cost-effectively. One recent study by ESG Research found that 82% of cybersecurity professionals believe that improving security posture as well as threat detection and response capabilities is a high priority for their organization[3].

At the same time, 76% of respondents to the same survey said threat detection and response is hard and getting harder. Their concerns include the dichotomy of the cybersecurity skills shortage and simultaneous growth in the volume and sophistication of threats, in the corporate attack surface, and in the security team's workload[4].

These and other reasons have led one ESG analyst to conclude: "Threat detection and response requires advanced skills that most organizations don't have. … It's abundantly clear to me that lots of organizations will throw in the proverbial towel and seek help from MDR players."[5]

WHAT IS MDR?

MDR is a managed-service approach to identifying and addressing threats in an organization's environment. According to the Gartner market definition, "MDR services offer turnkey threat detection and response via modern, remotely delivered, 24x7 security operations center capabilities and technology."[6]

The idea is that by leveraging the systems and expertise of a third-party MDR provider, CISOs can reduce security risks in their organization. They can access threat research and analysis, expert interpretation of the risks, and advice on mitigation—knowledge that would be difficult to hire and retain within the internal SOC. Moreover, because MDR is provided as a turnkey service managed by the third-party provider, it is fast to deploy, helping accelerate the maturity of an organization's security risk management.

3, 4, 5 CSO, "The growing demand for managed detection and response," Jon Oltsik, April 25, 2019.

6 Gartner, "Market Guide for Managed Detection and Response Services," Toby Bussa, et al., August 26, 2020.

All told, engaging an MDR provider can alleviate several challenges for the CISO, enabling the organization to invest less in its internal security operations and instead focus its attention and resources on its core business. It should, therefore, come as little surprise that "Gartner has observed a 44% growth in end users' inquiries [about MDR] during the past 12 months."[7]

THE ARMOR APPROACH

ARMOR'S APPROACH

- Hybrid and multi-cloud
- Protection to minimize threats
- Enterprise-grade products
- Compliance
- Secure and compliant hosting

Figure 1. Key findings from a Forrester Total Economic Impact study of Armor Anywhere

In August 2020, Armor was recognized as a Representative Vendor in the Gartner "Market Guide for Managed Detection and Response Services."[8]

Within the burgeoning market, Armor stands apart for its commitment to providing a holistic solution that combines security with compliance. This holistic approach expands the boundaries of MDR to include not only threat detection and response using multiple data sources, such as from Armor's enterprise-grade security capabilities, third-party security devices (ie. firewalls, endpoint security), and cloud-native environments (AWS, Azure), but also threat protection and consolidated security visibility across on-premises, private, public, and hybrid IT environments.

7, 8 Gartner, "Market Guide for Managed Detection and Response Services," Toby Bussa, et al., August 26, 2020.

> "The MDR services market is composed of providers offering 24/7 threat MDR services. They emphasize performing incident response functions and activities on behalf of the customer (e.g., acting like an extension of the customer's security team) across on-premises locations, remote assets, cloud services and OT/ICS environments. MDR services are designed to reduce the time to detect, as well as the time to respond to threats. They deliver customers the people, expertise, processes and technologies of a modern SOC in an easy-to-consume and standardized approach. Additional security operations functions, such as vulnerability management and log management, which are typically offered by managed security service providers (MSSPs), have emerged to complement the threat monitoring, detection and response offerings."
>
> — Toby Bussa, et al., Gartner[9]

In an IT landscape where most companies are running dozens, if not hundreds, of discrete cybersecurity tools, Armor consolidates oversight of those solutions into a single management console. With both internal and third-party threat intelligence, Armor identifies cyber threats, and—in concert with Armor's cybersecurity experts—supports customers in remediating those threats.

Companies that rely on Armor gain insight into what is happening in their environment, including which threats they are facing, where the threats are coming from, and how to minimize the impact to their organization. Acting as an extension of a customer's security team, Armor helps reduce the burden on security staff who may already be stretched thin.

9 Gartner, "Market Guide for Managed Detection and Response Services," Toby Bussa, et al., August 26, 2020.

Armor is uniquely equipped to serve cloud-native companies or those migrating to the cloud. Unlike most MDR providers, which come from a traditional, on-premises, network security or managed security background, cloud security has always been Armor's focus.

Many companies struggle to simultaneously manage the complexities of security and compliance. Recognizing this, Armor also offers an option to leverage their fully managed secure and compliant private-cloud infrastructure that includes, among other things:

- Latest infrastructure including network, storage, and compute
- Turnkey, robust, and integrated security and compliance controls across network and host
- Vulnerability threat management and patch management
- Disaster recovery and backup

By bringing all these capabilities together under one umbrella, Armor provides organizations better visibility into their security landscape. Leveraging Armor's expertise and technology to sift through large volumes of security findings enables a SOC team to focus on targeted inputs on issues that are important to their organization. This reduces security staff's alert fatigue and shortens the time they spend on security or compliance tasks. Taking advantage of Armor solutions enables a CISO to leverage Armor experts as an extension of their organization's security, freeing up their in-house resources to focus on what really matters to the business.

Armor has been recognized as a sampling of CWPP Providers in the July 2020 Gartner Report, "Emerging Technologies: Functionality Spectrum for Cloud Workload Protection Platforms (CWPP)."[10]

HOW ARMOR WORKS

Armor ingests security log data from a wide range of sources. It ingests logs from the enterprise-grade security tools integrated within the agent, from the organization's existing security systems and applications, and from public cloud security services, as shown in Figure 2.

10 Gartner, "Emerging Technologies: Functionality Spectrum for Cloud Workload Protection Platforms," Lawrence Pingree, July 2020.

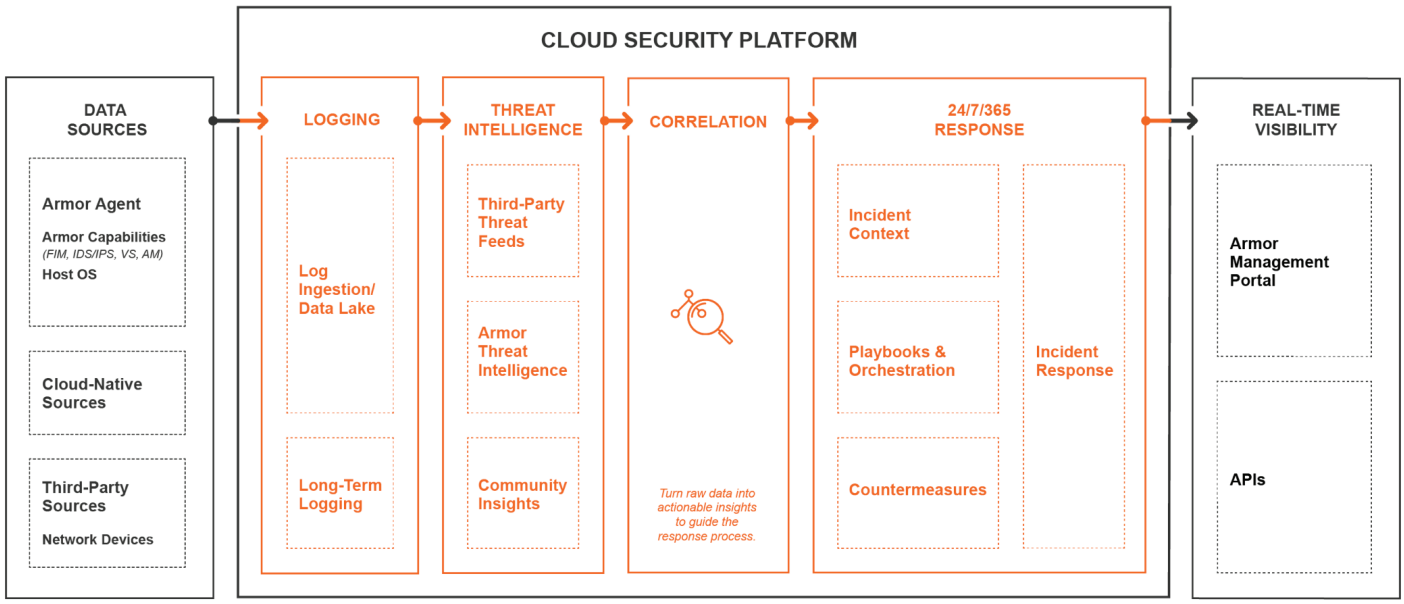

Figure 2. The Armor Anywhere architecture

The log data then flows into Armor's data lake. Leveraging built-in security information and event management (SIEM) capabilities, Armor automatically correlates the data received against both known and emerging threats from its threat research and third-party threat feeds.

Armor employs a threat research team that probes the dark web, analyzes its data lake, curates the threat intelligence, and examines investigation artifacts to uncover specific tactics, techniques, and procedures (TTPs) that may bypass conventional security products. These findings enhance the accuracy of threat detection across Armor's entire customer base.

All this information is analyzed and used to identify possible vulnerabilities and incidents. When appropriate, Armor's SOC team steps in to conduct second-level analysis. Armor also utilizes pre-built playbooks as part of its security orchestration, automation, and response (SOAR) platform in Armor Anywhere to automate response and provide remediations for customers.

> "One of the key reasons we host with Armor is that we want systems to be secure on multiple levels, from the application level, the SQL injection and WAF levels, to the network and protocol layer."
>
> — Tharak Krishnamurthy, CTO, VitalAxis[11]

11 Armor, "Finding HIPAA/HITRUST Compliance-Ready Cloud Security," 2020.

EFFICIENCY AND COMPLIANCE DIFFERENTIATES ARMOR

From an operational standpoint, Armor stands out in the fast-growing MDR market for its cost-efficiency. Many MDR providers rely heavily on human threat detection. While the judgment of internal experts is a crucial factor in Armor's MDR success, the incident detection and response team uses the automated correlation and analysis to greatly accelerate their activities. This means identifying an anomaly in log files requires fewer human resources, which saves money and accelerates detection for customers.

The accuracy of Armor threat detection also reduces its total cost of ownership (TCO). A recent study by Forrester found that across the millions of security events and data logs Armor analyzed, its false-positive rate was only 4% of all alerts.[12] This dramatically reduces the staff time that would otherwise be spent chasing false positives, both for the Armor team and within the customer's IT function.

Armor rapid and streamlined deployment further amplifies the staff time savings. Regardless of an organization's environment—in the public cloud, in a private cloud, hybrid IT environments, or hosted by Armor—Armor collects security data within minutes of installing the agent.

Armor Anywhere offers much more than a basic MDR solution, and at every stage of the threat detection and response process, Armor has been tuned to optimize efficiency. All told, Forrester found that Armor Anywhere's average ROI over three years is 774%.[13]

Perhaps one of Armor's most important differentiators is its tight integration of compliance capabilities into its solution. Armor provides an audit-ready compliance solution. It addresses certain compliance controls across different security and compliance frameworks and helps customers reduce the time and effort it takes to achieve an audit. In addition, Armor offers a cloud security posture management capability (CSPM). With this capability, Armor helps customers in public cloud environments manage their security posture and address accidental risks and misconfiguration against major security and compliance frameworks.

For healthcare SaaS provider VitalAxis, HIPAA compliance was a key factor in selecting Armor for its laboratory management and medical billing software. "We chose Armor because they understood HIPAA, understood cloud security and, most importantly, understood what was required to establish our solution as one hosted on a robust environment," says VitalAxis CTO Tharak Krishnamurthy.[15]

774% — average ROI over 3 years for companies that utilize Armor Anywhere.[14]

"We chose Armor because they understood HIPAA, understood cloud security, and, most importantly, understood what was required to establish our solution as one hosted on a robust environment."

— Tharak Krishnamurthy, CTO, VitalAxis[16]

12, 13, 14 Forrester, "The Total Economic Impact of Armor Anywhere," August 2020.

15, 16 Armor, "Finding HIPAA/HITRUST Compliance-Ready Cloud Security," 2020.

ARMOR MDR: LEADING SECURITY AT A LOWER TCO

Companies that are struggling to keep up with the resource requirements needed to confront the evolving cyber threat landscape need to consider Armor. Armor's security experts reduce the pressure to hire additional skilled cybersecurity staff. Armor also reduces operating expense by eliminating redundant point solutions and helping streamline compliance operations. Companies in the Forrester study reduced their overall security technology costs by 64%.[17]

With Armor, customers get an enterprise-grade protection at a lower TCO, retain control of their security experience, and have peace of mind knowing that Armor is detecting and helping them respond to threats across their environment.

For more information about Armor and the Armor Anywhere solution, visit armor.com.

To learn more about why an MDR platform is preferable to deploying individual point solutions, reference the 2021 Tag Cyber Security Annual at https://www.tag-cyber.com/advisory/annuals

17 Forrester, "The Total Economic Impact of Armor Anywhere," August 2020.

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167