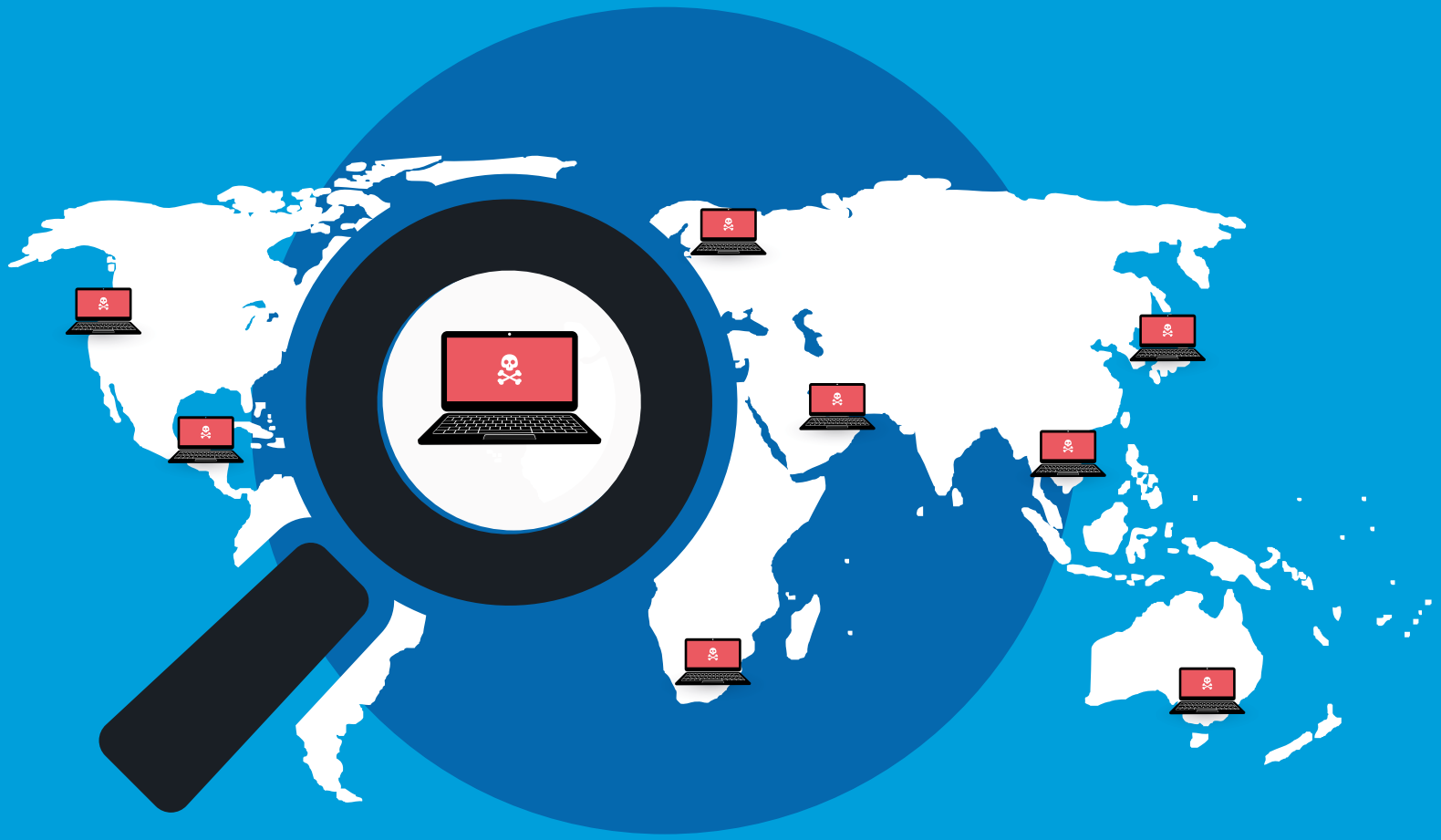
AT&T Cybersecurity

AT&T Business



Evaluator's guide for managed detection and response (MDR) services

Table of contents

Executive summary

A managed detection and response (MDR) service provider can help organizations establish or enhance their threat detection and incident response strategies. It can also help avoid the traditional obstacles associated with deploying advanced security infrastructure and hiring skilled security professionals. Organizations of all sizes can take advantage of MDR services to quickly scale their security and compliance efforts—often with greater cost-efficiency and a faster ROI than doing it on their own.

The MDR market is growing rapidly. Many managed security services providers define their own MDR service offerings based on their current capabilities and infrastructure. With so much variation in service definitions, it can create confusion as to what MDR does or does not provide to customers.

At a minimum, MDR services should provide 24x7 alarm monitoring and at least some lightweight incident investigation and response. But, as with any swiftly maturing market, a customer's mileage may vary. It pays to do a lot of due diligence before settling on a managed security services provider (MSSP) or MDR provider. That evaluation should not only look into the quality of service offered, but also the technologies underpinning the service.

Organizations evaluating the MDR market should consider the following 10 elements in their decision-making process.

Elements to consider

The technology stack

As with any managed security service, it's important to "look under the hood" to evaluate the security technologies that the MDR provider uses to perform threat detection and incident response. A thorough technology evaluation can help you determine how broad and potentially effective the MDR provider's threat detection capabilities may be. It can also help you identify technical limitations or gaps that may require you to supplement the service with other security controls.

Some MDR solutions on the market today are based on a single-security technology, such as endpoint-based detection and response (EDR). This may limit the visibility the service provider has into the threats facing your critical infrastructure.

Organizations should seek out an MDR solution that uses multiple detection technologies that work together for effective detection and response across networks and endpoints. Look for an MDR solution that delivers on essential security capabilities, such as asset discovery, vulnerability assessment, network- and host-based intrusion detection, and SIEM correlation. The solution should also have capabilities like user activity monitoring and dark web monitoring.

An MDR service that combines multiple integrated security capabilities can help provide broad threat coverage and early detection and can help to reduce false positives. It can also enable the MDR providers' security analysts gain important threat context quicker in an investigation—which can lead to a faster containment time.

Elements to consider

Cloud security monitoring

As organizations adopt public cloud services and infrastructure, protecting those environments is of utmost importance. In today's hybrid IT environments, organizations must be able to monitor critical assets whether they are in the data center or in the cloud. And an MDR solution should provide that visibility by default.

Some MDR providers may be limited in their support for cloud security monitoring. Or, they may require you to upgrade your service or purchase an additional service module. These limitations may hinder your cloud transformation or result in unforeseen, additional costs.

Evaluate MDR solutions for their cloud security monitoring capabilities, even if your organization currently has no data and assets in the cloud. If you're not currently using cloud infrastructure or services today, having a solution that is ready to support your future cloud migration can save you time and costs. It can also simplify things for you if you don't have to change your service or MDR provider when it's time to migrate.

Look for a provider that offers native cloud security monitoring for your business-critical IaaS and SaaS environments as part of their MDR solution by default. These capabilities should integrate virtually seamlessly with the provider's network security monitoring for centralized visibility across networks and endpoints on premises and in the cloud.

Additionally, your MDR provider should be able to identify security configuration errors and other vulnerabilities in your cloud environments. Based on their findings, they should be able to provide recommendations for improving your cloud security posture.

Elements to consider

Alarm monitoring and validation

A noisy, un-tuned security analytics platform can produce hundreds and thousands of security alarms. If an MDR provider isn't reviewing and validating every single alarm to weed out non-actionable issues and false positives, then the service is not going to alleviate the burden on your security analysts. Make sure your MDR provider has processes and staff to review and validate every security alarm, rather than simply forwarding them on to your team.

Evaluators should dig into how their prospective MDR providers triage and escalate security incidents that require additional investigation or threat hunting activities. Look for an MDR provider that measures its success on accuracy of identifying actionable incidents—not just how quickly they notify you of any security alert. Also, ask how your MDR provider will work with you to continually tune your environment to reduce false positive and streamline security operations.

Elements to consider

Incident response

The ‘R’ of MDR—response—can vary greatly from service to service. Some MDR services include ‘lowercase r’ response; they only go as far as passing along recommendations on security alerts. Thus, organizations should carefully vet the MDR provider’s incident response definitions and service-level agreements (SLAs) to see to it that they meet your expectations and needs. Having a clear understanding of the roles and responsibilities between the provider’s incident response team and your own security team can save precious time during an actual security incident.

Evaluators should look for an MDR provider that can help assess their incident response needs from the outset. A quality MDR service will strategize with you to develop and document a custom incident response plan that aligns to your security and compliance goals, priorities, and resources. Look for a provider that plans to work with you during onboarding and implementation.

You’ll want them to review your security program goals and priorities, the criticality of systems and data, compliance requirements, and more in order to fine tune incident response processes to your specific needs.

And, of course, the MDR service should have a robust security operations center (SOC) with staffed 24x7 with security analysts and incident responders ready to execute on that plan once the service is in place.

Elements to consider

Orchestration and automation

Increasingly, security programs are incorporating security orchestration, automation, and response (SOAR) tools to improve efficiency and response time to incidents. Even if you enlist an MSSP to manage your threat detection and incident response program for you, the use of orchestration and automation can help to improve the efficacy and efficiency of the service.

Evaluators should seek out an MSSP with a strong commitment to SOAR capabilities. At a minimum, providers should be able to automate continuous data collection and security analysis for near-real-time threat detection across your environments.

Going further, providers that use advanced security orchestration capabilities and pre-built integrations with other essential security tools can help accelerate and ease incident response activities. For example, your MSSP may be able to automate or orchestrate security policy changes on your firewall after detecting an activity with a known malicious IP address, regardless if you manage the firewall or the MSSP manages it for you.

Evaluators should ask about API support, technology partnerships, and the ease of integration with both on-premises and cloud platforms.

Elements to consider

SOC transparency and availability

MDR is not an outsourcing arrangement in the traditional sense and should not be performed in black-box conditions. Even with an MDR provider at your side, your security team owns your overall security program—they will likely participate in the security monitoring activities at some level.

Thus, it is imperative to understand: (1) how an MDR provider will communicate with your security team when incidents occur, and (2) more broadly, how the provider will collaborate with your team to help work towards your security and compliance goals.

Ask:

- Does the MDR provider share access to the detection and response platforms they use?
- Is the provider transparent about how they conduct threat detection, hunting, and investigatory activities?
- Is there an audit trail or record of activities performed by analysts?
- Are SOC analysts available to me 24x7 by phone, email, and other communication channels?
- Is there clear and actionable guidance about what my team needs to do in order to resolve security incidents?
- Beyond incident response, how often does the MDR provider meet with my team to discuss our service and program goals?

The customer should be able to see the technical details that MDR analysts have available to them in their SOC tools. A customer should also expect open and timely response to questions and requests. Even more important, evaluators should confirm whether the MDR provider enables you to access to your own raw log data. Customers may be surprised once they sign on with some MDR services to find that that MDR provider does not grant access to log storage or otherwise makes it difficult to obtain.

At the end of the day, organizations should look for a high level of collaboration and regular touchpoints that are clearly defined and documented as a part of the service.

Elements to consider

Compliance reporting

Common market definitions for MDR services place compliance reporting out of scope. However, with all the functions commonly provided by MDR standing as key areas under many regulators' purview, it's important to be able to get the visibility and reporting you need to demonstrate compliance during an audit. The right MDR provider could help to provide invaluable support for your compliance readiness efforts. See if they offer a consolidated reporting view of regular vulnerability scans, malware detection, collection of firewall logs, file integrity monitoring, and incident response habits.

Customers can get more bang for their MDR buck if they seek out a provider that will assist with their compliance reporting needs. Also, make sure the MDR provider has earned its own compliance certifications, such as for PCI DSS, SOC 2 Type 2, and ISO 27001. Doing so can give customers confidence in working with a service provider that understands and can successfully navigate the compliance process.

Elements to consider

Threat intelligence

Threat detection technologies and security analysts are only as good as the threat intelligence that fuels their work. Thus, the quality of the threat intelligence that powers your MDR service should be no secret. Evaluate the quality of your threat intelligence based upon diversity, timeliness, and resilience.

Evaluators should probe into the sources of threat intelligence that powers their MDR provider's detection capabilities. Look for diversity in those sources and ask the provider if they use a variety of threat intelligence sources or rely on a single source. If a provider is at all vague about their threat intelligence sources, those could be potential red flags for buyers.

In addition, pay attention to how soon your defenses are updated after a new exploit or vulnerability is discovered in the wild and frequency of threat intelligence updates.

Finally, evaluate the threat intelligence for its resilience. Threat intelligence that helps to identify higher-order tools, tactics, and procedures (TTPs) promotes resilient detection, as TTPs are less likely to change frequently than indicators like IP addresses and file hashes. Carefully examining the diversity, timeliness, and resilience can help you to determine the quality of the threat intelligence.

Elements to consider

Deployment and onboarding

MDR buyers invest in managed security services in order to buy time—speeding up response time and minimizing time spent on building out detection and response capabilities or staff. Deployment times are a big consideration. Every day it takes to implement a solution is an extra day the business is exposed to risk. Not only that, but when it comes time to prove ROI to the business, those metrics can be greatly skewed by lengthy deployment schedules.

Evaluators should also ask their service provider up front about their deployment timelines. How long does it take to get technology in place and the service up and running?

Don't be fooled by marketing hype. Make them prove their claims by providing customer references who can corroborate those timelines.

Elements to consider

Scalability and adaptability

Today's IT environment moves fast to keep pace with business demands. With the coming tide of digital transformation, an organization can't afford to be slowed down by security constraints. Before signing on the dotted line, MDR evaluators should think about whether their provider is ready to support your organization's growth and IT transformation.

Look for an MDR solution that offers speed and simplicity in scaling. Whether you plan to expand your footprint with new satellite offices or retail locations, merge or acquire another company, or otherwise grow your IT environment to keep up with business demands, you should be ready to extend your security coverage without complex change orders or lengthy deployments.

Understanding the costs of scaling your MDR service is equally as important. Pricing should be transparent, and evaluators should look closely to see that there aren't limitations on events per day (EPD), user seats, or number of assets monitored. These can limit flexibility and cause cost overruns.

Evaluators should ask for information about the MDR provider's architecture and ask tough questions not only about the costs for monitoring today's environment but also what it'll take to scale up as your environment grows.

Evaluation pitfalls to avoid

As evaluators work their way through the above considerations, they should take care to avoid the following mistakes, oversights, and misperceptions common to the MDR evaluation process.

Falling into the DIY hidden costs trap

Smaller organizations in particular may be susceptible to 'sticker shock' and perceive MDR as too expensive or sophisticated for their needs. However, organizations must carefully consider the direct and indirect costs of building and maintaining an effective threat detection and incident response program, as well as the risks associated with not taking any action. Costs to consider include (1) technology licenses and infrastructure, (2) threat intelligence subscriptions, and (3) the salaries of skilled security analysts, threat researchers, and incident responders. All in all, DIY may cost you more both in expense and elevated cyber risk than choosing an end-to-end MDR solution.

Limiting search to local service providers

Thanks to modern cloud-based SOCs with 24x7 operations, your MDR provider doesn't necessarily need to be located in the same zip code as you. Expanding the scope of your evaluation to national and global MSSPs can help you find the best fit for your organization's needs while still making it possible to select a preferred region or country for your log data storage.

Failing to evaluate against your long-term security goals

Many organizations have a sense of urgency in their selection of an MDR provider, either because they have recently experienced a breach, want to safeguard against a future breach, or have a fast-approaching compliance audit to prepare for. However, limiting your evaluation to focus solely on your current security objectives can lead to challenges and unforeseen costs in the future. It's important to consider what major IT or business transformation initiatives your organization is planning for the next 1–3 years and to evaluate MDR providers on their future readiness. Similarly, ask your MDR provider how they plan to evolve their service to continually meet the needs of customers as they transform networks with SD-WAN technologies, public cloud services, 5G and IoT services, and more.

Service lock-in

As discussed throughout this white paper, enlisting an MDR provider can often be the fastest and most cost-efficient way for under-resourced security teams to establish an effective threat detection and response program. However, as your security goals and resources evolve, you might decide to transition threat detection and response activities to an in-house team. But, your MDR provider might not be able or willing to put you in the driver's seat. That could mean starting over by building your own technology stack.

Many MDR providers offer multiple, flexible threat detection and response options. These can allow customers to transition virtually seamlessly across a fully managed service, a co-managed service, or a fully customer-managed service, while retaining the same technology platform or environment. This can help customers to avoid service lock-in and support a painless transition of service without downtime or data loss.

How AT&T Cybersecurity can help

AT&T Cybersecurity stands apart from other MDR solution providers with AT&T Managed Threat Detection and Response, a sophisticated MDR service that helps you detect and respond to advanced threats before they impact your business. It builds on our decades of expertise in managed security services, our award-winning Unified Security Management® (USM) platform for threat detection and response, and AT&T Alien Labs™ threat intelligence. With advanced features like 24x7 proactive security monitoring, security orchestration, and automation in one turnkey solution, you can quickly establish or scale your security program without the cost and complexity of building it yourself.

Here's how AT&T Managed Threat Detection and Response stands up against the evaluation criteria described above.

Elements to consider	AT&T Managed Threat Detection and Response
The technology stack	AT&T Managed Threat Detection and Response is built on our award-winning unified security management (USM) platform, which combines the essential security capabilities needed for effective threat detection and response in a single pane of glass. Key capabilities include asset discovery, vulnerability assessment, network intrusion detection (NIDS), endpoint detection and response (EDR), and SIEM event correlation and log management.
Cloud security monitoring	AT&T Managed Threat Detection and Response provides native cloud security monitoring capabilities for IaaS (AWS®, Azure) and SaaS environments (Office 365, G Suite™, Okta, and Box), using management APIs to continuously collect a rich data set from those environments. In addition, AT&T Alien Labs threat intelligence addresses advanced threats that specifically impact cloud environments.
Alarm monitoring and validation	Our SOC analyst team provides 24x7 proactive alarm monitoring. This team reviews every security alarm in the USM platform, working to reduce false positives and non-actionable alarms so that your team can focus on responding to actual threats, rather than sifting through noise. In addition, our analysts conduct in-depth incident investigations, providing your incident responders with rich threat context and recommendations for containment and remediation, helping your team to respond quickly and efficiently.
Incident response	When a security incident occurs, our analyst team works side-by-side with the customer's security resources to help them respond quickly and effectively. Our analysts conduct in-depth incident investigations on actionable alarms and escalate incidents based on severity. Investigations provide rich threat context on the incident, which may include additional threat intelligence, related alarms and events, conclusions, relevant files, an audit trail of activities, and response recommendations. This gives the customer a consolidated view of the situation, helping them to take swift action. Our analysts are available 24 x 7 to provide support throughout and can even initiate incident response actions according to your incident response plan, taking advantage of the built-in security orchestration and automation capabilities of the USM platform.

Elements to consider	AT&T Managed Threat Detection and Response
Orchestration and automation	AT&T Managed Threat Detection and Response uses the powerful security orchestration and automation capabilities of the USM platform to streamline incident investigation and response activities and to help accelerate time to response. The USM platform makes it easy to automate the incident response actions towards networks and devices as well as other integrated security controls, enabled through the platform's AlienApps™ integration framework. The USM platform has 300+ AlienApps integrations with widely used IT, security, and business productivity tools including Box, Cisco Umbrella™, and Palo Alto Networks®.
SOC transparency and availability	With AT&T Managed Threat Detection and Response, customers aren't left in the dark about their security posture. Rather, they have access to the same web-based portal that our AT&T SOC analyst team uses to monitor the environment on a daily basis, and our analyst team is available 24x7 by phone, email, and Slack. Our SLAs start within 5 minutes of an incident investigation severity assignment for Category 1 critical issues. In addition to incident response activities, our analyst team leads weekly review calls with the customer to cover all investigations and incident response activities as well as a monthly meeting to review service metrics related to our SLAs, and to review progress towards the customer's security program objectives and may provide recommendations for improvements.
Compliance reporting	We support customers' compliance reporting requirements using the pre-built and highly customizable reporting templates in the USM platform. In addition, AT&T Managed Threat Detection and Response includes long-term log storage, including raw log retention in a highly secure environment that has earned multiple compliance certifications by third-party assessors, including for PCI DSS, ISO 27001, SOC 2 Type 2, as well as attestations of HIPAA compliance and GDPR readiness.
Threat intelligence	AT&T Managed Threat Detection and Response is fueled with continuously updated threat intelligence from AT&T Alien Labs, so your defenses are able to detect emerging and evolving threats. AT&T Alien Labs, the threat intelligence unit of AT&T Cybersecurity, produces timely threat intelligence that is integrated directly into the USM platform in the form of correlation rules and other higher-order detections to automate threat detection. This team has a unique vantage point into the AT&T IP backbone, global USM sensor network, Open Threat Exchange® (OTX™), and other diverse threat data sources. AT&T Alien Labs goes beyond simply delivering threat indicators—we perform deep, qualitative research that provides insight into adversary tools, tactics, and procedures (TTPs).

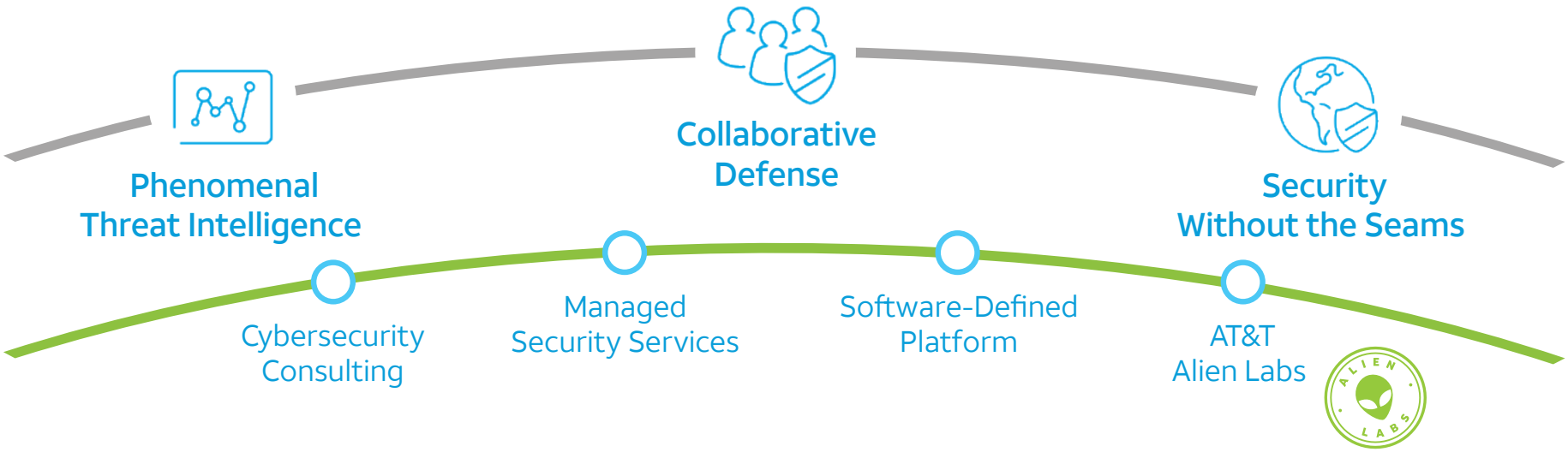
Elements to consider	AT&T Managed Threat Detection and Response
Deployment and onboarding	With the goal of getting AT&T Managed Threat Detection and Response service fully operational within the first 30 days of signing up, our SOC analyst team conducts an onsite onboarding engagement with the customer's team to install, configure, and tune the deployment according to the customer's requirements. During onboarding, a lead analyst facilitates an incident response plan review and threat modeling exercise with the customer's team. We want to understand each customer's unique environment so we can deliver the best service possible. We identify customer-specific goals and priorities for their security program, the criticality of systems and data, compliance requirements, and more.
Scalability and adaptability	With AT&T Managed Threat Detection and Response, it's easy to bring an additional location or environment online without having to install an appliance on site. Hosted in our highly elastic cloud environment, the USM platform readily scales to meet our customers' growing business needs. The service is priced according to the total amount of online, searchable events retained, so customers don't have to worry about limitations by assets, environments, or number of employees.

Learn more about AT&T Managed Threat Detection and Response on our website!

About AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning – helping to enable our customers around the globe to anticipate and act on threats to protect their business.

Unified Security Management



This document is intended to include general information for learning about MDR services. Use of names of third-party companies in the document are for informational purposes only and do not constitute any endorsement by AT&T Cybersecurity.

AT&T Business