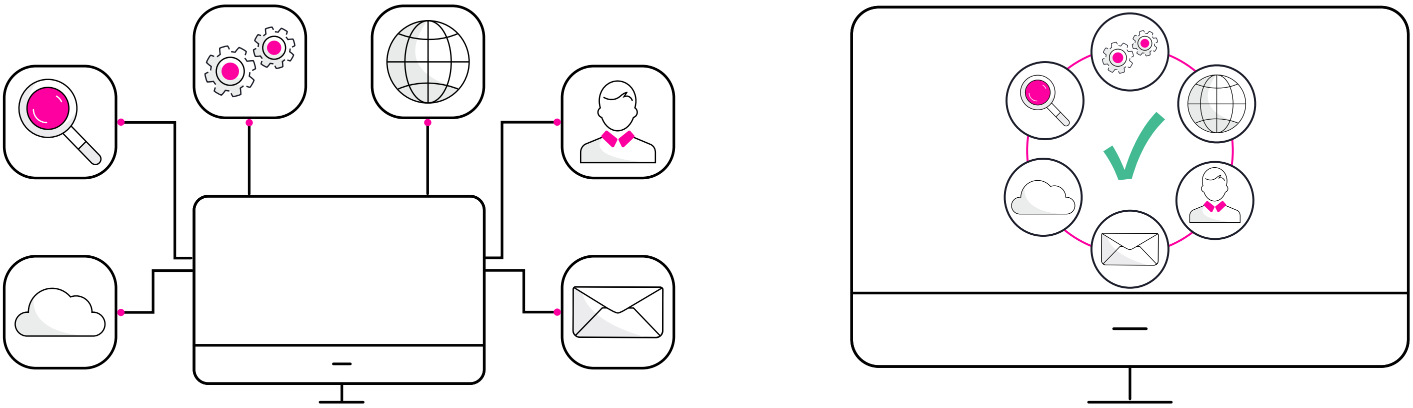
# From MSP to MSSP in 24 Hours



Managed service providers (MSPs) are increasingly looking to become managed security service providers (MSSPs) to boost revenue and better address their clients’ needs. The road to transitioning to an MSSP, however, has traditionally required significant time and budget to obtain the necessary technologies and skills required to fully protect client organizations from sophisticated cyber-attacks.

Fortunately for MSPs, the road to becoming an MSSP has just become much shorter and far more affordable than ever.  Cynet can help transition an MSP to a fully operational MSSP in one day. Yes, you read that right. This ebook describes how any MSP can become a full-fledged, highly capable MSSP in a mere 24 hours by using Cynet's 360 AutoXDR platform and 24x7 MDR services.

# The Traditional Road to Becoming an MSSP

MSPs are faced with significant challenges when transitioning to an MSSP. The dynamic nature of cybersecurity requires deep and continuously updated expertise to not only stay abreast of the latest attack approaches, but also understand the myriad protection technologies that can be brought to bear to protect organizations. Among the hurdles MSPs face when trying to become and MSSP include:

## Choosing the right security technologies

Most companies operate a hybrid work environment, where employees, contractors and partners work across multiple physical sites and remotely. The technology environment is typically also hybrid, with a mix or on-premises and cloud computing assets. Protecting all these users and assets requires a sophisticated and highly capable technology stack that is tightly integrated and expertly maintained for optimum performance. Additionally, MSSPs typically operate a multi-tenant technology stack to simplify the task of providing security across the entire customer base.

## Gaining the appropriate cybersecurity expertise

If cybersecurity was easy, we wouldn't need MSSPs! However, the sophistication and rapid evolution of threats requires highly trained and seasoned cybersecurity expertise to operate and update protection technologies. These experts must also stay abreast of the latest developments in the vast cybercriminal underground to ensure they are prepared for what's coming next. The widespread, global cybersecurity skills shortage only exacerbates the task of building a capable team.

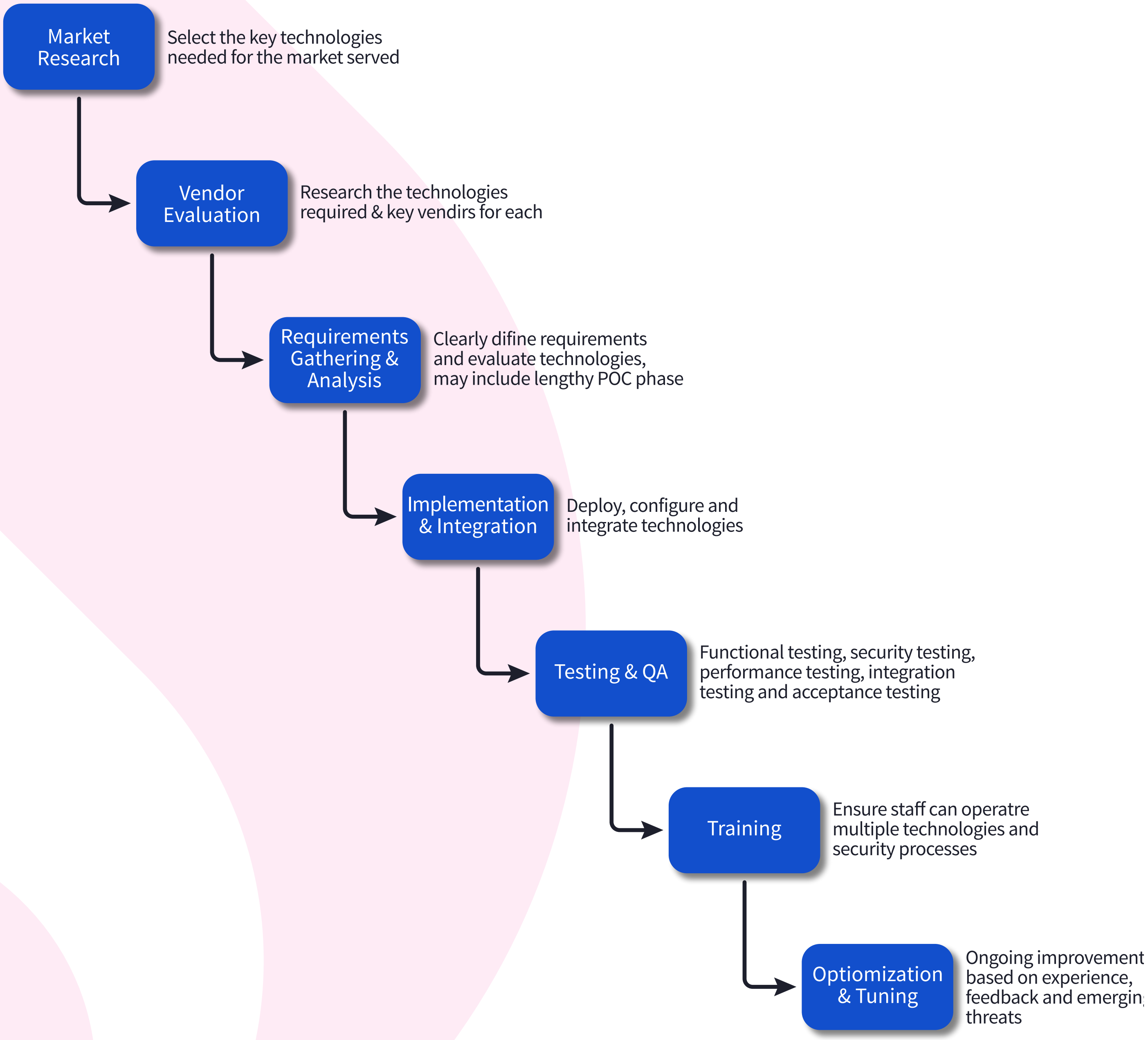
## Providing 24x7 coverage

We know that attacks happen around the clock with cybercriminals often targeting off hours and holidays to detonate sophisticated ransomware to maximize the likelihood of success. Providing three full shifts of security analysts capable of monitoring, investigating, and responding to alerts is challenging and expensive.

## Having sufficient budget

It should be obvious by looking at some of the requirements to become an MSSP above that it can be a quite expensive and time-consuming proposition. While building out services over time is an option, there are some fundamental capabilities required at the outset for any MSSP to be considered a viable option by prospects. The more and stronger the capabilities, the higher the likelihood of success in this highly competitive market.

As one would expect, setting up an MSSP can be a time-consuming, expensive proposition. Researching security vendor technologies, negotiating terms, installing and integrating disparate technologies, training on multiple vendor interfaces, and maintaining and updating the security stack can be daunting. A typical process for selecting and implementing the technology stack required to become an MSSP looks something like the following:


Market Research
Select the key technologies needed for the market served
Vendor Evaluation
Research the technologies required & key vendirs for each
Requirements Gathering & Analysis
Clearly difine requirements and evaluate technologies, may include lengthy POC phase
Implementation & Integration
Deploy, configure and integrate technologies
Testing & QA
Functional testing, security testing, performance testing, integration testing and acceptance testing
Training
Ensure staff can operatre multiple technologies and security processes
Optiomization & Tuning
Ongoing improvement based on experience, feedback and emergin threats

**Typical MSSP Technology Selection & Implementation Flow**

As you might expect, the above process typically requires at least several months before reaching vendor selection in the Requirements Gathering & Analysis phase. After the vendors are selected, implementation, integration, testing and training also require several months as MSSP multi-vendor technology stacks tend to be quite complex.

Most MSSP end up managing over a dozen vendors to gain their required protection capabilities. For example, the technology stack and vendor mix might look like the following, depending on the technologies desired and vendor preferences.

| Capability | Vendor 1 | Vendor 2 | Vendor 3 | Vendor 4 | Vendor 5 | Vendor 6 | Vendor 7 | Vendor 8 | Vendor 9 | Vendor 10 | Vendor 11 | Vendor 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Next-Generation AV (NGAV) | ✓ | | | | | | | | | | | |
| Endpoint Detection & Response (EDR) | | ✓ | | | | | | | | | | |
| Automated Remediation | | ✓ | | | | | | | | | | |
| SIEM / CLM | | | ✓ | | | | | | | | | |
| Threat Hunting | | | | ✓ | | | | | | | | |
| Email Protection | | | | | ✓ | | | | | | | |
| Multifactor Authentication (MFA) | | | | | | ✓ | | | | | | |
| Darkweb Checks | | | | | | | ✓ | | | | | |
| Security Awareness Training | | | | | | | ✓ | | | | | |
| Security Policies & Procedures | | | | | | | ✓ | | | | | |
| Deception Tactics with Honeypots | | | | | | | | ✓ | | | | |
| Managed Incident Response | | | | | | | | ✓ | | | | |
| User Behavioral Analysis (UBA) | | | | | | | | ✓ | | | | |
| Network Traffic Analysis (NTA) | | | | | | | | | ✓ | | | |
| SOAR | | | | | | | | | | ✓ | | |
| SSPM / CSPM | | | | | | | | | | | ✓ | |
| Managed SOC / MDR | | | | | | | | | | | | ✓ |
| **Cost / User / Month** | | | | | | | | | | | | |

**Example MSSP Technology Vendor Matrix**

But it doesn't end there. Determining the skills needed to operate the technology and support clients, hiring, training, and managing a bench of deep and varied cybersecurity experts is also a formidable task.

And, you must hit the ground with a fully functioning security stack and a knowledgeable support staff that can support clients 24x7. That's a lot of prep work just to get to where you need to be to support your first client on day 1.

# A New Option: Transition from MSP to MSSP in One Day

Fortunately, with Cynet, moving from an MSP to an MSSP has become far easier than the traditional approach. The Cynet 360 AutoXDR platform, along with support from CyOps, Cynet's world-class MDR team, provides virtually everything to transition your MSP to an MSSP. Moreover, this transition can take place in a single day. Below is an overview of what you can achieve with Cynet.

# Broad Threat Visibility and Protection

Broad visibility across the primary prevention and detection components that provide the most pertinent threat telemetry forms the basis of the Cynet 360 AutoXDR platform. The Cynet platform is purpose-built to include components that cover the primary attack vectors, providing layered security protection out of the box, including:

- NGAV/EPP - Next Generation Antivirus/Endpoint Protection Platform - for basic endpoint malware prevention and detection and endpoint control.
- EDR - Endpoint Detection and Response - for more advanced endpoint protection, detection, and response.
- NTA - Network Traffic Analytics - for malicious activity on your network.
- UBA - User Behavioral Analytics - to detect anomalous user behaviors.
- Deception – to expose attackers that have gained access to your environment.
- SSPM/CSPM – SaaS Security Posture Management/Cloud Security Posture Management - to reduce the risk introduced by SaaS and Cloud misconfigurations.

These native technologies provide the prevention and protection required for today's threat environment. Natively combining signals from multiple points of telemetry provides the context required to detect stealthy (and otherwise undetectable) attacks while providing far greater detection accuracy (and thereby slashing false positives). When all prevention and detection components are part of a single platform, data and alert information can be easily normalized and combined; a feat that is highly difficult when trying to coordinate multiple vendor point solutions.

Moreover, this layered security approach ensures threats that bypass first line defenses are detected and thwarted as quickly as possible. Something that may seem harmless by one security solution suddenly becomes cause for concern when intelligently paired with information from other security solutions.

# Extensive Response Automation

Cynet 360 AutoXDR provides automated response capabilities to immediately eliminate or quarantine threats detected across the environment. Many threats trigger an automated response capability to investigate the attack, automatically collecting information associated with the incident, determining the root cause and scope of the attack and then identifying all attack components across the environment. You can configure whether attack components are remediated automatically or manually. Cynet Response Automation includes the following components:

- CLM – Centralized Log Management - for storing and analyzing important log data collected across IT components and security controls.
- SOAR – Security Orchestration, Automation and Response - to fully automate response actions to threats across the entire environment (includes extensive investigation and remediation capabilties) .

Cynet 360 AutoXDR SOAR also includes pre-built and customized response playbooks that string together multiple investigation and remediation actions to more closely suit your environment and policies. This also allows MSSPs to customize response actions to specific clients or parts of a client’s environment. For example, you could define different investigation and response workflows when responding to a threat on an ecommerce server versus an internal chat application.

# Managed Detection and Response Services

Cynet XDR extends and improves your security resources with a team of world-class cybersecurity experts – CyOps. The CyOps team continuously monitors client environments 24/7 to prioritize alerts, informing customers in real-time of critical security events and guiding them through the response process. Cynet customers can submit files to CyOps for analysis at any time, request ad-hoc threat investigations and forensic analysis, and receive guidance through remediation steps. CyOps services include:

- Alert Monitoring - Continuous management of incoming alerts: classify, prioritize and contact the customer upon validation of active threats.
- Attack Investigation - Deep-dive into validated attack bits and bytes to gain full understanding of scope and impact, providing the customer with updated IoCs.
- Threat Hunting - Proactively search for hidden threats leveraging Cynet 360 Auto XDR™ investigation tools and over 30 threat intelligence feeds.
- 24/7 Availability - Ongoing operations at all times, both proactively and on demand, per customers' specific needs.
- Exclusions, Whitelisting and Tuning - Aligning Cynet's alerting mechanisms to the customers' IT environment to reduce false positives and increase accuracy.
- On-demand file Analysis - Customers can send suspicious files to analysis directly from the Cynet 360 Auto XDR™ console and get immediate verdicts.
- Remediation Instructions – Following an attack investigation, concrete guidance for users regarding which endpoints, files, user and network traffic should be remediated.

CyOps additionally offers optional "Platinum Services", including enhanced oversight, credential theft monitoring, monthly threat intelligence reports and more. These "value added" services are very attractive to the small to mid-sized companies served by managed service providers.

# Bonus: Sales and Marketing Support

Success delivering MSSP services requires more than having a solid technology and support infrastructure in place. Cynet additionally provides a rich set of enablement resources so your MSSP business can grow profitably. This includes sales and technical enablement along with a rich set of marketing content that can be leveraged to generate business. An extensive e-learning partner portal that includes sales and technical certification programs ensures training is always available and effective. An onboarding framework is in place to help new MSSP partners plan, learn and execute Cynet sales process and customer implementation strategies quickly.

# Time (and Money) is Everything

Going back to the MSSP Technology Vendor Matrix shown earlier, it should be clear how Cynet can help consolidate much of the required technology capabilities on a single integrated platform. Because no one vendor can (or should) supply all requisite cybersecurity technologies, additional protections are required – but the bulk of the key breach protection technology stack can be acquired off-the-shelf with the Cynet 360 AutoXDR platform. The matrix below shows the key technologies supplied in the Cynet 360 AutoXDR platform. And remember, the technologies are natively built as integrated components so the entire platform works seamlessly, intuitively, and exquisitely.

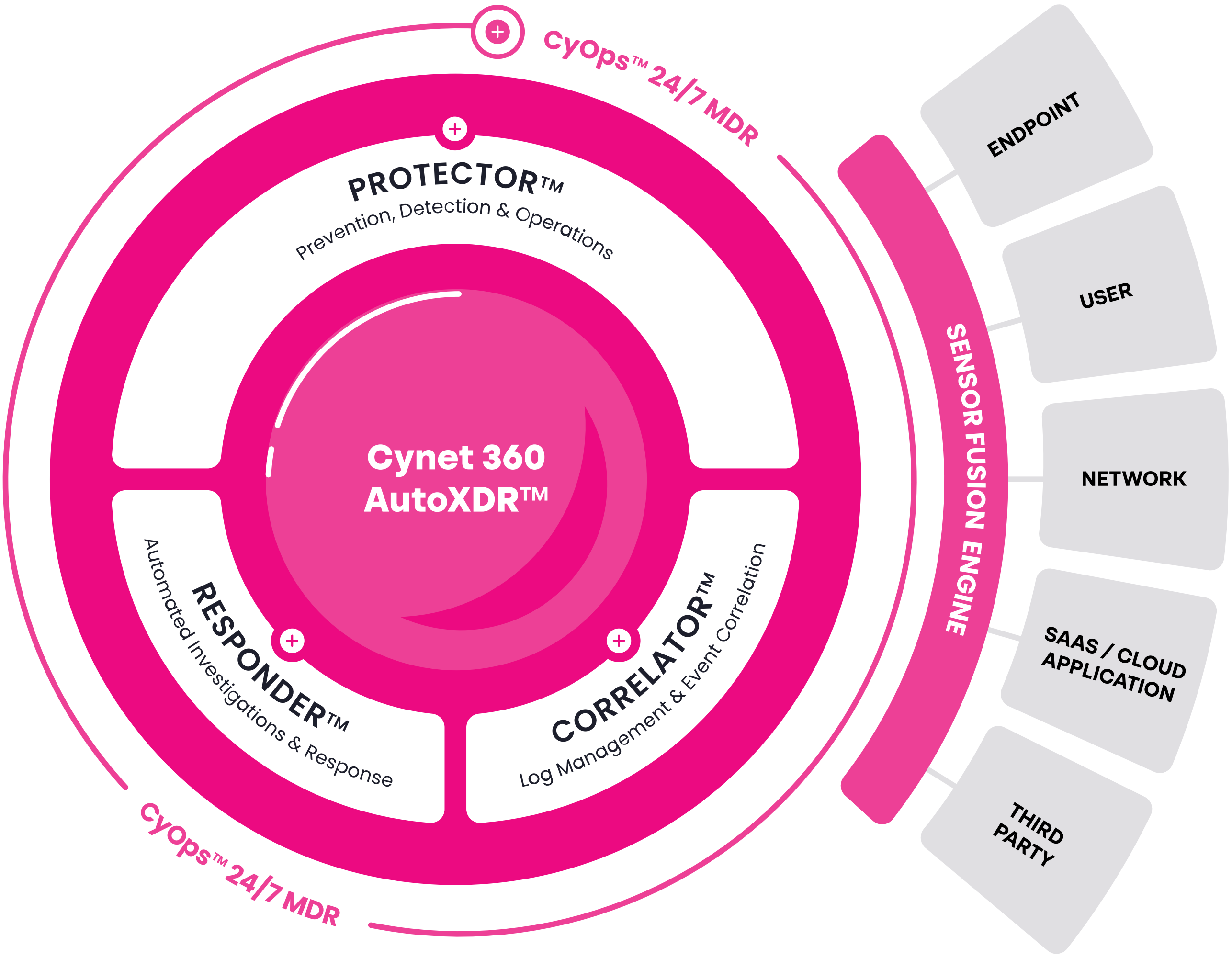
| Capability | Vend. 1 | Vend. 2 | Vend. 3 | Vend. 4 | Vend. 5 | Vend. 6 | Vend. 7 | Vend. 8 | Vend. 9 | Vend. 10 | Vend. 12 | Vend. 12 | Cynet |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Next-Generation AV (NGAV) | ✓ | | | | | | | | | | | | ✓ |
| Endpoint Detection & Response (EDR) | | ✓ | | | | | | | | | | | ✓ |
| Automated Remediation | | ✓ | | | | | | | | | | | ✓ |
| SIEM / CLM | | | ✓ | | | | | | | | | | ✓ |
| Threat Hunting | | | | ✓ | | | | | | | | | ✓ |
| Email Protection | | | | | ✓ | | | | | | | | |
| Multifactor Authentication (MFA) | | | | | | ✓ | | | | | | | |
| Darkweb Checks | | | | | | | ✓ | | | | | | |
| Security Awareness Training | | | | | | | ✓ | | | | | | |
| Security Policies & Procedures | | | | | | | ✓ | | | | | | |
| Deception Tactics with Honeypots | | | | | | | | ✓ | | | | | ✓ |
| Managed Incident Response | | | | | | | | ✓ | | | | | ✓ |
| User Behavioral Analysis (UBA) | | | | | | | | ✓ | | | | | ✓ |
| Network Traffic Analysis (NTA) | | | | | | | | | ✓ | | | | ✓ |
| SOAR | | | | | | | | | | ✓ | | | ✓ |
| SSPM / CSPM | | | | | | | | | | | ✓ | | ✓ |
| Managed SOC / MDR | | | | | | | | | | | | ✓ | ✓ |
| Cost / User / Month | | | | | | | | | | | | | |

**Capabilities Supplied by Cynet in the Example MSSP Technology Vendor Matrix**

The entire Cynet 360 AutoXDR platform and CyOps MDR services are fully built, proven, and ready to go. Eliminate months of preparation and considerable costs with a ready-built “MSSP in a box” solution that can transform any MSP into a fully qualified MSSP overnight. The Cynet agent can be deployed to over 5,000 endpoints in an hour with immediate protections, visibility and insights. It really is that easy.

# About Cynet

Cynet enables any organization to put its cybersecurity on autopilot, streamlining and automating their entire security operations while providing enhanced visibility and protection, regardless of the security team’s size, skill or resources and without the need for a multi-product security stack. It does so by natively consolidating the essential security technologies needed to provide organizations with comprehensive threat protection into a single, easy-to-use XDR platform; automating the manual process of investigation and remediation across the environment; and providing a 24-7 proactive MDR service - monitoring, investigation, on-demand analysis, incident response and threat hunting - at no additional cost.



Learn More