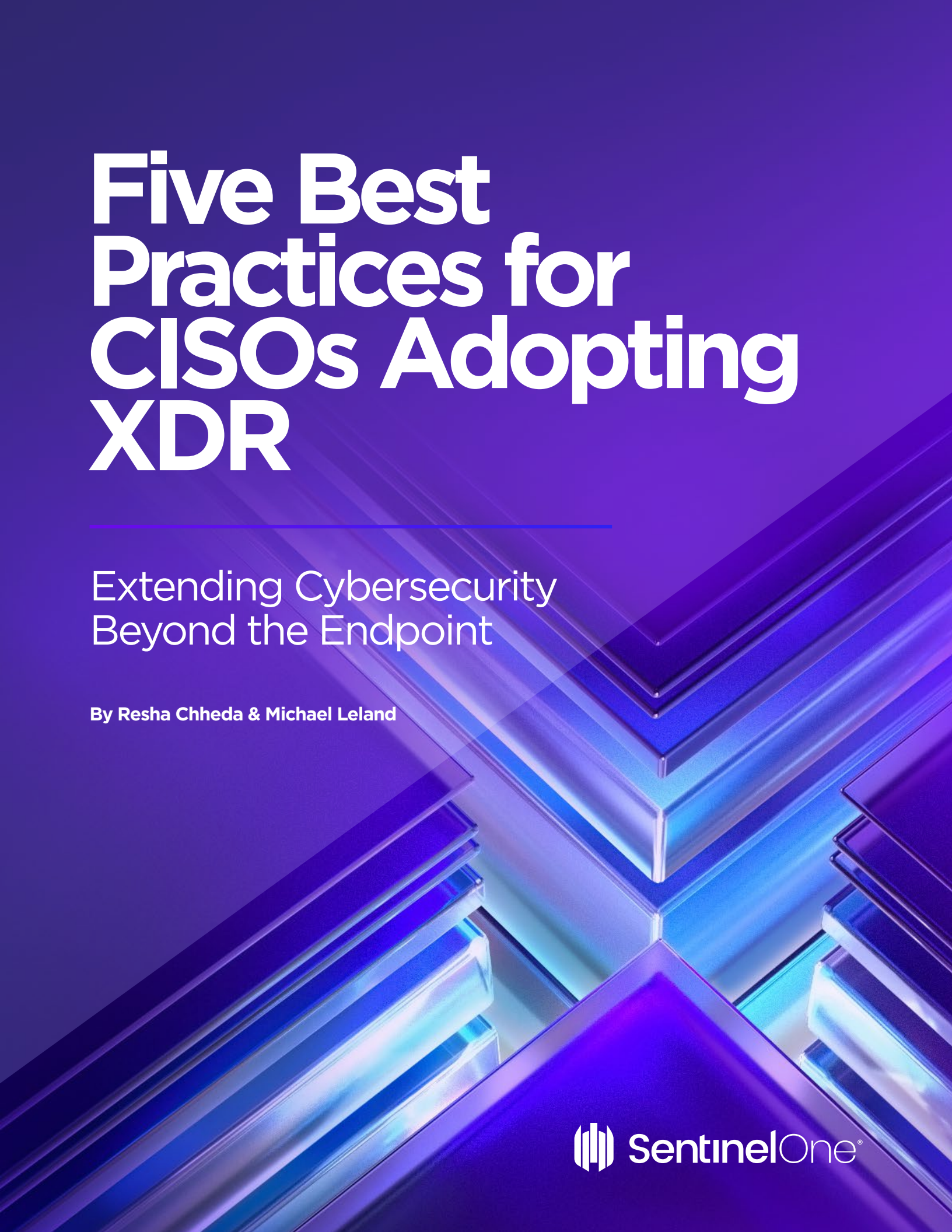
Five Best Practices for CISOs Adopting XDR

Extending Cybersecurity Beyond the Endpoint

By Resha Chheda & Michael Leland



SentinelOne®

Table of Contents

INTRODUCTION

The XDR Buzz

Any New Technology Enters The Marketplace Amid a Blaze Of Hype

This is as true for a new smartphone as it is for the latest games console or even the latest development in cybersecurity. That's the case with eXtended Detection and Response (XDR), which has grown in profile over the last few years, to become the new buzzword in cybersecurity.

40%

Of organizations will use XDR in the next 5 years

The hype can often be little more than over-zealous marketing, but sometimes it's justified. One new technology that is certainly worth the buzz is XDR, which addresses a number of weaknesses in existing cybersecurity tools and has the potential to improve incident response and remediation while also lowering costs and increasing productivity.

Too good to be true? Well, nothing is perfect but we think that once you've read this ebook you will be convinced that XDR is an important tool for the modern SOC of the future. And it is the future, for now, because according to Gartner, fewer than five percent of organizations were using XDR at the beginning of 2022. However, they expect that total to grow to 40 percent over the next five years.

There are several reasons for that, as we will discuss in the first chapter of this ebook. Cybersecurity teams are currently in a difficult position. Threats are increasing and so are the number of tools being deployed to deal with them. However, managing those tools and responding to the alerts they trigger

just increases the burden on already overstretched teams. With a shortage of cybersecurity skills, that pressure is hard to solve by adding more people.

Though the premise of XDR has been talked about a lot over the last year by industry leaders and the analyst community, XDR remains an evolving concept. Understandably there is still confusion in some quarters over exactly what it is, and we'll deal with some of the misconceptions in the second chapter of the ebook.

XDR can be a valuable tool to handle many of today's cybersecurity problems. We'll look at that - and the impact XDR can have on meaningful KPIs - in subsequent chapters. Our conclusion talks about five key best practices you should consider on your XDR journey.

SentinelOne's own Singularity XDR has, over the last few months, outperformed every other vendor in the MITRE ATT&CK evaluations in more ways than one, achieved unrivaled success in the Gartner Critical Capabilities report, and positioned itself firmly in the leaders quadrant of the 2021 Gartner EPP Magic Quadrant.

Every external data point is important to us, and we pride ourselves on being a data-driven company, but perhaps no data point is as good an indicator of how your industry sees you as the extent to which they emulate your choices. We are convinced that XDR has a vital role to play in the future of cybersecurity. After reading this paper, we think that you will be too.

> "Fewer than five percent of organizations were using XDR at the beginning of 2022. That number is expected to grow to 40 percent over the next five years
>
> GARTNER

CHAPTER 02

The Current Market State

CHAPTER 02

High Volume, High Velocity, Sophisticated Threats

Today's security teams are facing a vast range of threats. Ransomware attacks are more widespread and ransom demands are increasing. Cryptojacking, where criminals steal computing power to mine cryptocurrency, has become more common.

Meanwhile, malware, phishing and other attacks must be guarded against and there are emerging threats such as deep fakes and AI-driven attacks that are becoming more prevalent and harder to detect and defend against. And these attacks can also be indirect: companies can find themselves compromised by attacks on third-parties within an organizations' software supply chain, either deliberately or as collateral damage.

As attack vectors multiply and the threat landscape evolves and extends rapidly, from endpoints to networks to the cloud, many enterprises address each new vector with a best-in-class solution addressing those specific attack surfaces. This is an understandable response, but it creates a forest of disconnected tools that make it hard for security teams to see the forest for the trees. Security data is collected, stored in disparate silos, and analyzed in isolation, without crucial context or correlation, leaving gaps in what security teams can detect and analyze - and, therefore, what they can respond to.

Integrating these tools is often costly and can be difficult, or even impossible. Even tools from the same vendor might be incompatible if they don't have common data formats, event taxonomies, or APIs.

"

It takes an average of 287 days to identify a data breach with containment averaging 80 days.

PONEMON COST OF DATA BREACH REPORT

82%

Credential theft and misuse factors into 82% of all reported breaches.*

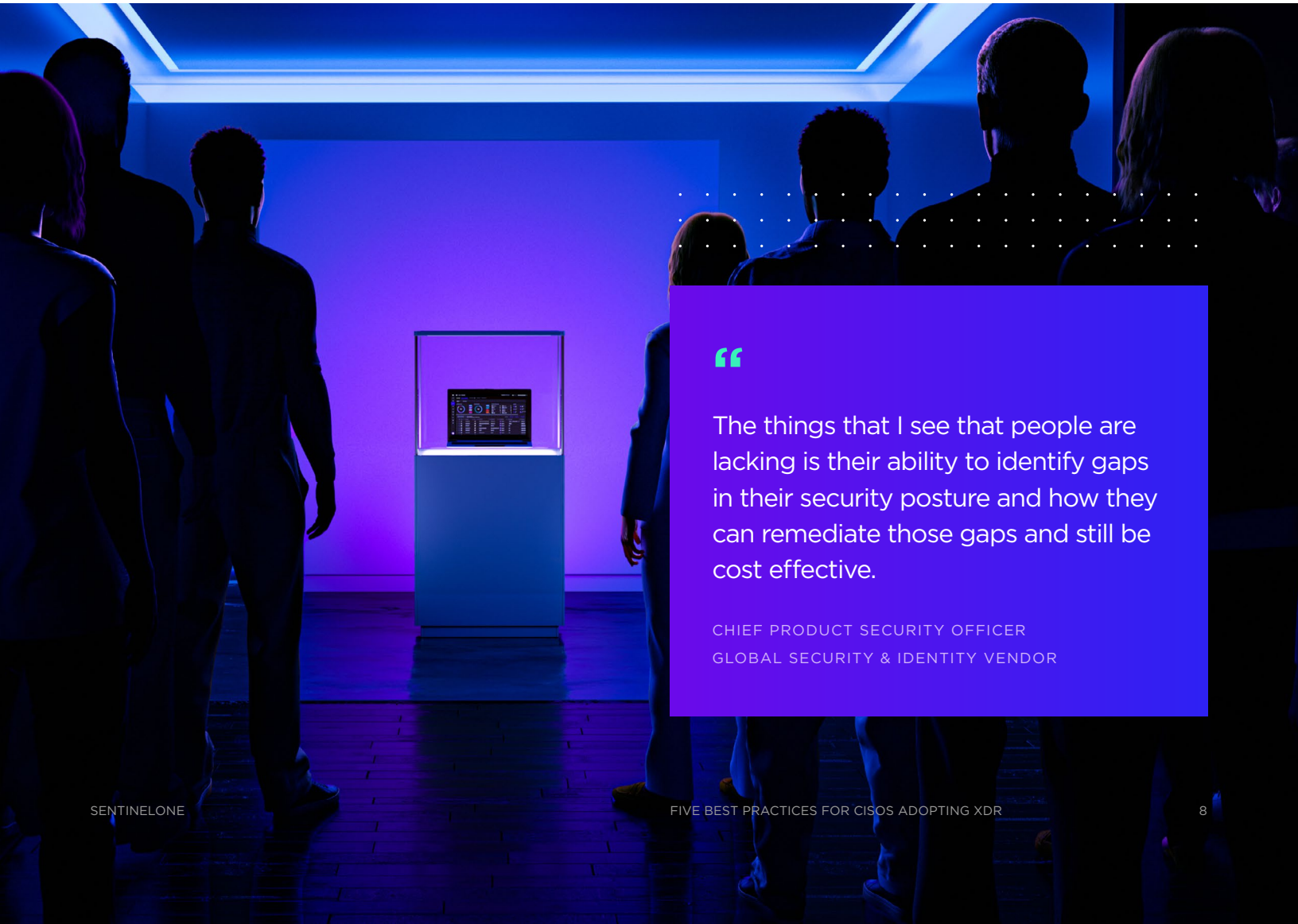
*Source: Verizon Data Breach Report, 2022

Overwhelmed Security Teams

The overwhelming majority of data breaches involve some kind of human action, whether that is manipulation via phishing, malicious action by an insider, or simply human error. That means the security team must not only guard against threats but also perform an educational role, ensuring that everyone in the organization understands that they have a role to play in cybersecurity.

This is a strain on a team that spends much of its time carrying out repetitive and tedious tasks just to ensure basic safety. As the number of deployed security solutions grows across the enterprise, the capacity needed to manage them and respond effectively to their alerts grows with it. This can put an enormous strain on security administrators, who can quickly become overwhelmed by this torrent of data.

Managing a seemingly endless string of alerts and evaluating incidents makes it more likely that something will be missed because staff start to operate on 'autopilot'. This work also keeps them from more rewarding tasks that make better use of their expertise. And all of this is happening at a time when there's a shortage of skilled cybersecurity experts, so the staff that are doing the job are overworked and demoralized. This makes retention harder, which exacerbates the skills shortage.



> "The things that I see that people are lacking is their ability to identify gaps in their security posture and how they can remediate those gaps and still be cost effective.
>
> CHIEF PRODUCT SECURITY OFFICER
> GLOBAL SECURITY & IDENTITY VENDOR

Broken Existing Security Tools

Of course, none of this is new. This has been the status quo for some time now, which is important because current solutions are not doing enough to address it. Security Information & Event Management (SIEM) tools and Security Orchestration & Automated Response (SOAR) platforms have failed to address these challenges because of complexity and cost.

Mature security operations teams use SOAR platforms to construct and run multi-stage playbooks that automate actions across an API-connected ecosystem of security tools and solutions. But this cost and complexity means that it is appropriate only for mature teams who find themselves lucky enough to employ teams of highly qualified programmers and full-stack developers.

As for SIEM, in a recent report Gartner wrote that "many organizations have not deployed SIEM tools, have failed or incomplete implementations, or only use SIEM for log storage and compliance." The report added: "XDR products aim to solve the primary challenges with SIEM products, such as effective detection of and response to targeted attacks, including native support for behavior analysis, threat intelligence, behavior profiling and analytics."

XDR products aim to solve the primary challenges with SIEM products, such as effective detection of and response to targeted attacks

> "One of the big struggles that always gets brought up in higher-level CIO conversations is 'It is challenging to keep our security controls aligned with the pace of change going on in our IT infrastructure.' Alignment gaps, even short lived, result in added risk to the overall operation.
>
> DAVE GRUBER
> PRINCIPAL CYBERSECURITY ANALYST AT ENTERPRISE STRATEGY

CHAPTER 03

The Rise of XDR

CHAPTER 03

XDR Has Emerged As a Simpler And More Efficient Way to Deal With the Broad Array of Threats

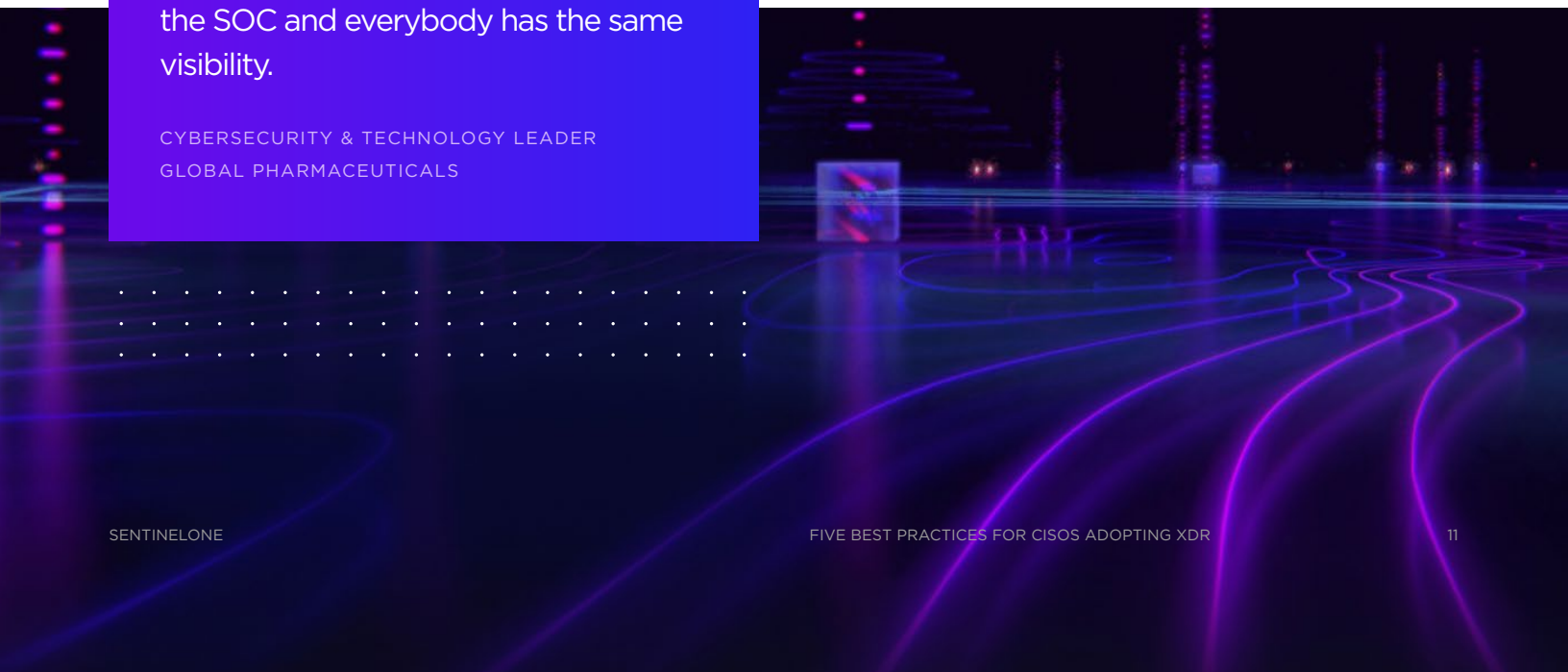
It is not a product that you buy but a new way of managing security. An XDR platform collects and correlates data across a broad array of network and security surfaces, including servers, endpoints, cloud workloads, network intrusion prevention systems, identity and access management products, email and more.

It analyses the data it collects, then prioritizes and sorts the results, identifying even advanced threats to prevent breaches and attacks. Compared to older tools and technologies, XDR provides a higher fidelity and confidence of cyber awareness and allows security teams to identify and eliminate security vulnerabilities without adding extra tools or more people.

> “We want an enterprise-first mindset, making sure that we’re looking holistically across the organization so the SOC and everybody has the same visibility.
>
> CYBERSECURITY & TECHNOLOGY LEADER
> GLOBAL PHARMACEUTICALS

It’s still a relatively new term, in a sea of acronyms and new products, so it is understandable that there is often confusion about what exactly it is. Gartner’s definition is: “XDR is a SaaS-based, vendor-specific, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed security components.”

Some people think it is a new way to describe an SIEM tool, but that isn’t correct. Others see it as another name for Endpoint Detection and Response (EDR), which isn’t quite correct either. There are important differences between XDR and both of these older technologies.



XDR Versus SIEM

SIEM has taken a broad approach from the outset, collecting, aggregating and analyzing a vast array of log and event data from almost every source across the enterprise. That includes governance and compliance, rule-based pattern matching, heuristic and behavioral threat detection like UEBA (User and Entity Behavior Analytics), and hunting across telemetry sources for IOCs or atomic indicators. However, while XDR also analyses a broad range of sources, there are crucial differences.

SIEM tools typically require a lot of fine-tuning and effort to implement. This adds cost and complexity. SIEM platforms were never designed to scale to the level required to ingest the massive volume of event telemetry from noisy platforms like cloud infrastructure or even EDR. Security teams can be overwhelmed by the sheer number of alerts coming from a SIEM tool, which means that critical alerts can be lost in the noise or ignored. In addition, even though a SIEM captures data from dozens of sources and sensors, it is still a passive analytical tool that issues alerts.

An XDR platform solves the challenges of an SIEM tool with effective detection and response to targeted attacks, including behavior analysis, threat intelligence, behavior profiling, and analytics.

> “
>
> My definition of XDR is one control plane for our security team with as much context and data as possible from other telemetry sources surrounding whatever particular event my team happens to be looking at.
>
> CISO, OIL & GAS MULTINATIONAL

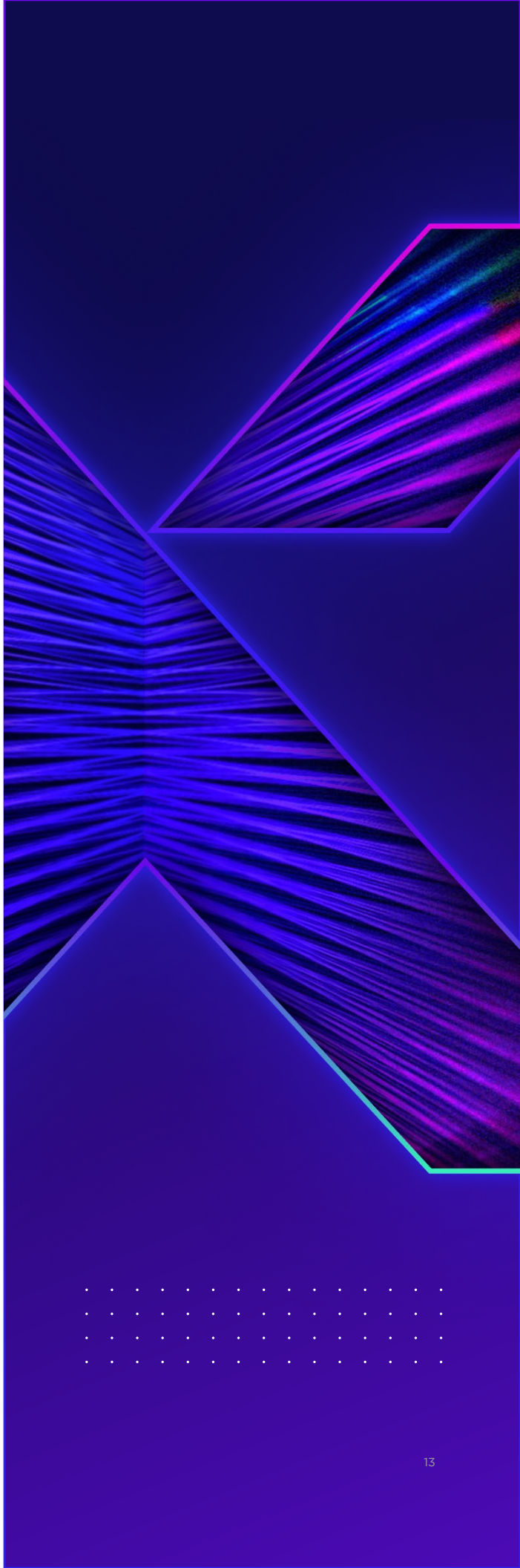
	SIEM	XDR
Business Focus	Risk-Centric	Threat-Centric
Deployment Models	On-Premises, Cloud, Hybrid	Cloud-Native, Hybrid
Use Cases	• Compliance (Log Management) • Reporting • Threat Detection (Correlation) • Triage & Hunting	• Threat Detection (AI) • Triage & Hunting • Intelligent Response
Data Models	Rigid, normalized, structured data schema	Open, flexible data architecture
Analytics	Rule-based correlation + ML (boiled on)	Machine Learning models + Rules
Operational Models	• Consume Everything (that you can afford) • Build Static Detection Logic • Determine Actionability	• Consume Relevant / Actionable Data • Enrich Investigations / Net New Detections • Prescribe One-Click Responses

XDR versus EDR

While XDR and SIEM are tangentially related, the new technology has more in common with EDR. In fact, XDR is an evolution of EDR that broadens the scope of detection far beyond endpoints. EDR has been around for about a decade now. It monitors endpoints, recording every activity and event in the search for suspicious behavior. Then it correlates information to add vital context to detect advanced threats. Finally, it runs automated response activity, such as isolating an infected endpoint from the network, in near real time.

EDR solutions are excellent for obtaining security information from the organization's endpoints. However, they don't offer the telemetry necessary to provide the broad organization-wide visibility that gives an accurate depiction of an attacker's behavior and goals, which may span multiple sources. XDR solves this problem by gathering telemetry from multiple security layers and potential attack points. That enables continuous monitoring and near real-time detection and remediation of threats identified on protected assets including endpoints, servers, containers, cloud workloads and mobile devices. Additionally, with the help of threat intelligence feeds, XDR systems can proactively search for concealed threats across a sea of historical telemetry stored in a cloud-scale data lake.

XDR improves on the threat detection and adversarial defense capabilities of EDR. It unifies visibility and control across all connected security platforms, which provides context around potential threats that makes remediation efforts easier. It also allows security teams to react faster because of the correlation of data from multiple security vectors. With improved triage and automated contextual enrichment teams can respond more quickly, before the scope of the threat broadens. Out-of-the-box integrations and pre-tuned detection mechanisms across multiple different products and platforms help improve productivity, threat detection, and forensics.



CHAPTER 04

Why XDR is Emerging as The Answer for CISOs

CHAPTER 04

The Threat Landscape Is Broader And Deeper

Existing tools are costly and complex, and the cybersecurity industry relies on too few staff under too much pressure. XDR can help by providing improved protection, better detection capabilities, greater productivity and lower ownership costs. This is what older technologies, such as SIEM, promised but were never able to deliver.

01. Comprehensive Detection & Protection

XDR offers improved protection, detection and response capabilities in part because it removes the fragmentation that holds back existing systems. Unchecked, that leads to longer dwell times and threats that are harder to detect, but XDR shares local threat intelligence immediately across all the component security products, which makes blocking threats everywhere more efficient and in most cases, fully automated across the connected ecosystem of security tools.

> “
>
> I think historically challenges have always been around finding good, solid people. And when you have budgetary constraints, that’s where the people game becomes a little difficult.
>
> CHIEF PRODUCT SECURITY OFFICER
> GLOBAL PHYSICAL SECURITY & IDENTITY VENDOR

02.
Better TCO

Overall, XDR is economical and less complex than an SIEM tool and it is broader and more capable than EDR. XDR enhances existing security solutions by making use of current technologies to proactively identify and manage security threats. It aims to converge siloed security tools and is a powerful force multiplier to reactive security solutions. An effective detection and response capability can be provided by one package instead of many. Acquisition costs, support costs and training costs are all lower and security operations productivity increases.

03.
Centralized Controls

With XDR, organizations are better able to address cybersecurity risks from a unified standpoint. XDR's single pool of raw data collates information from across the entire ecosystem, which means threat detection and response is faster, deeper and more effective than with EDR. This also means that XDR can provide more visibility and context. Incidents that would not otherwise have been addressed will surface, allowing security teams to act quickly to identify and remediate the attack and reduce its scope.

04.
Improved Security Team Productivity

As Gartner describes it: "The benefit is that analysts spend more time on 'incidents' and less time on a stream of 'alerts' that often lack context. For example, network alerts can be confirmed or debunked by endpoint activity analysis. The total volume of alerts can be reduced by orders of magnitude by combining individual product alerts into systemwide incidents."

A centralized tool means that incidents can be dealt with quickly because staff have the necessary data and context in one place, but it also reduces the need for training because staff no longer have to learn multiple workflows, dashboards and tools. The end result is security operations analysts who are more empowered, less overwhelmed and in greater control of daily security information flows.

> “
>
> Being able to play nice with other tools in the SOC is important to us so that we can share data back and forth to get enriched visibility. My security team can follow the storyline and have all the details they need in one place.
>
> CYBERSECURITY & TECHNOLOGY LEADER
> GLOBAL PHARMACEUTICALS

05.
Automation

XDR provides automated tools boosting up detection and response while diminishing manual steps required to process security procedures. Combining multiple detection methods in the way that XDR does means that it can combine weak signals from multiple areas into a stronger signal or take externally acquired threat data and add that to internal sources. All this can once again be enhanced with automation, which makes it much less likely that important alerts will be missed.

Many security solutions generate alerts that need investigation from the cybersecurity team. This is not always necessary and, given the number of alerts these systems can generate, it is frequently impractical as well. Many security teams do not have the staff required to respond to every incident. XDR frees capacity among the security team by automating repetitive tasks with AI and built-in context and correlation tools. Less time is spent on a never-ending flood of alerts and more time is available for the smaller number of incidents that require manual investigation.

CHAPTER 05

Key Considerations While Adopting XDR

Evaluate

CISOs who are considering XDR should start with the obvious question of what they want to protect. What are the 'Crown Jewels' that must be protected at all costs? What other areas are important to protect? Then they must consider their existing tools. These need to be offering sufficient protection so that the enterprise is prepared for an attack. If the existing tools don't do that then there will be gaps that need to be filled - often with more tools.

Simplify

Second, it is worth asking whether the existing tools can be simplified. They might be providing sufficient protection but is their data connected? Are they swamping the security team with alerts? If they are then there is scope to simplify. The machines should be a force-multiplier for the security team, not the other way round.

Automate

Finally, the CISO should consider how much of their security response is automated. Are alerts having to be dealt with manually? If so, this will be another time-consuming task for security staff. This is another area where XDR can help. XDR can be a kind of SOAR-lite - a simple, intuitive, zero-code solution that provides consistent and measurable actionability from the XDR platform to connected security tools.

Questions to Consider on Your XDR Journey

01.
What are the 'Crown Jewels' that must be protected at all costs? What other areas are important to protect? Are there any visibility gaps?

02.
Is all of the data connected? Are the tools swamping the security team with alerts? How quickly can an analyst identify and respond to a high-severity threat?

03.
Is your team spending too much time doing manual tasks? Does your secops team have a library of response playbooks to deal with specific threat activities and if so, are they automated?

CHAPTER 06

5 Best Practices for CISOs Adopting XDR

CHAPTER 06

Hopefully we have established that there is more to XDR than just 'buzz'. With cybersecurity teams facing ever-evolving challenges, XDR is a vital tool.

The Five Best Practices for CISOs Considering XDR

01

Leverage a Strong EDR Foundation

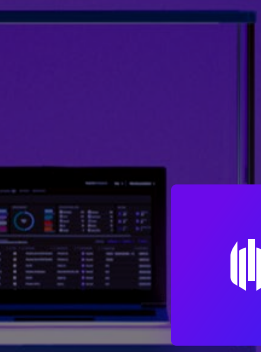
XDR is based on a solid EDR foundation and all the benefits that brings. That means, for example, drawing on EDR's high fidelity telemetry to provide all-important supporting data from endpoints, as well as the real-time detection and remediation capabilities of EDR. However, XDR extends beyond endpoint protection to providing detection and response coverage across the entire organization. This means that it provides greater visibility and more context into threats. The high fidelity telemetry that makes EDR so valuable and provides vital supporting data from endpoints, is now available from more sources. Likewise EDR's ability to offer real-time behavioral detection and remediation can be applied more broadly across the organization with XDR. Alerts that might otherwise have been missed at an early stage can now be identified earlier and remediated before they have a significant impact. And it is easier to get a more complete understanding of what is happening within the whole enterprise security estate.

SentinelOne's Singularity XDR lets analysts take advantage of insights from aggregated event information gathered from multiple tools and services and combined into a single, contextualized 'incident'. It also provides customers with a central enforcement and analytics layer point hub for complete enterprise visibility and autonomous prevention, detection, and response, helping organizations address cybersecurity challenges from a unified standpoint.

02

Maximize the Value of Your Existing Security Investments

XDR helps maximize the value of your security investments. While a native XDR requires the vendor to supply all the required sensors for typical use cases, an open XDR, concentrates on backend analytics and workflow and integrates with the organization's existing workflow. That makes sense because many organizations have tools and technologies deployed in their SOC that it would be wasteful to simply decommission. These best-in-breed technologies provide reliable point solution coverage and each comes with a steep learning curve and operational burden for SecOps efficiency. Switching those out for a new tool, simply starts you on another learning curve with a new burden. XDR can allow you to make use of these existing tools, connecting them through built-in integrations.



SentinelOne's Singularity Marketplace makes it easy to add integrations to third-party systems, such as SIEM or SOAR solutions, with just a few clicks. Email, identity management systems, cloud services and other third-party systems can all be brought into the XDR system, which is a huge improvement on having to secure each one individually and use a different dashboard to manage alerts. These integrations can then be enabled and automated without the need to write complex code.

03

Increase Efficiency of Your Security Team

XDR unburdens the SOC team. Cybersecurity analysts are already overloaded and the situation is likely to get worse as threats increase, tools proliferate and the skills shortage continues to negatively impact the efficacy of security operations practitioners. That's why it's important to have a tool like the behavioral engine in SentinelOne's XDR solution, which automatically correlates related activity into unified alerts, which drastically simplifies the task for analysts.

In the end, fewer alerts, fewer clicks and fewer screens mean increased SOC efficiency.

For example, with our Recorded Future integration, threats are auto enriched from 800,000+ sources, enabling customers to accelerate threat investigation and triage capabilities. Customers can also make use of an extensive library of threat hunting queries curated by SentinelOne research which continually evaluates new methodologies to uncover new IOCs and Tactics, Techniques, and Procedures (TTPs). But all of this can be consolidated into fewer alerts, which reduces the strain on security teams. For example, in the 2022 MITRE Engenuity's ATT&CK Evaluation, which tested leading XDR solutions against a range of benchmarks, SentinelOne's Singularity XDR consolidated two days of continuous testing into just nine campaign-level console alerts. This demonstrates the ability to alleviate SOC burdens by using machine speed to correlate and contextualize large numbers of alerts. However, Singularity uses patented Storyline Active Response (STAR) technology to fully index every event as it happens in real time, allowing for a real-time view of what is happening and where it is happening, so that cybersecurity teams don't have to try to piece together events afterwards, when it is too late.

04

Automate Remediation to Contain Attacks Faster

Central to the above points is automation. It's crucial to maximizing the value of your existing tools and to unburdening the SOC team. Automation can improve both threat detection and response. Automation reduces the amount of manual effort needed, helps with alert fatigue, and significantly lowers the skillset barrier of responding to alerts. All of this leads to better outcomes for the SOC in the form of shorter containment times and an overall reduction in response times.

In SentinelOne's Singularity XDR solution, for example, STAR is our cloud-based Automated Hunting, Detection, and Response engine. Every query that can be run in Singularity can also be defined as a rule that monitors every incoming data-point in near real-time. Once triggered, these rules can initiate anything from a simple alert to a complex playbook of actions. XDR expands that powerful capability to their entire connected ecosystem of security tools across the enterprise. Automated response actions now extend to third-party applications. For example, you can force step-up authentication in your identity management tools when the system detects suspicious behavior. Users will then be asked to submit additional forms of authentication. And you can automatically block email or web connectivity for suspicious resources or users accordingly, again based on predefined rules and triggers. This provides cybersecurity professionals with vital third-party risk calculations and management tools in support of new convictions - ultimately enabling SOC teams to contain attacks faster.

05

Deliver Measurable Outcomes

A final takeaway is that ultimately, XDR is means to an end and needs to deliver the KPIs and proof points that the board wants to see. As concern grows around cyberthreats, the board will increasingly demand evidence that the organization is protected from the latest threats and is investing appropriately to ensure tomorrow's adversarial techniques will be quickly and effectively detected and mitigated. XDR is effective in detecting techniques and tactics that indicate malicious behavior across the entire enterprise security estate and can monitor stealth behavior, effectively identify fileless attacks, lateral movement, and actively executing rootkits.

This capability, and the above benefits, mean that XDR can deliver improvements in Mean Time to Detect (MTTD), Mean Time to Investigate (MTTI) and Mean Time to Respond (MTTR) - giving the board reassurance that they are protected. Importantly, XDR does this while also delivering efficiency benefits and cost savings.

> "When I joined the organization three years ago, we were probably sitting in the 50 to 60 percent endpoint protection coverage. This year our objective was to get to 95 percent. We had a big celebration internally when we hit 95 percent for the first time. There are some small pockets of a few other things, but that's our primary KPI.
>
> CYBERSECURITY & TECHNOLOGY LEADER
> GLOBAL HEALTH IT VENDOR

CHAPTER 07

Parting Thoughts

CHAPTER 07

What CISOs Have to Do With XDR is Go Beyond the Buzz and Focus on What Really Matters: the Outcomes it Can Deliver

CISOs must identify KPIs not only to determine the effectiveness of their tools and processes but also to communicate that effectiveness to the board. Cybersecurity is not always something the board understands, but board members will be aware of the growing risk of attacks and will want to know that their defenses are aligned with the company's risk profile and appetite.

The world of cybersecurity is constantly changing and it is often wise to be skeptical about new trends. However, as we have explained in this ebook, XDR is more than a new trend. It is not a new buzzword or a hot new product. Rather, it is a new way of thinking about security, a platform that can be deployed to make an organization fit for the modern challenges in the cybersecurity world. With teams short of staff and those staff overwhelmed by alerts and drowned in data, a new approach is long overdue. XDR goes beyond the latest marketing buzzwords to deliver meaningful differences for organizations of every size. It is an essential part of the future of the modern SOC.

SentinelOne®

Visit SentinelOne.com for more details about XDR.
To contact sales email sales@sentinelone.com
or call +1-855-868-3733.

More Capability. Less Complexity.

SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution.

S1-eBook-003-Five_Best_Practices_for_CISOs_Adopting_XDR_05272022