Infocyte

Buyer's Guide

What to Look for in a Managed Detection and Response Solution

Contents

What is Infocyte

Infocyte is the platform for proactive cyber security.

Our technology enables the world's smartest security teams to detect, and respond to environmental vulnerabilities and sophisticated cyber threats across endpoint, data center, and cloud environments within a single pane of glass.

Large enterprises with a security operations center (SOC) leverage our platform to maintain compliance, reduce risk, and optimize security operations.

Small and mid-market organizations with no SOC, fewer technical resources, and smaller IT budgets, leverage Infocyte as a managed service, delivered through one of our partners, including some of the world's leading managed security service providers.

For our partners, Infocyte represents the fastest path for delivering cost-effective and flexible consulting services (i.e. compromise assessments and incident response) and ongoing Managed Detection and Response (MDR) services to their customers.

Status Quo

As business professionals, we're aware that the frequency of cyber attacks continues to surge...

Bad actors such as individual hackers, nation states and criminal networks use the latest cybersecurity weapons to achieve everything from political instability to the theft of funds, data, and identities.

Every IT asset in your environment — physical, virtual, and serverless — is a target. Workstations and servers are breached constantly by file-less malware and advanced persistent threats, and cloud infrastructures (i.e. hosts, workloads, containers and serverless infrastructures) are being attacked more and more.

Defense alone cannot win the fight against cyber attacks. As a result, Managed Detection and Response providers have emerged as an ideal solution for organizations that lack the tools, technology, and talent to effectively keep their environments clean and secure.

But, before selecting a Managed Detection and Response (MDR) provider, there are several things to consider. For starters, all MDR providers should be able to analyze data from endpoints, detect and respond to cyber threats, and generally strengthen your organization's security posture. But, there are stark differences between MDR providers, such as detection techniques and methodologies, the effectiveness of the MDR platforms they use — not to mention the cost and impact on your environment — and the speed at which these MDR security service providers can respond to incidents.

It's important to consider these differences, because each can have a significant impact on your overall cybersecurity strategy.

A Proactive Approach

Most organizations have at least one — if not many — prevention and defense technologies in place, such as firewalls, anti-virus (AV) software, and/or endpoint protection platforms. However, as industry experts and analyst firms agree, defense alone is not enough. Defensive cybersecurity tactics are only capable of preventing around 99% of known cyberattacks.

Proactive cybersecurity tactics, on the other hand, like asset discovery, vulnerability scanning, threat hunting, and incident response, actively expose and eliminate the 1% of cyber threats your defensive technologies are prone to miss, closing the gaps in your defenses.

Taking a proactive approach assumes three things:

1. You've been hacked and your environment (and endpoints) are compromised.
2. Attackers, using file-less malware, advanced persistent threats (APTs) and other sophisticated TTPs will breach your existing defenses.
3. Assets in your environment (physical, virtual, and serverless) cannot be trusted until proven otherwise and zero trust in your assets is both finite and fleeting.

Accordingly, you need a managed security solution that is capable of detecting advanced attacks and vulnerabilities, and one that enables your security team to effectively and efficiently address these security incidents. Further, your MDR provider should validate and conclusively certify your assets are "clean." This validation needs to be conducted on a periodic

basis (ideally automated) on-demand when needed and triggered in the case of dynamic cloud environments.

Please remember, not all detection methodologies and incident response tactics are created equal. Some have been around for years and require teams of highly skilled — and highly paid — forensic experts to gather memory dumps and analyze the raw data using techniques such as volatile memory analysis. This is where many small and mid-market organizations draw the line, coming to the conclusion that MDR services cost too much.

Unfortunately, these organizations — small and mid-market companies — are the ones who most need an MDR provider because they lack access to specialized (and expensive) people, tools, and technology to maintain a secure organization.

As a result, they often layer on an increasing number of defensive solutions. But, simply investing in more defensive solutions offers a false sense of security and leaves many organizations caught off-guard when a successful attack occurs.

EDR, AV, or UBA/UEBA?

To address cyber attacks, hidden threats and vulnerabilities, most MDR providers leverage Endpoint Detection and Response (EDR) platforms, Next-gen antivirus (NGAV) software, and/or User/Entity Behavior Analytics (UEBA/UBA) tools. As more businesses are learning, even these enterprise-embraced tools and time-tested approaches leave too many gaps — especially in complex and dynamic cloud environments...

These MDR platforms and tools may employ one or more of these detection methodologies:

1. **Threat Analysis** (individual malware scan of the endpoint)
2. **Data-centric** (monitor/analyze logs or behaviors)
3. **Network analysis** (monitor endpoint-related traffic)
4. **Forensics-based** (live memory extraction and analysis)

The underlying risks inherent in these different approaches are too important to ignore.

To give just a few examples, some AV engines and some EDR platforms with file-less and memory-based attack features typically only monitor the door to your memory (aka monitoring key API calls used in malicious injection) in order to prevent or detect the attack in "real-time." They do not actually analyze memory, which is almost exclusively handled offline via a third-party memory forensics tool, after a full physical memory acquisition.

In addition, some EDR platforms will monitor for changes to the most common persistence mechanisms, but do not offer capabilities to collect and hunt within the hundreds of possible locations. EDR platforms may also be limited to the EPP protection suite footprint, leaving gaps in coverage and potentially driving avoidable costs to get coverage across the environment.

As for UBA/UEBA solutions, their approach to detecting attacks is based on Big Data. The presumption is that all the data required for insight or intelligence is available, and that all you have to do is to analyze a huge volume of information, which can take weeks.

There are two problems with approaching cyber attacks from this data-centric angle. First of all, no data sets can be guaranteed to be complete. Secondly, there are data points that simply are not available because the available tools aren't specifically gathering that intelligence. This is because these solutions are incapable of collecting data from endpoints themselves. They rely on specific sources for data to analyze, including SIEMs, AV solutions, and other defensive security products.

As a result, MDR solutions leveraging UBA/UEBA tools may allow some sophisticated attackers to breach your environment undetected, as in the case of an advanced persistent threat (APT) or a prolonged and targeted cyberattack in which an intruder gains a foothold within an environment for an extended period of time, called dwell time.

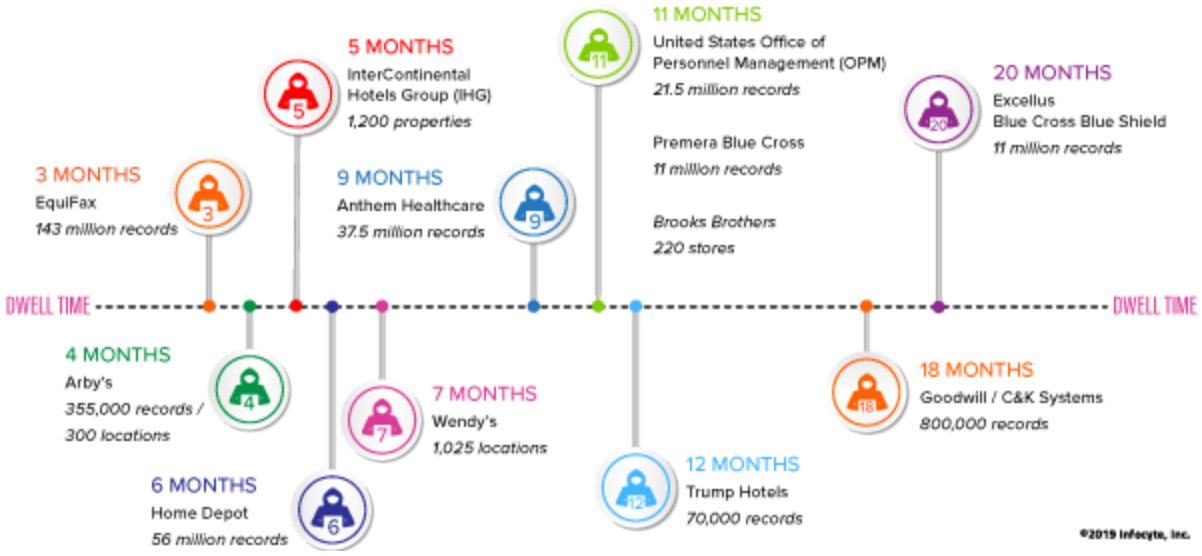

Image: infamous breaches and their dwell times

You should also keep in mind that UBA/UEBA solutions require either a number of experts (i.e. managed security services provider, internal/virtual SOC, security team, etc.) to manage them productively and/or a significant amount of specialized training, lifting the delivery cost of your MDR solution and putting it out-of-reach for some organizations.

Equally important to note, these data-centric approaches often take weeks to gather enough data for actionable results.

A better approach is to find an MDR provider that leverages an agentless, forensics-based platform — described in the next section — that can be deployed quickly and deliver meaningful results in near real-time.

Asset and Application Visibility

An important component of any cybersecurity strategy is knowing what assets and applications live within your environment — because your MDR provider can't possibly protect what they don't know exists.

There are several tools designed for asset discovery, identifying and cataloging the assets and applications on your network, but understanding these assets from a forensics context is of vital importance and often not inherently part of asset discovery tools.

Being able to enumerate the assets in your environment *and* gather meaningful data — OS, connection status and protocol, application footprint, and more — enables managed security teams to baseline a network, identify and classify assets and application data, flag vulnerable assets/applications, and use that data to streamline the delivery of your MDR solution.

Deep Analysis

The most effective method for addressing cyber attacks, threats, and vulnerabilities quickly and effectively is a hunting, detection, and incident response (IR) solution with deep analysis and forensics-based capabilities.

For example, Forensic State Analysis (FSA) assesses the health of an endpoint by validating what is running in memory at a given point in time. Asset discovery includes scanning networks to discover live hosts, servers, other assets, and the applications running on those endpoints, helping to identify vulnerabilities. While EDR and UEBA tools analyze logs of network-wide events and sensor data for malicious activity, FSA is a forensic approach to post-breach detection that assumes devices are already compromised and seeks to validate every endpoint is clean. The automation inherent in the Infocyte HUNT platform enables users to effectively deploy rapidly, dynamically, and at scale.

FSA does not rely on a host operating system to report real-time events. Instead, the solution examines executable memory space to reconstruct what is happening and collect anything of interest — such as injected memory, forensic artifacts, executable programs, modules, hooks and more. This data is then analyzed using a variety of post breach analytics techniques, as well as reputational, and multiple threat intelligence sources. Combining this live host forensic data and these analytic techniques, FSA determines the compromise state of endpoints.

ROI: Key Use Cases for an MDR Platform

When it comes to evaluating and selecting an MDR solution, knowing the capabilities (and limitations) of their MDR platform can help you make an informed decision.

Here are a few important use cases to consider for an MDR platform and managed security services provider.

Incident Response

Improving Incident Response (IR) readiness is the single most impactful way to reduce your organization's cyber risk. Your hunting/detection platform needs to include IR capabilities, so your team can either investigate, contain, eliminate the threats and vulnerabilities it finds, or be able to alert a support/security team to handle IR.

Unlike many IR tools, Infocyte HUNT leverages extensive automation — delivering actionable data rather than requiring manual work from the user. These automations, paired with Infocyte's ease-of-use and ease-of-deployment, allows almost any technical resource to configure, deploy, and use our platform.

Root Cause Analysis

A root cause analysis (RCA) tool can help IR teams trace the source of suspicious activity or identified threats across their environment. Properly designed, it should quickly correlate and combine the historical activity (events) of identified threats and malicious leads in the form of an activity timeline. This timeline includes events like file creation, file modification, process execution, and user login events.

These events are organized chronologically and combined into a single timeline, so incident responders can get a clear picture of how the attack started, where, and when — in addition to how it has evolved and moved laterally through your IT environment over time.

Compromise Assessments

Compromise assessments (CAs) need to quickly verify whether a network has been breached and quickly identify the presence of known or zero day malware and persistent threats — active or dormant — that have evaded your existing cybersecurity defenses.

Compromise assessments should validate everything currently running or scheduled to run on endpoints, and analyze each system's volatile memory to discover signs of manipulation or hidden processes. For speed and efficiency, the scans should be agentless and not require software to be pre-installed. Typically, the procedure should take just a few minutes to complete. In addition, the scans should be completely independent of the network's existing

security infrastructure and do not rely on a potentially compromised host opening system to deliver results.

Fast, lightweight and future-proof

For organizations of any size, an MDR solution should be fast, easy to deploy, and easy to use.

Along with these base requirements, the best MDR solutions should be "future-proof" with built-in scalability, a flexible architecture that supports integrations, multi-tier pricing and programs to accommodate the growth and evolution of your organization.

Speed can separate a good MDR solution from the *best* MDR solution. Threat detection and incident response technologies that can inspect thousands of nodes (individual assets) per hour are much faster than traditional, log-based tools that require massive amounts of data, and additional time to analyze that data (not to mention skilled technical resources to interpret and act on the findings).

In addition to speed, your MDR platform should be easy to use. This means easy for your MDR provider, plus internal IT administrators, in-house security professionals, and even executive stakeholders. Everyone from the top down should be able to use the solution, understand the value it provides, and interpret the data presented, with ease.

Beyond speed and ease of use, you need an MDR solution that will grow and age with your organization. Grow with product/platform enhancements and expand through integrations with other cybersecurity technologies like SIEM, orchestration an intelligence tools, and ITSM to further optimize security operations across your entire organization.

The solution should also have the capability of protecting client assets on the cloud just as clients now protect their on-premise networks, servers and workstations. In addition, the solution's architecture should support serverless assets, cloud workload protection and workload-centric security offerings that target the protection requirements of server workloads in cloud-based data centers.

An agentless platform, one which could interrogate and inspect your cloud-based architecture via API, can speed deployment by eliminating the need for pre-installed software — especially

with ephemeral instances and serverless assets. This simplicity in deployment and lightweight architecture can provide consistent visibility and control for physical machines, virtual machines, containers and serverless workloads — regardless of location.

Summary of Key Capabilities

Every organization is unique in its cybersecurity needs, resources, IT infrastructure, budgets and business goals. This list is not meant to be exhaustive, but when adopting a proactive approach to cybersecurity through an MDR provider, as recommended by industry experts and analysts alike, consider these capabilities:

Agentless Visibility

- Agentlessly gathers intelligence about your environment
- Enumerates the active assets and applications on your network
    - Physical (local and distributed) workstations, systems, and servers
    - Virtual machines and servers
    - Cloud architectures (instances, containers, and workloads)
- Identifies and stores hostname, IP, operating system and version
- Catalogs user accounts and identity-related data
- Inventories applications, version, advisories, and CVSS data

Proactive Threat Detection

- Finds known threats and unknown/unidentified threats.
- Hunts and operates independently of the host OS.
- Hunts within memory, with discovery and analysis of injected code, rogue threads, overwrites, hooks, and fileless malware via Automatic Memory Extraction.
- Hunts for persistence, collecting and analyzing triggers for dormant and time-delayed attacks or malicious commands.
- Hunts for historical infections, collecting and analyzing execution artifacts like shimcache, prefetch, etc.
- Hunts for vulnerable software, finding all installed software with known vulnerabilities and weaknesses.
- Hunts for non-compliant systems, using agentless asset discovery capabilities.
- Collects data for analysis directly.

- Gathers data from tens of thousands of endpoints per day.
- Identifies persistence mechanisms to discover attacks that are dormant or scheduled to run in the future.
- Strips identifying information about originating endpoint from data leaving the enterprise.
- Operates without installing permanent software.

Vulnerabilities

- Identify registry, running application and installed application vulnerabilities that exist in hosts, processes, modules, drivers and items resident in memory.
- Match against published vulnerability databases to identify new and emerging threats.
- Vulnerability engine that is capable of customizing rules based on CVE.
- Transformable scan results to match appropriately to results from vulnerability databases since vendors can be represented differently in vulnerability databases than they are in registries.
- Highlight and alert when vulnerabilities or indicators of compromise are present.
- Provide details of the vulnerability or compromised finding to aid in quick remediation.
- Score the vulnerability finding so that proper risk assessment can be made regarding the urgency of remediating the finding.
- Provide the ability to flag a vulnerability finding to identify actual problems versus false positives.
- Allow flexibility to whitelist or blacklist identified threats to reduce false positives.

Deep Analysis

- Determines the probability of unknown attacks running, in a manner that is clear and transparent to the user.
- Presents cross application communications (hooks).
- Completes endpoint analysis within minutes; large environments within hours.
- Functions outside a statistical model.
- Conducts volatile memory analysis.
- Gathers modules without inspecting the PE header or querying the host OS.
- Unmaps memory into native PE/ELF file structures for later analysis by vendors or other third parties.

Incident Response

- Certifies endpoints are attack and breach free — quickly and at any time — in support of incident response activities.
- Allows user to define, manage, and control dwell time — closing the breach detection gap.
- Circumvents attacker stealth techniques like automorphic malware, which attempt to thwart threat hunting and detection technologies.
- Provides the ability to conduct periodic reviews in a fast, easy and efficient way.

Learn More

Develop a proactive prevention, detection, and IR strategy with Infocyte.

Request an Infocyte proof of concept (POC) to ensure a full and successful evaluation of our platform and MDR service across your on-premise, hybrid, and cloud assets. Our MDR services are supported by our global network of partners, including some of the world's leading cybersecurity companies. Find out why Infocyte HUNT has been recognized as a leader in delivering cost-effective managed threat detection and incident response services by organizations like AT&T, Check Point Software, and PwC.

Request a live demo of our award-winning MDR platform at www.infocyte.com/demo

www.infocyte.com

About Infocyte

Developed by former U.S. Air Force cybersecurity officers, Infocyte's dedicated forensics-based MDR platform helps security teams discover the post-compromise activity of cyber attackers that have bypassed your defenses. The company's unique approach to security—a proactive approach—enables organizations large and small to control attacker dwell time, expose and eliminate hidden cyber threats and vulnerabilities to defend their networks, IT assets, and critical information from a data breach.