



# A new world demands a new approach to cybersecurity

Protect your business and take back your time with a robust XDR approach to cybersecurity.





# Now more than ever, cybersecurity is everyone's business.

**In a fully connected and distributed world, every organization is vulnerable to attack. Here's why your cybersecurity posture matters when the edge is expanding further than ever before.**

We see it everywhere: in how we work, live, socialize, and take care of ourselves. *Life can change in an instant.* Now, more than ever, we know that it's impossible to take our safety and security for granted. Today's unprecedented challenges have solidified a reality we've known for many years: **in the modern information age, data security and digital resilience are everyone's responsibility.**

**Any organization that deals with data is vulnerable,** from small players to large multinationals. Devastating ransomware attacks and public security breaches that compromise personal information are just two examples of attacks that could bring your company to a standstill. And, because **attackers can infiltrate your systems without your knowledge**, you could unknowingly give an attacker a considerable head start in damaging your organization by compromising your most precious assets: your data.

The sudden shift to remote work opened up more fissures in the cybersecurity landscape, from a sharp rise in phishing attacks to increased ransomware breaches. With bad actors emboldened, the likelihood and impact of cyber attacks have increased. These threats continue to evolve as attackers exploit uncertainty, unprecedented situations, and rapid organizational changes. As just one example, many ransomware

families are now equipped to steal data, not just encrypt files. As your organization adapts to changing conditions, you could face potentially significant cybersecurity challenges that demand a rapid and effective response.

151%

INCREASE IN RANSOMWARE IN  
1H 2021 COMPARED TO 1H 2020

US \$4.62M

AVERAGE COST OF  
RANSOMWARE BREACH (2020)



# When it comes to thwarting cyber attacks, it's *about time*.

**Deploying a robust cybersecurity solution to quickly address today's threats while anticipating future attacks has always been complicated. Today, it's become critical.**

In today's environment, **you need to assume that there is currently an adversary with malicious intent with a foothold in your environment.** Your responsibility is to find and eradicate that foothold before infiltrators compromise your systems.

While some threat vectors can do immediate damage, most attackers take their time after infiltrating your network. Malicious actors can gain access to your system without leaving a trail of evidence. The longer the dwell time between a security breach and the discovery of that breach, the more time you've given the hackers to perform reconnaissance and find ways to hurt your business. If you don't have any way of knowing that your company has been compromised, time will be on your adversaries' side.

And time is money. The faster a data breach can be identified and contained, the lower the monetary damages. Breaches with a lifecycle less than 200 days were on average \$1.26 million less costly than breaches with a lifecycle of more than 200 days (\$3.61 million vs. \$4.87 million respectively), a difference of 26 percent.

How can your organization recapture the time advantage from potential attackers? With threats constantly evolving, your cybersecurity solution must be able to meet the needs of today's environment and anticipate that adversaries will deploy ever more sophisticated attacks in the future. Many companies attempt to set up, integrate, and monitor tools to protect their data and network. But these do-it-yourself solutions can



be time-consuming, complicated, and expensive to deploy and maintain. Hiring, training, and maintaining a specialized, highly-trained team to stand up, maintain, and regularly update security solutions costs you both time and resources.

Even with adequate financial resources, cybersecurity experts are hard to find. It all adds up to an environment that can overwhelm even the most well-meaning organizations. The worst decision of all? The decision to do nothing and hope for the best, simply because you don't know where to start.

## 287 days

**AVERAGE DWELL TIME: THE AMOUNT OF TIME IT TOOK TO IDENTIFY AND CONTAIN A DATA BREACH IN 2020, A 2.8% PERCENT INCREASE OVER 2019.**

Ponemon, 2021 Cost of a Data Breach study

**ACCORDING TO PONEMON, ONLY 39 PERCENT OF SURVEY RESPONDENTS INDICATE THAT THEY ARE GETTING FULL VALUE FROM THEIR SECURITY INVESTMENTS.**



# A Common Challenge: Focusing on Tools not Telemetry

**eXtended Detection and Response offers next-level threat detection and response, accelerating your ability and effectiveness to “triangulate” threats.**

According to JupiterOne, **70% of respondents say that security hygiene and posture management has become more difficult over the past 2 years.**

In an attempt to solve this issue, organizations often stand up a SIEM (security information and event management) system to aggregate and correlate logs from their environment: a costly and complicated process. Yet **skilled adversaries know how to conceal themselves** to all but the most experienced security experts. The ability for organizations to rapidly and continuously analyze events, behaviors and alerts from all aspects of the security stack is paramount, but a SIEM alone lacks the context needed to accelerate detection and response times, monitor network flows, and continuously test configurations.

The solution is a cybersecurity program with the right combination of tools and techniques to

**BY REQUIRING YOU TO SPEND SO MUCH VALUABLE TIME WATCHING YOUR NETWORK, CYBERCRIMINALS ALREADY HAVE YOU AT A DISADVANTAGE.**

offer robust three-dimensional insight into your entire system. The more sources of telemetry your security solution draws from, the more accurate your view of your networks will be. Yet to be fully effective, your solution must be able to converge and correlate data in order to garner insights from the noise. This approach requires both an understanding of each security tool deployed, and the experience to be able to correlate the data

accurately. Without this level of expertise, simply layering on tool after tool can result in a cacophony of alerts, unnecessary redundancy, and an overall lack of efficacy that puts you at risk of missing critical alerts.

It's similar to the triangulation of mobile devices leveraging cell towers. Just as the more towers a cellular device pings off increases the effectiveness of triangulation, so it is with detection and response. Instead of relying on analyst interpretation from disparate and siloed tools; XDR (“eXtended” Detection and Response) offers next-level threat detection and response, collecting and automatically correlating data across multiple security layers and tools – email, endpoint, server, cloud workloads, and network – so threats can be detected faster and security analysts can improve investigation and response times. XDR accelerates your ability and effectiveness to “triangulate” threats.

XDR is architected to extend visibility and analysis to include threat intelligence, telemetries, vulnerabilities, and other relevant IT information. By choosing and integrating the right tools, and by understanding threat actors' behavior, you can achieve a fully-realized security program with a correlated single pane of glass allowing you to pinpoint and thwart attacks in real time.

**THE MORE POINTS OF INTEGRATED TELEMETRY YOU HAVE AND THE BETTER THEY WORK TOGETHER, THE FASTER YOU CAN TRIANGULATE IN ON AND IDENTIFY BAD ACTORS IN REAL TIME.**



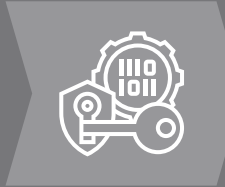

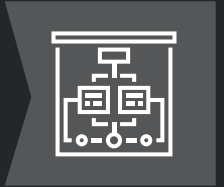


# While adversaries have quickly evolved, many tools have not.

## The need – and solutions – for Detection and Response have extended beyond the endpoint; but “buyer beware”.

A fully-managed security solution with a robust and complete security stack can bridge the gap between your organization’s time and resource demands, providing the required expertise to stand up a multilayered security program that detects threat actors wherever they emerge, in real time. Yet without industry-standard language in place, many providers use terminology that suggests their solutions are far more robust than they are in practice.

For example, many solution providers utilize the term “XDR” (eXtended Detection & Response) to describe services that in reality provide only EDR (endpoint detection and response); the same holds true for MDR offerings on the market – it falls upon the buyer to have a clear understanding of what the provider does, and if the service maps to their needs. With such a dynamic market, it is helpful to understand how security services have grown and changed, and how the scope of the solution provided differs between tiers of service.

<b>SIEM</b>  A Security Incident & Event Management tool alone will generate alerts, but won't tell you what you need to do to counter threats, or which alerts need prioritization.  	<b>Managed SIEM</b>  Outsourced SIEM Management provides remote management of the SIEM you own. These providers often don't have the expertise in any one SIEM as their focus is too wide. This is only slightly better than SIEM alone.  	<b>EDR</b>  Endpoint Detection & Response helps security teams gain visibility into malicious activity on an endpoint, and remotely contain and mitigate attacks.  	<b>MDR</b>  Managed Detection & Response providers deliver 24/7 threat detection, incident validation, and can offer lightweight remote response services.  	<b>DataEndure XDR</b>  eXtended Detection & Response is the next level of threat detection and response that correlates and analyzes previously disparate SIEM, EDR and NTA data, allowing timely triangulation of threats.  
---	---	--	--	--





## DataEndure delivers the gold standard for cybersecurity

### Enlisting a team with decades of cybersecurity expertise helps you take back your time.

Put time back on your side by strengthening and accelerating your ability to respond to an ever-changing threat landscape. DataEndure works by your side and on your behalf and can offer you a fully realized security program, for a fraction of the time and expense of going it alone.

DataEndure utilizes a **Modern Defense-in-Depth** approach: a security construct emphasizing a multi-layered approach to digital defense that supports and secures today's distributed workforce and ever expanding edge. It's considered the gold standard for cybersecurity, and with good reason: with so many tools and techniques integrated into a single program, multiple lines of defense can be deployed to detect and respond to even the most sophisticated bad actors, inside or outside of your organization, before they can do any damage.

By enlisting experts, **you gain your time back to focus** on your core business. A telemetry-based approach to prioritizing threat responses can be realized faster than developing an in-house

solution, giving you **increased time to value**.

Finally, by enlisting managed cybersecurity experts, you take away one of the most valuable tools a cybercriminal has to hurt you, the time it takes to discover and remediate an attack in progress (**dwell time**). The end result: a robust managed security solution that helps you **turn time to your advantage**.

#### The DataEndure X-Factor

DataEndure's XDR-as-a-Service brings a practical and proactive approach to threat detection and response by integrating, correlating, and analyzing data across many security tools. With users and devices expanding outside the traditional edge – and farther from IT visibility and support, XDR allows for the timely identification of threats in your environment by triangulating multiple points of telemetry from many sources to find the bad actors, not just the indication of a compromise or risk.

# Our Approach

Our goal is to ensure you have the best possible security posture available in the industry. Our approach combines many integrated technologies and methodologies which provide the critical telemetry to help accelerate threat detection and improve investigation and response times.



**1. Advanced Phishing Protection is the first line of defense.** It's a dangerous strategy to rely on security awareness training for your users as a solid first line of defense. With cyber-adversaries who are crafty and agile, you also have to protect users from themselves by preventing the phishing, impersonation and spoofing attempts from getting to them at all.

**2. DNS Defense is your second line of defense.** It's not enough to prevent DDOS attacks, you must have threat intelligence to know where bad sites are and block them in case your first line of defense doesn't work.

**3. Endpoint Security is the third line of defense.** Your endpoint security solution should not just be focused on file-based threats - the days of signatures and definitions are long gone. To prevent malicious execution, you must be able to monitor tactics, techniques and procedures executables are using, stop them in their tracks and roll back the damages.

**4. Security Operations & Orchestration is the critical final layer of defense.** Your SOC needs to include telemetry from all aspects of your environment, not just the endpoints and not just the network. While a SIEM is critical for full security log aggregation, correlation and management, it is not enough on its own. For full visibility into the health of your security posture, it also must include User and Event Behavioral Analytics, Network Traffic Analysis, Host Intrusion Detection Service, Network Intrusion Detection Service, File Integrity Monitoring, Advanced and active threat intelligence, Continuous Vulnerability Assessment, Security Orchestration & Automated Response and running continuous simulated attacks (purple team activities) leveraging the MITRE ATT&CK Matrix TTPs. All of these sources of telemetry must be aggregated and correlated to enable rapid identification of indicators of compromise so that your security team can begin investigation of threats.

## Modern Layered Defense-in-Depth



# The DataEndure difference

Don't take our word for it. Here's what just a few of our customers have to say about why our cybersecurity solutions work for them.



## SECOND HARVEST FOOD BANK

"As one of the largest food banks in the nation, we distribute food through a network of 309 nonprofit partners at 985 sites. Over the years, DataEndure has served as our technology advocate, helping Second Harvest establish and maintain the digital resilience we need at a cost we can afford, from data protection and disaster recovery to security visibility. We have peace of mind knowing their expert tools and talent are actively monitoring our network 24x7."

(Elizabeth Whamond, Director of Information Technology)



## THERMA

"Our priority is to deliver innovative mechanical solutions to our clients, on time and on budget. If our data is in any way compromised, our mission is at risk. DataEndure strengthens our security posture, serving as a sentry, with expert tools and talent at work on our behalf, protecting us from known and unknown threats that could render us inoperable."

(Mike Fisher, Chief Operating Officer)



## NORDIC NATURALS

"Our company credo is to do whatever it takes to offer high-quality nutrients that bring health benefits to as many people as possible. In a data-driven world, ensuring the safety and security of our network and our digital assets is a critical part of that mission. DataEndure provides us with the advanced threat detection and response capabilities we require, at a fraction of the cost of maintaining an internal security team."

(Joar Opheim, Founder & CEO)





# Get started today.

## **Help your security keep up with the speed of business.**

DataEndure addresses your security and compliance challenges in a cost- and time-effective manner, so that you can focus on growing your company without spending precious time thwarting potential threats. Serving as an invested security advocate with the latest technology and deep expertise, DataEndure can help your organization become less reactive and more resilient in an ever-evolving threat landscape, without draining IT resources and budget. Help your security keep up with the speed of business with DataEndure as your trusted partner.

## **Get started today with a complimentary Security Health Check**

Our complimentary Security Health Check helps ensure your security tools and controls are working and can detect threats and respond to incidents no matter where you are operating. And our 30-day “Go Live” Guarantee gives you the time advantage, ensuring your service is up and running quickly and your security posture fortified.

## **About DataEndure**

DataEndure is in the business of successful outcomes, helping customers achieve and maintain digital resilience for more than 35 years. We have grown up with the industry, which gives us unique expertise and perspective that we use to help your business bypass traditional data challenges, and establish what really will or won't work for you. We bring together the gold standard of technological insight and capabilities with a comprehensive solutions portfolio and innovative managed security services that help our clients better manage their IT risks, respond well when assets are threatened, and protect and access critical information wherever it resides. Our managed security services support and secure customers across 23 countries and 4 continents. What can we do for you?

Learn more at [www.dataendure.com](http://www.dataendure.com).

