Cynet

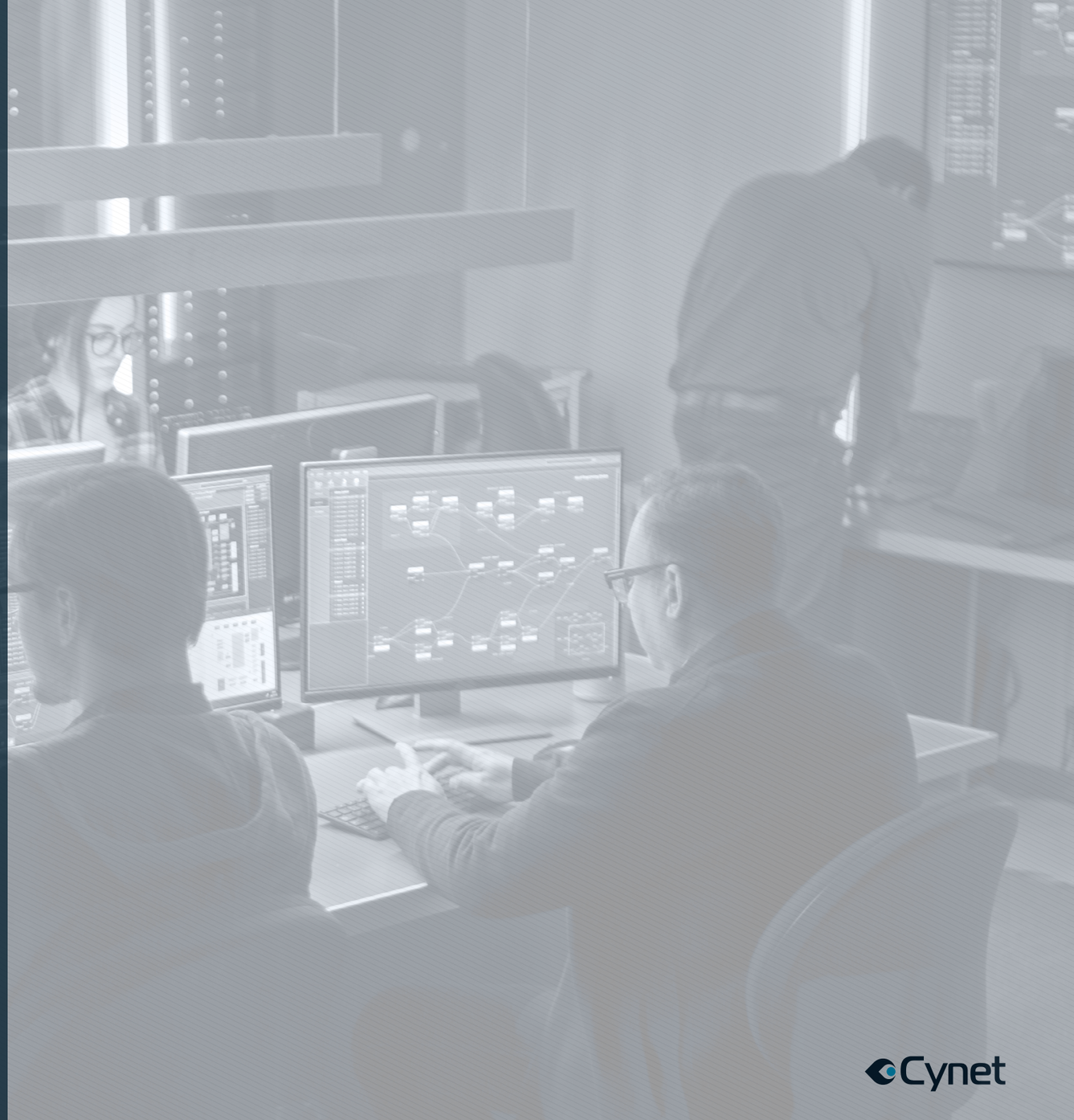
Creating a Large Company Security Stack on a Lean Company Budget

Introduction

Cybersecurity practitioners know that threats are expanding, attacks are proliferating, and companies are more at risk than ever. The typical solution? To expand cybersecurity stacks to address new threats and techniques. Essentially, we've entered an arms race with malicious actors. Attackers find new, more dangerous and stealthier attack tactics, and we build higher walls, add more technologies, and expand our stacks to meet the challenge.

This is now the way of the world for enterprise-level companies. Budgets keep expanding to buy better platforms, add new services, and keep organizations protected. Spending money is a necessary ingredient of a strong defense. But what about the companies that don't have the budget? What can a leaner company do when they face the same threats as a major corporation, with only a fraction of the resources at hand?

The answer used to be "not much", but that's hardly the case today. Although there are hundreds of platforms, tools, and services organizations can use to defend themselves, leaner companies don't need many of them. In fact, lean organizations can find ways to easily gain the protections of a large company security stack without having to overextend themselves or sacrifice their organizations' defenses. The question is, how do you do it?

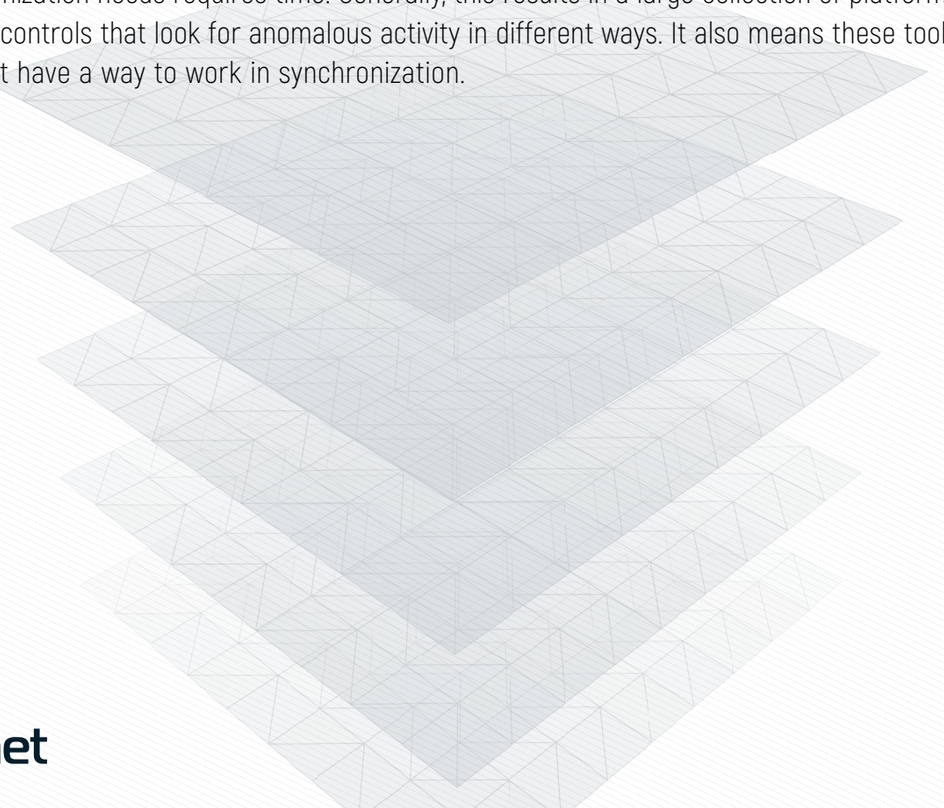


Cynet

The breach protection essentials

Building a security stack today requires multiple moving parts, as well as tools to manage all the disparate technologies. At large companies, this usually falls on members of the security team whose job is to ensure everything is working harmoniously. To better understand what a "large company" security stack looks like, let's break down the components.

Most organizations follow a similar pattern when building or upgrading their breach protection stack – they research, evaluate, install, and then learn how to operate multiple prevention/detection tools. Adding new tools is complex and ensuring the tools do what an organization needs requires time. Generally, this results in a large collection of platforms and controls that look for anomalous activity in different ways. It also means these tools must have a way to work in synchronization.



Cynet

The side effects of layered protection

If an organization follows the layered protection principle, multiple tools are required to achieve full protection. The key philosophy is that no tool is 100% effective, so there must always be redundancies for when one fails. This means most organizations will have many, or all of the following:

- Next-generation antivirus (NGAV)
- Endpoint protection (EPP)
- Endpoint detection and response (EDR)
- User and entity behavior analysis (UEBA)
- Network traffic analysis (NTA)
- Email protection
- Deception technology
- Cloud access security broker (CASB)

Each of these tools collect massive amounts of data and signals, and then constantly issue alerts and notifications. Managing each individually would be logistically impossible.

Finding order in the signals chaos

This is where security information and event management (SIEM) come in. As the volume of data, signals, and alerts increase, organizations need a way to manage the whole system and SIEMs offer a ready-made fix. They collect, normalize, and integrate all the disparate signals from detection and prevention tools to prioritize and make sense of all the information. This provides a significant increase in visibility as it reduces the need to monitor every minor detail in favor of a single pane of glass view.

Unfortunately, it also comes with downsides. On top of the multitude of tools organizations already pay for, they must also invest in a SIEM – both in money and resources. Setting aside the financial cost, SIEMs require careful calibration and installation to properly integrate the various signals, manage updates and compatibility, and constant testing to ensure everything is running smoothly.

Drowning in alerts

SIEMs might help organize the chaos, but they cannot fully remove it. One of the biggest bottlenecks for many security teams – especially leaner ones – is the volume of alerts a traditional security stack will produce. Handling investigation and response for each alert manually is simply unfeasible. Moreover, dangerous alerts (such as ransomware) require immediate action and multiple steps to resolve before the threat proliferates.

This creates a need for an additional step in the security chain - response automation. However, to automate your cybersecurity workflows, you need yet another tool.

Cynet

Automating investigation and response

Security orchestration, automation, and response (SOAR) platforms have become a key ingredient in security organizations' ability to properly respond to constant threats. If SIEM tools are the intelligence part of a security stack, SOAR tools offer action.

SOAR tools let organizations automate large parts of their cybersecurity operations - investigation, response, and remediation - and optimize response times and results. Often, they'll use playbooks (pre-written automated responses to malicious actions) to accelerate remediation and reduce the need for human intervention.

However, they suffer the same downsides as SIEM tools. They're expensive, they require a lot of manual input – including installation and integration, maintenance, and constant testing – and they add more complexity and cost to an already unwieldy security stack.

Cynet

How can lean teams manage all this?

The type of stack laid out above is far more common among organizations that are well-funded and well-resourced. Even so, this represents just the basics. For leaner teams, finding the right security stack requires approaching the challenge in a different way. Instead of expanding the number of hyper-specialized tools and adding more complexity, they must find ways to make it more agile and adaptable.

Most often, leaner security teams will leverage external help in the form of managed detection and response (MDR) services, which can provide crucial manpower and expertise to any security team. The level of assistance can vary greatly from general monitoring and notification to 24/7 support and threat hunting. However, this also raises the price tag of a full-fledged security stack.

Cynet

Simplifying security stacks

Leaner companies – those with limited budgets, leaner security teams, and fewer resources – simply cannot afford the complex security stacks implemented by their Fortune 2000 peers. A lean business may have an NGAV or an EDR or even a network detection and response (NDR) platform, but usually not all of them.

This turns their security into a single layer, expanding the threat surface for attackers and limiting the organizations' ability to mitigate the damage. Moreover, leaner security teams likely do the work manually, reducing their ability to react swiftly and effectively. From threat hunting to alert management, this means much fewer time spent on crucial tasks. They're also missing important signals, alerts, and actual threats trying to sort through the mountain of data they amass.

The answer is not to attempt to emulate larger security teams' stacks, but to find solutions that work within a lean security team's framework. This is where extended detection and response (XDR) tools come in.

Cynet

Consolidating tools for greater visibility

One of the biggest issues with tools like EDR and EPP platforms is that their focus – the endpoint – is not the only attack surface malicious actors use or rely on to penetrate a company's systems. Indeed, many attacks only become dangerous long after they've infiltrated a network. Therefore, overly prioritizing the endpoint limits visibility and lowers the impact of a security stack.

XDRs, on the other hand, include a variety of tools packaged in a single platform that offer much greater visibility across an organization's entire environment. Instead of a singular focus on endpoints, XDRs usually include tools such as UEBA and NDR that increase the area teams can monitor exponentially. This in turn reduces the capacity of malicious actors to move laterally across a network and can help detect seemingly harmless actions that may actually be parts of an attack.

Most importantly, XDRs prioritize automating detection and response, as well as investigation. This reduces the manual workload, as well as the strain that comes with handling the normal volume of alerts that a complex security stack generates. XDRs also offers the three key capabilities associated with a large company security stack discussed above in a single, unified platform:

Prevention and detection

Think about the list of separate tools mentioned at the beginning of this eBook. Each tool normally requires a separate interface, each of which produces its own signals, alerts, and data. Moreover, each tool produces this data for each component being protected. This alert overload makes a conglomeration of tools less useful than a single one.

XDRs include many (and in some cases all) of these prevention and detection tools natively. This is beneficial in two ways. First, it means that all signals and data are standardized and already integrated. This makes it easier to process, creates a more reliable sorting and investigation method, and keeps alerts under control. Second, it can reduce the number of false positives and provide much faster response since the tool doing the detection is the same one responding to a potential threat.

Instead of having to hop around to multiple platforms, XDRs are SIEM-like in their ability to centralize data flows and provide a single truth that improves detection and response.

Automated response

Perhaps the biggest differentiator offered by XDRs is their ability to automate large parts of a company's cybersecurity operations. Using the input from the platforms' detection tools, as well as connecting with every endpoint, network, and user in an environment, XDRs can typically respond much faster than their SOAR counterparts.

Automated responses require the ability to quickly understand the situation and apply the right response. For complex SOAR tools that must interact with tens of different tools, this means slower responses. XDRs provide the ability to trace an attack from its source through its conclusion more easily.

Perhaps even more crucially, XDRs can offer a much broader range of responses than traditional EDR tools. For example, instead of simply deleting a malicious file on an endpoint, and XDR could trace its passage, find other activity on the network that might be connected, and immediately disconnect any device that displays similar suspicious behavior.

MDR services

Most XDR providers offer an optional MDR service with their platform. The reasoning is simple. Even with more advanced and complex tools to defend themselves, organizations with lean security teams must still prioritize their scarce time and resources to make the greatest immediate impact. This means that many important tasks, such as threat hunting and even simply keeping a constant eye out for threats in the environment, are often deprioritized in favor of responding to immediate problems.

MDRs provide a buffer between an organization's capabilities and their needs, can help round out any gaps and offer a more robust defense. However, most vendors don't include this service in their platform license. Instead, it's often an additional fee or a separate third-party service. Even so, it's a crucial aid for leaner organizations that cannot afford to hire full security teams.

The advantage of a one-stop shop

Regardless of the price structure a particular XDR vendor might offer, the results are the same – XDRs offer protection equal to (and in some cases better than) traditional security stacks for a variety of reasons. Primarily, the ability to manage an entire suite of security tools in a single dashboard, with native integration and a single data flow, makes it much easier for security teams of any size to manage their organization's defenses.

Beyond that, it also removes many of the biggest challenges traditional stacks face. For instance, instead of having to manage a complex update and patch schedule for a variety of tools – which must then be reconfigured and retested with a SIEM and/or SOAR tool – organizations simply need a single update, patch, or fix to avoid any potential security lapses.

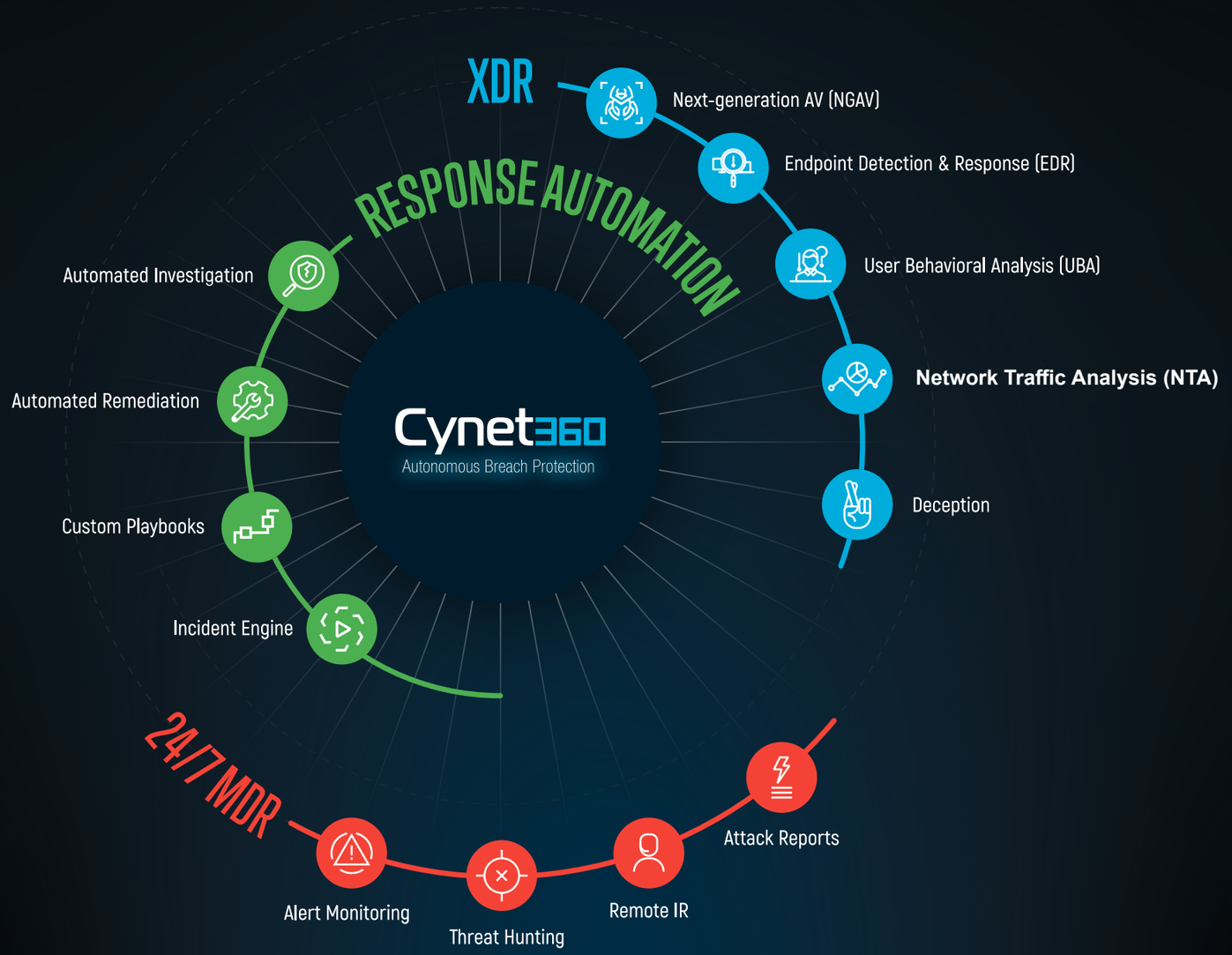
More importantly, it reduces the technical capital required to implement these protections. Instead of lengthy deployments, constant training, and complications stemming from human error and faulty implementations, many XDRs offer simple and fast installation that requires little more than a few clicks and minutes.

Finally, all of this would be irrelevant if an XDR didn't solve the key problem – cost. Here is a major difference between XDRs and traditional "large company" stacks. Instead of multiple licenses, costs and vendor management headaches, organizations can gain an equivalent security posture that costs a fraction of the cost and reduces ongoing maintenance to a minimum. In the end, it's not about how to get better with more tools, but how to get more with less and avoid security lapses that might come from increasingly complex and complicated systems.

About Cynet

Cynet enables any organization to put its cybersecurity on autopilot, streamlining and automating their entire security operations while providing enhanced levels of 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



Cynet