10 CISOs with Small Security Teams Share their Must Do's and Don'ts

How to Manage Security Like a Fortune 500 Company with your Small Security Team

“ Do invest in communicating upstream.

CISO at a chip manufacturing company

This might seem obvious but it’s incredible how this is overlooked when you’re in the rut of “getting things done”. This tip folds within a few sub-tips:

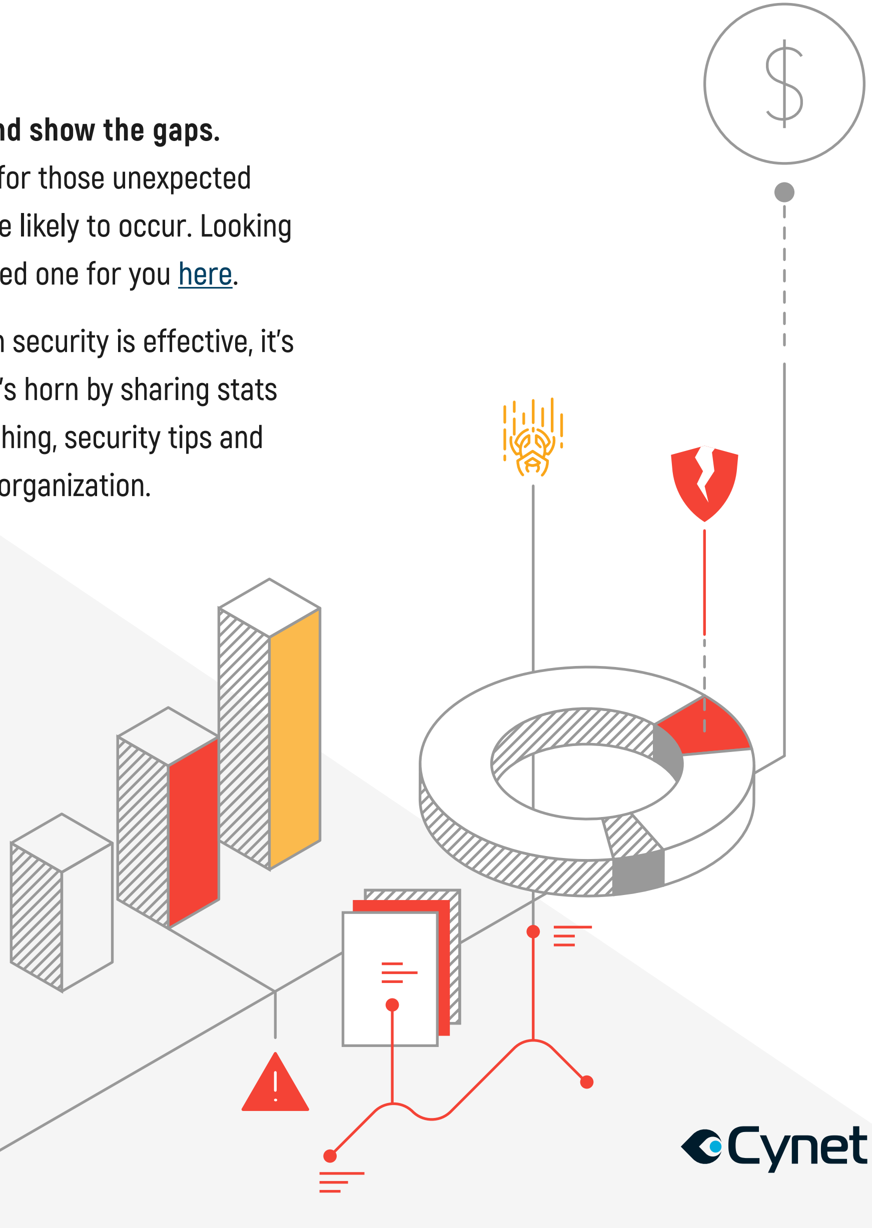
Speak in a business language. Ditch the “fileless attack” language and present the stats, trends and overview of new threats, the business risk they pose and the company’s posture to defend against them.

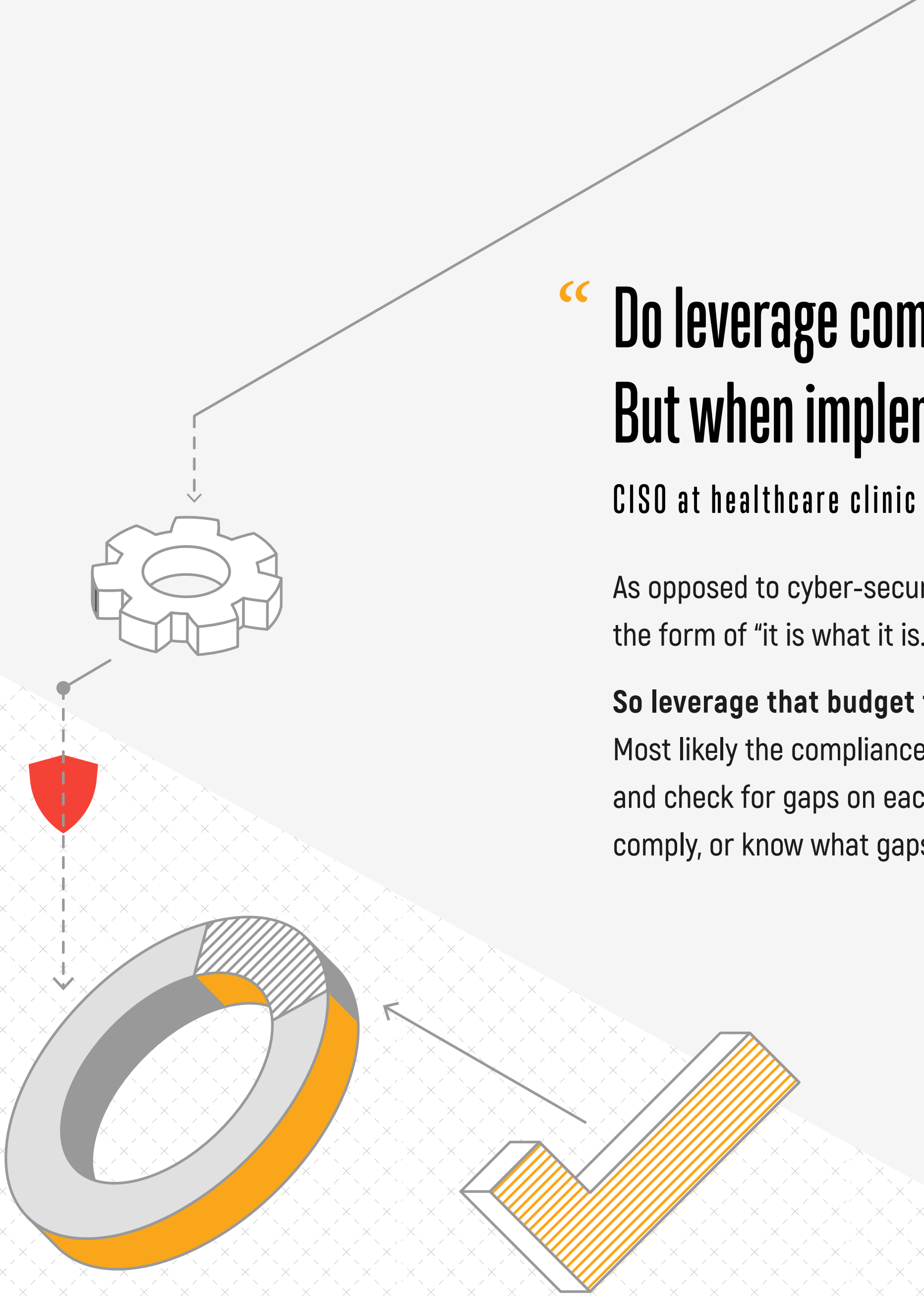
Make sure that you have an annual cybersecurity plan. Present it and revert to it in board meetings. To help you out, we provided you with a security plan presentation template here.

Set expectations on your plan. Communicate and discuss what can be done and won’t be done given this plan, and the business risks to be expected.

Present the security budget and show the gaps. Don’t forget to set aside budget for those unexpected incidents which unfortunately are likely to occur. Looking for a budget template? We created one for you here.

Communicate frequently. When security is effective, it’s virtually invisible. Toot your team’s horn by sharing stats on avoided threats, ongoing patching, security tips and new capabilities throughout the organization.





> “Do leverage compliance to get that security budget.
> But when implementing, look at security first, compliance later.

CISO at healthcare clinic with multiple branches

As opposed to cyber-security budget requests, the compliance budget discussion takes on more or less the form of “it is what it is.” That said, you already know that compliance does not equate security.

So leverage that budget to put in the necessary security controls when implementing your plan. Most likely the compliance requirements will fall into place. To verify, do a controls vs. regulation matrix and check for gaps on each regulation. This approach is also forward-looking and will help you easily comply, or know what gaps exist, when the next regulation comes along.

> “Do consider the accompanying cost when purchasing a product - from deployment to having an analyst follow up on alerts and maintenance.
>
> CISO at retail company

When investing in a new solution, make sure you understand the associated investment, beyond the actual product cost and the security coverage. Some parameters to consider:

Are you getting all the functionality you need up-front, or do you need to purchase additional components or even separate products?

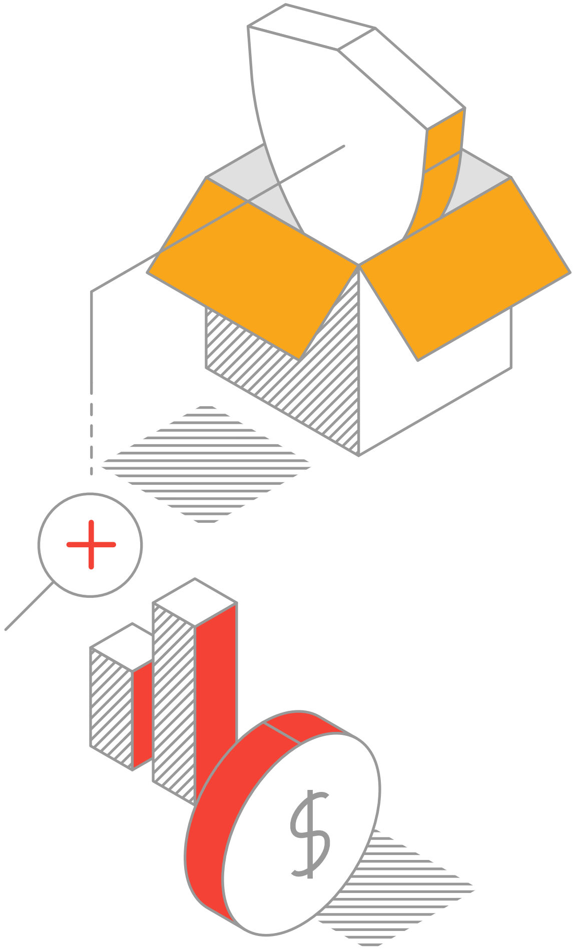
Is the product complex to deploy? How long does it take to deploy one instance? 1000 instances?

What are the maintenance and upgrade requirements? What is the frequency of updates?

Do you need to check the dashboard constantly or do alerts enter your SIEM?

What is the false positives rate?

What type of data are you receiving and how helpful is it to respond to an incident?



Ask your vendor for a trial period to assess these kinds of parameters. Take it a step further and give preference to companies that offer a try/buy model so you can see what implementation is really like and then evaluate the full capabilities of the actual product vs. a slimmed down version typical in a POV evaluation. You want to make sure that any hidden costs or operational issues cause the solution to be unmanageable.

“Do consolidate as many security platforms as you can.

CISO at a software company

Security is known for its innovation, but is also infamous for its point solutions.
When point-solutions become commodities, they start consolidating and that is something that can benefit all CISO. Instead of stacking up multiple products on top of eachother, do some market research to see if there are companies that offer all the products on a single, unified platform.

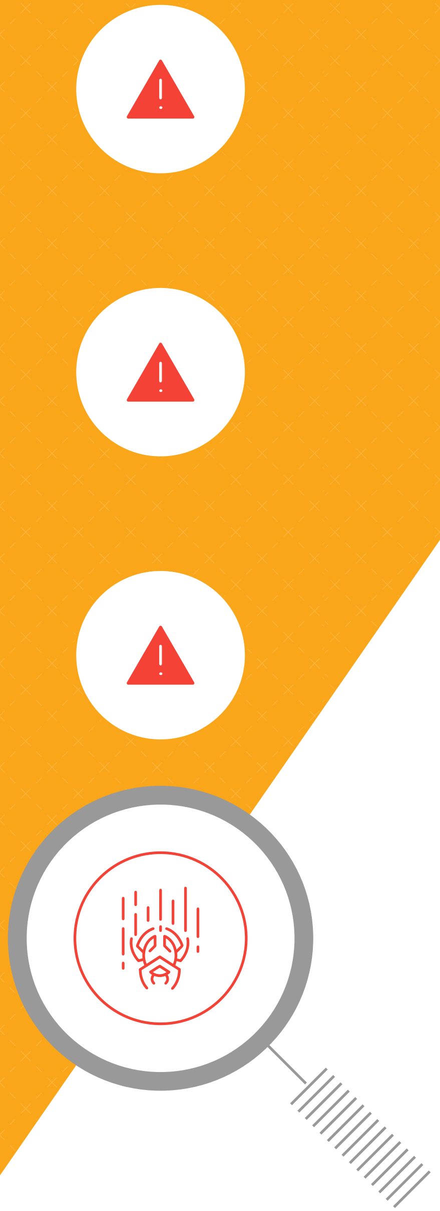
Take that extra mile to understand what “consolidated” or “unified” really mean. You don’t want to go with a single vendor with multiple siloed products as you will be back to square one and will continue stacking solutions. Look for that single product that inherently, and by design, consolidates various technologies into a single platform. For instance, Cynet’s 360-degree Autonomous Breach Protection, built from the ground up as an XDR solution, combines EDR, NGAV, UBA, Network Detection and Response as well as Deception all-in-one.

> “ Don’t necessarily go for the priciest or most well-known brand. But don’t compromise on security.

CISO at regional bank

Remember the BlackHat Sponsorship Hall in 2010? Just tabletops with demo laptops. Fast forward less than a decade, and every vendor in the hall was touting how it was bigger, larger and louder than its competitors. With multiple competitors, an expanding attack surface and a stream of new security technologies it's easy to get caught up in the marketing noise.

Take a step back and see what other solutions are out there. Check comparison sites, read blogs, speak to your colleagues. You might be surprised to find other very strong brands. To make sure the vendor provides the coverage you're looking for, check if they passed third party evaluations and see how they rank for security effectiveness. For instance, MITRE Engenuity performs ATT&CK evaluations where they run known threats against various vendors, of all sizes, and present their results.

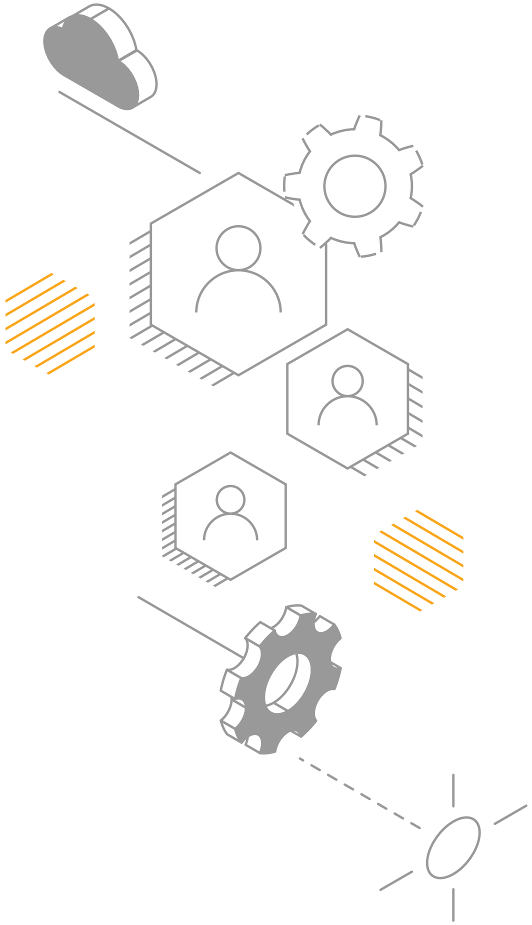


> “Don’t go chasing all alerts. Have a policy on which ones you follow up on. Furthermore, leverage your products to help you triage.

vCSO serving NJ tri-state area

Security teams, by definition, operate on alerts. But small security teams do not have the luxury to follow up on each alert.

Set a policy for when you really do need to chase an alert. It could be on Critical and High, or just on Critical. It might be on specific servers or on critical data. That said, some products will help you better triage and provide more context around an alert and even chain related alerts. That way, not only do you follow up on the alerts according to policy, but you already receive pinpointed data as to the root cause of the incident, remediation advice and even automated response actions according to the severity and type of incident. Make sure that you do follow up on some alerts that have been automatically remediated since the remediated threat could be part of a larger campaign - the alert is sometimes just the starting point.



> “ Don’t work against your company employees, but with them. Listen to their needs and consider how to bake in security without blocking operations.

CISO at gaming company

Employees will nearly always try to subvert a security policy if it slows down their operations. Instead of creating a single uniform policy for all entities at the company, **think of multiple policies per role and how to overcome challenges.** For instance, you may be able to get away with taking the laptop of the marketing manager to perform an investigation, but not that of the CEO who demands 24/7 availability.

Another example is endpoint security latency issues. Employees are used to instantaneous computing power so if you have multiple agents or a hefty one, those employees will push you to find alternative solutions. Be on the lookout for those vendors who understand your business needs. Always ask your vendor for the best deployment architecture for your company along with expected computing and processing stats.

> “Do automate as much as possible. If you find yourself doing something manually, think that there must be a way to automate it.

CISO at software company

Make sure you’re leveraging the power of newer automation technologies to avoid menial or repetitive work. Playbooks are all the rage in cybersecurity, to automate relevant workflows to have quick and effective remediation plans. Automated remediation shouldn’t be confined to just a single component such as the endpoint, but include network and user remediation actions as well.

“ Don’t stop short at just purchasing a product. Check your vendor’s customer success and servicing offering.

CISO at insurance company

You don’t want to be left with a semi-functioning product that you don’t know how to operate or be left alone dealing with an incident when additional resources might exist with your vendor. When engaging with a vendor, check with them for the following:

How much product training do I receive? Is there any initial setup cost?

Is there a dedicated customer success manager working on my account?

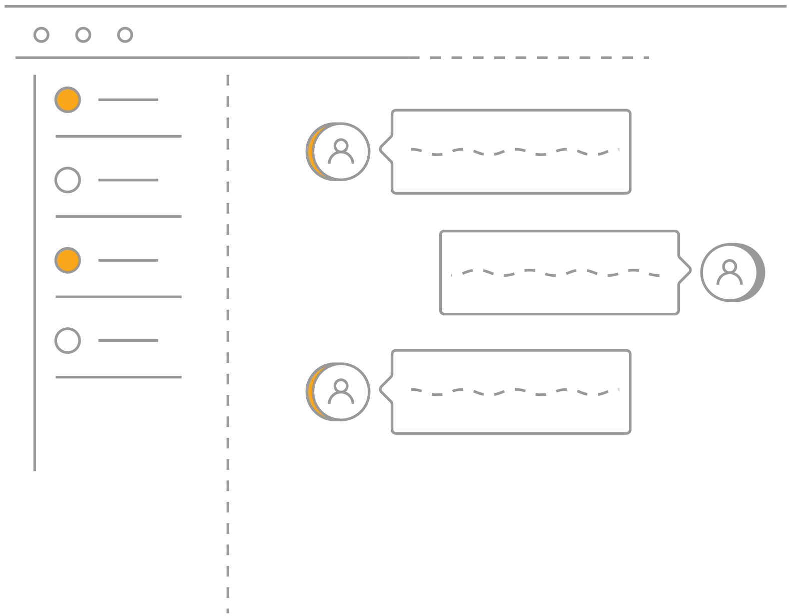
How proactive is customer success on my account?

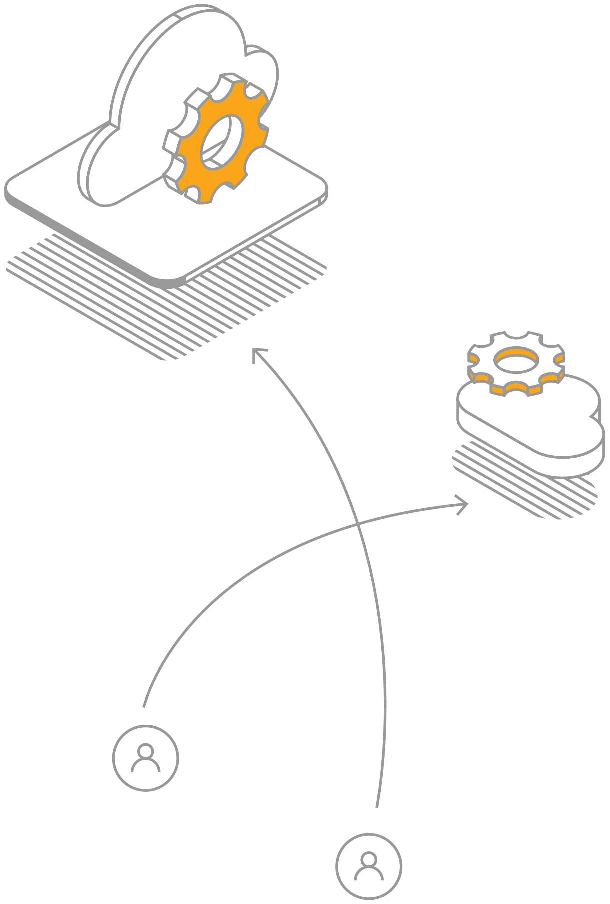
What is the SLA on an open ticket?

Do you have servicing for incidents (aka MDR)?

What tiers and scope of servicing do you have and what are their costs?

How available is the servicing team?





“ Do leverage SaaS offerings to reduce costs, overhead and resources.

CISO at law firm

More and more companies are offering SaaS solutions or Cloud components that reduce deployment and management times and costs, maintenance resources and most likely, are less costly than their on-premises alternatives. Furthermore, many of the security technologies are more effective as a Cloud-based architecture given their stronger processing capabilities.

Check your security stack and perform some research to find what you may be able to swap with a SaaS-based solution. Keep in mind that even security solutions that still require on-premises components - such as an endpoint agent - may have a SaaS-based computing server. This type of architecture enables you to quickly and easily deploy the technology, ensures that the agents are kept lightweight, provides you with a centralized server for processing and management and ultimately, reduces costs without compromising security.

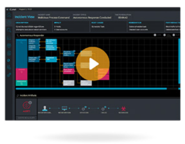
Next Steps

The challenges faced by CISOs with small security teams are certainly different from CISOs with large teams and larger budgets. This tends to make "small team CISOs" a bit more creative and pragmatic than their larger team counterparts. Cynet continuously publishes resources geared towards helping small security teams navigate through the evolving world of cybersecurity. You'll find a plethora of resources including templates and reports to surveys available for free in Cynet's extensive resource library.

Samples of Cynet Resources

XDR-Taking Prevention, Detection and Response to the Next Level

Download eBook ›



Watch an On-Demand Video of Cynet XDR Platform

Watch Demo ›

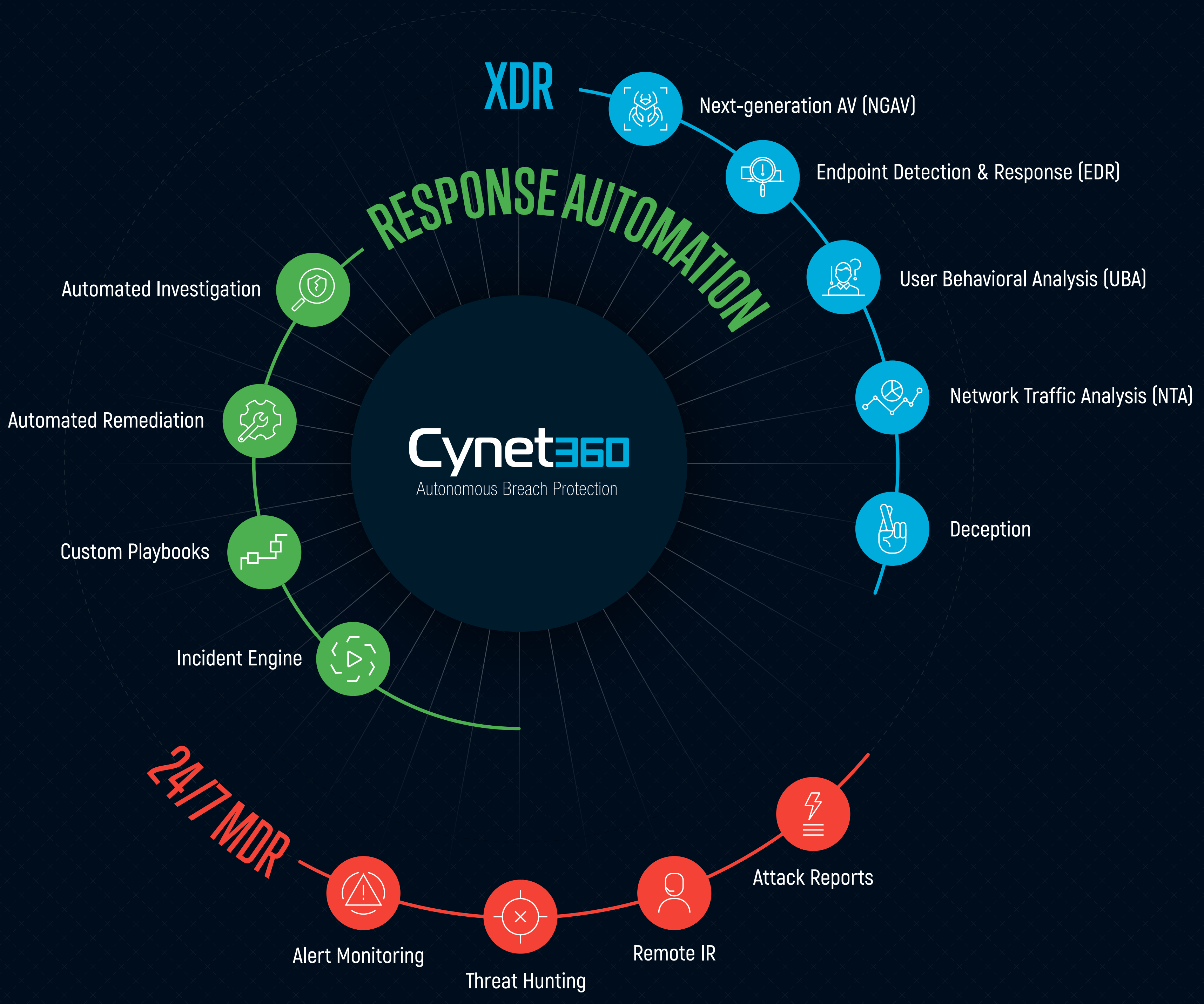
Is your EDR Providing the Best Bang for your Buck?

Download eBook ›

START LEARNING TODAY!

About Cynet

Cynet 360 is the world's first Autonomous Breach Protection platform that natively integrates XDR endpoint, user and network attack prevention and detection capabilities with an incident engine that fully automates investigation and remediation actions, backed by a 24/7 world-class MDR service. End to end, fully automated breach protection is now within reach of any organization, regardless of security team size and skill level.


XDR
Next-generation AV (NGAV)
Endpoint Detection & Response (EDR)
User Behavioral Analysis (UBA)
Network Traffic Analysis (NTA)
Deception
RESPONSE AUTOMATION
Automated Investigation
Automated Remediation
Custom Playbooks
Incident Engine
Cynet360
Autonomous Breach Protection
24/7 MDR
Alert Monitoring
Threat Hunting
Remote IR
Attack Reports