The Complete Checklist for

Choosing an Extended Detection and Response (XDR) Provider

WHITEPAPER

PREPARED BY
BITLYFT CYBERSECURITY

INTRODUCTION

If you're seeking Extended Detection and Response (XDR) services, you understand the critical importance of proactive protection and that your organization needs a complete integrated solution to protect against modern cybersecurity threats.

A combination of recent events has resulted in an explosive increase in cyberattacks that have drastically affected internal security and IT teams. Extended Detection and Response addresses many of the issues facing modern enterprises including short-staffed cybersecurity teams, discreet attacks that exploit human error, increased cybercrime activity, burnout, alert fatigue, etc.

Yet, XDR is a complex set of services, and every vendor doesn't supply the same offerings. When searching for a comprehensive solution for your unique industry, it's important to understand the services you need and how to choose an XDR vendor that will adequately meet those needs.

If you compare XDR vendors, you'll assess the tools and human professionalism they offer with their services, as well as their communication style and willingness to share valuable information about their security methods.

When there is so much ground to cover, it can be easy to enter a business relationship without getting a full understanding of the services you'll be provided. In the world of cybersecurity, a misunderstanding could leave critical vulnerabilities hackers can exploit.

THIS CHECKLIST IS DESIGNED TO PROVIDE ORGANIZATIONS WITH THE RESOURCES TO COMPARE XDR VENDORS AND FIND A SOLUTION FOR COMPREHENSIVE SECURITY THAT ADDRESSES MODERN CYBER THREATS AND ELIMINATES GAPS IN SECURITY.

UNDERSTANDING THE VALUE OF XDR FOR YOUR UNIQUE ORGANIZATION

XDR offers customized security plans that can act as an extension of your existing internal team or provide a complete security solution for companies without an internal team. To get the full benefits of XDR services, it's important to take stock of your cybersecurity needs and determine what you hope to address with XDR. To be defined as XDR, services must feature some specific offerings. However, there are vital differences between the styles and levels of services that fall under the XDR umbrella.

WHAT XDR DOES

In the past, traditional security services depended on a technology-driven model to prevent hackers from breaching an organization with firewalls and antivirus solutions for each device. Today's modern enterprises need a solution that provides a strong perimeter defense as well as services that detect and respond to threats in real-time.

XDR offers complete end-to-end security that grants full visibility into your entire network and provides data collection, detection, response, and remediation for modern threats. With the combination of a preconfigured cybersecurity stack and professional security services from an off-site SOC, XDR provides these critical services:

- **Log Collection With Prioritized Alerts:** SIEM and EDR help organizations sift through massive volumes of alerts and determine which should be addressed first with contextual information that distinguishes false alerts from real threats.
- **Threat Hunting:** Human threat hunters use creative thinking and experience to identify evasive and new threats that automated services can't detect.
- **Managed Investigation Services:** With security alerts that provide added context and analysis of log activity, data analysts can determine the scope and details of an attack. These details can be used to address vulnerabilities and plan an effective response.
- **Guided Response:** Next steps to contain and remediate a threat is provided through automated response or details provided by your off-site SOC. Instructions range from the isolation of an affected device to step-by-step instructions to eliminate a threat or recover from an attack.
- **Remediation:** Managed remediation offers professional services to return your network to a known good state.

UNDERSTANDING THE VALUE OF XDR FOR YOUR UNIQUE ORGANIZATION (CONT)

WHAT XDR DOESN'T DO

Unfortunately, XDR doesn't guarantee your network will never suffer from a successful attack.

EXTENDED DETECTION AND RESPONSE MUST INCLUDE THESE COMPONENTS

 A remotely delivered Security Operations Center	 Rapid Detection	 Analysis
 Investigation	 Active threat response through threat mitigation and containment	 A turnkey experience using a predefined security stack to collect relevant logs, data, and contextual information

However, there are no requirements to outline how XDR vendors provide these services or the level of involvement an off-site SOC will supply. Without specific details, the services supplied by XDR vendors can vary quite drastically. This means there is no promise that XDR will offer:

The most up-to-date tools and technology	A specific level of interaction with your off-site SOC
A high level of customizability	An incident response that includes human involvement

The level of services you receive depends directly on your XDR vendor. That's why it's critical for you to ask difficult questions when comparing providers to ensure you invest in comprehensive protection that will address your cybersecurity gaps.

YOUR CHECKLIST FOR CHOOSING AN XDR PROVIDER

Making decisions about the security requirements of your organization demands a structured plan and strict attention to detail. Every business has different needs, and your vendor should have tools and methods in place to offer flexibility. By defining what you expect before comparing providers, you'll have the information to accurately compare the services provided by each vendor you're considering.

No matter how many questions you ask, a high-quality security provider should be happy to spend as long as it takes to provide you with a firm understanding of their services. Good communication is critical to your security solution. The way XDR vendors handle your interview is your first glimpse into their communication style.

DEFINE YOUR XDR REQUIREMENTS

Before interviewing vendors, it's important to know what you hope to accomplish by investing in XDR services. Determine whether you want services that act as support for your existing tools and expertise or a complete protection solution. Define the assets you want to protect, and what potential issues you hope to resolve. Consider compliance requirements for your industry and if any new certifications must be obtained in the near future. Take time to identify specific scenarios to discuss with potential vendors.

Suggested Questions

- [ ] Can you provide customized services that act as an extension of our existing team and tools?
- [ ] Do you offer complete security plans?
- [ ] How do you address protection for cloud-based apps, endpoints, and remote employees?
- [ ] Do you provide industry-specific solutions?
- [ ] How quickly can we expect to experience the full value of your services?

YOUR CHECKLIST FOR CHOOSING AN XDR PROVIDER

UNDERSTAND THE TECHNOLOGY

XDR services include the assistance of off-site cybersecurity experts as well as a pre-defined technology stack designed to protect your network. The tools provided for network security will either be created by your vendor or a carefully curated combination of existing tools and systems. As networks become increasingly complex, it's important to understand the technology that will be used to protect every device and endpoint against threats.

Suggested Questions

- [ ] Is your technology supplied by third-party providers? If so, what experience and success have they achieved?
- [ ] What data sources are used for log collection?
- [ ] Does detection utilize threat chain models?
- [ ] How does your system prioritize alerts?
- [ ] Do threat reports include contextual information?
- [ ] Do you respond to various types of attacks?
- [ ] Are automated response actions included?
- [ ] Is UEBA automatically included in XDR services?
- [ ] Is SOAR automation capabilities part of your package? If not, can they be added to expedite the remediation process?

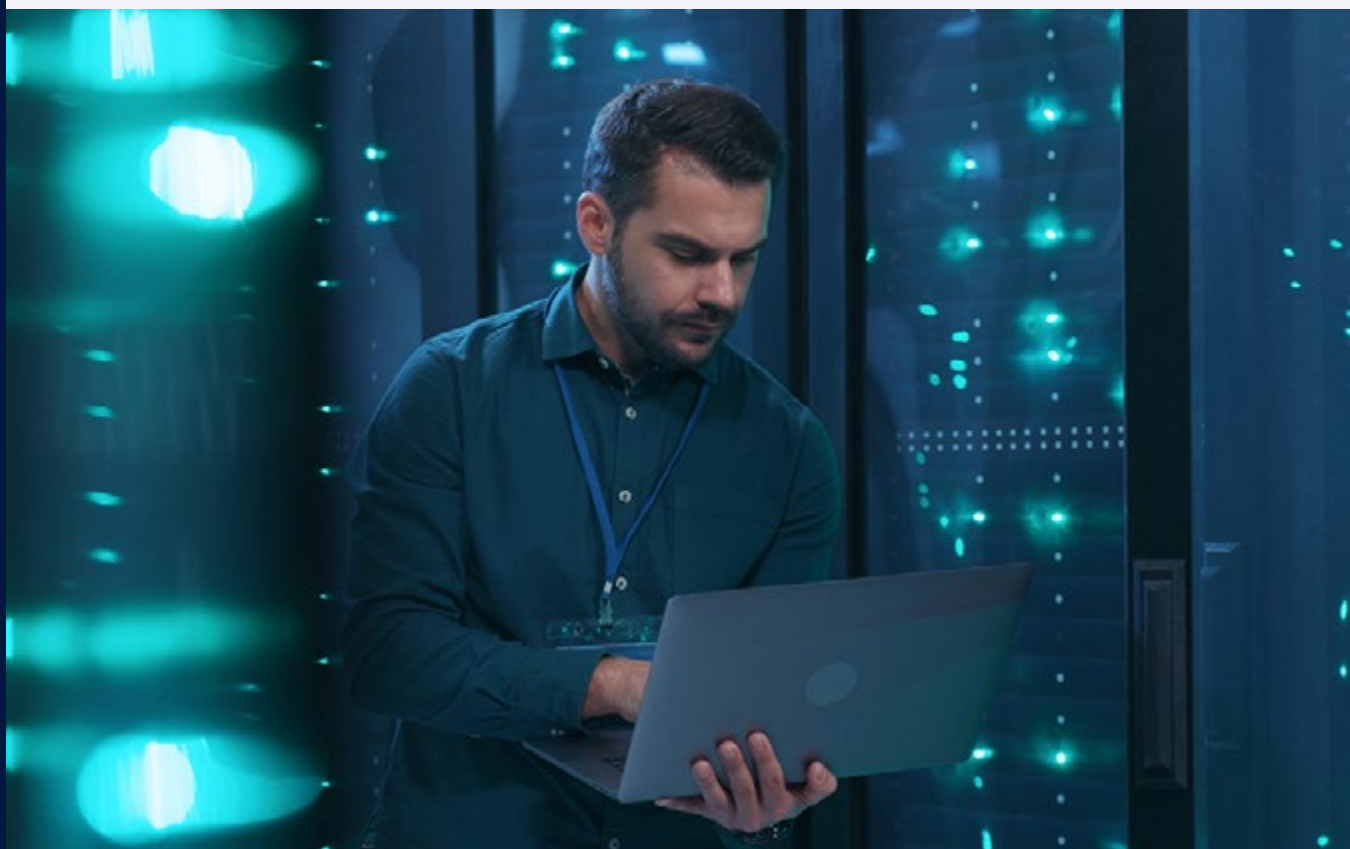
CHECKLIST FOR CHOOSING AN XDR PROVIDER

EVALUATE YOUR PERSONNEL NEEDS

The workload of cybersecurity professionals is growing drastically, yet the headcount among security teams is remaining the same. One of the most valuable components of XDR is the humanitarian assistance provided by the vendor's off-site SOC. Even if you have an internal security team, your goal may be to use the off-site team supplied by your vendor for services after hours. Whether you're seeking a full security solution or professionals that act as an extension to your team, it's important to understand exactly what the human element of an XDR solution will provide.

Suggested Questions

- [ ] How many people will be assigned to my organization?
- [ ] Will analysts be providing services 24/7?
- [ ] Are professionals optimized with software solutions?
- [ ] Will your team continuously assess the organization's performance in achieving security objectives?
- [ ] Does your team investigate all threat types?



CHECKLIST FOR CHOOSING AN XDR PROVIDER

IDENTIFY INDUSTRY REQUIREMENTS

While the needs of a small retailer aren't exactly the same as a large financial corporation, both facilities must follow certain compliance requirements. A security vendor that has worked with companies in your industry is more likely to know and understand the compliance laws you face and specific security objectives for the industry.

Suggested Questions

- [ ] Do you have experience in our industry?
- [ ] How do you help companies prepare for specific compliance audits and other requirements?
- [ ] Can you identify the compliance laws in my industry?
- [ ] What knowledge do you have of industry-specific threats?
- [ ] Do you take steps to help your clients prepare for new certification requirements and updated regulations?

DETERMINE PROFESSIONALISM

Your organization's security is an important factor in how you do business and should be provided by a certified vendor with a proven track record of success. It's important that you perform due diligence to get a firm understanding of the professionalism of a vendor before signing a contract. A good XDR provider should be able to share certifications as well as information about the qualifications of security analysts.

Suggested Questions

- [ ] Can I see your SOC2 certification and other third-party security audit results?
- [ ] What are the qualifications of your security analysts?
- [ ] Can you arrange for a meeting with security analysts to discuss my security needs?
- [ ] What's the average tenure and attrition rate of the team?

CHECKLIST FOR CHOOSING AN XDR PROVIDER

EXPLORE YOUR COMMUNICATION PREFERENCES

Assistance and communication from an off-site SOC is an essential feature of all XDR solutions. However, an XDR vendor can handle communication any way they want. As you might expect, the frequency, mode, type, and value of communication can vary widely from one vendor to the next. Assess your needs and determine what you expect from your relationship with an XDR vendor.

Do you expect routine communication that assesses your ongoing cybersecurity posture as well as vital communication during an incident? Determine exactly what level of correspondence you'll receive before choosing the XDR provider right for your organization.and specific security objectives for the industry.

Suggested Questions

- [ ] How often will you communicate with my team?
- [ ] What types of communication do you provide?
- [ ] What type of experience can I expect when I need to contact the team?
- [ ] Do you provide proactive communication about ongoing cybersecurity posture as well as detailed alert and response communications?
- [ ] What are your service level agreements?
- [ ] How quickly can I expect a response to questions?
- [ ] How will we work together during a security incident?

CHECKLIST FOR CHOOSING AN XDR PROVIDER

CONSIDER YOUR FUTURE NEEDS

Businesses must constantly evolve to meet the needs of consumers. This means your network and the security protecting it must be able to adapt quickly to change. Most organizations will require an XDR solution that can scale with growth and handle technology changes like the adoption of new applications and cloud migration for data storage and sharing.

Suggested Questions

- [ ] How do you meet my company's growth requirements?
- [ ] Are your applications cloud-based?
- [ ] Do you offer ongoing employee training as companies expand the workforce?
- [ ] Will there be extensive start-up costs if new devices or network requirements arise?
- [ ] Is there data allotment or retention limitations?

CHECKLIST FOR CHOOSING AN XDR PROVIDER

IDENTIFY YOUR RESPONSIBILITIES VS THOSE OF YOUR VENDOR

Whether your organization has an internal team or is seeking a complete cybersecurity solution, you need services that go beyond automated alerts. Since XDR providers offer different tools and methods when it comes to alerts, investigation, and response, it's important to know what your vendor expects you to accomplish without assistance.

For example, a notification about suspicious behavior without context alongside a recommendation that simply suggests you investigate the threat provides nothing more than an additional headache for your internal team. To learn exactly what to expect from your vendor, ask them questions about what they expect from you.

Suggested Questions

- [ ] Does your team provide 24/7 human monitoring of log collection?
- [ ] What types of alerts can we expect to see?
- [ ] Do you prioritize alerts related to urgency and relevance?
- [ ] Do you implement technology that works alongside our existing security efforts?
- [ ] How do your detection and response strategies differ for on-prem technology vs cloud infrastructure?
- [ ] Can you provide a step-by-step example of what we can expect from you during an incident?
- [ ] Do you provide complete visibility into the services you implement for my network?
- [ ] Can I see examples of actual reports?
- [ ] What level of response do you provide for threats in real-time?
- [ ] Do your incident response capabilities surpass automated response when necessary?
- [ ] What do you expect from our organization/internal team?

ASSESS YOUR INFRASTRUCTURE

One of the major appeals of managed services is that organizations don't have to place a large upfront investment in infrastructure and tools. However, it's also important that a vendor's software will work with your existing systems and tools. Take stock of the devices and infrastructure that will interact with security software. Note any cloud-based apps your organization depends on for convenient daily workflows.

Suggested Questions

- [ ] What are your software requirements?
- [ ] Will my organization need to make immediate infrastructure changes to work with you?
- [ ] Will changes be required for secure scalability?
- [ ] Do security solutions integrate with popular cloud platforms like Office 365?

CHECKLIST FOR CHOOSING AN XDR PROVIDER

SEEK PROACTIVE SERVICES

Responsive services aren't enough to be effective against modern attacks. If you depend on a security provider that reacts when an attack happens, you'll face critical damage before the attack is stopped. Proactive protection uses a variety of tools and human threat hunting capabilities to recognize suspicious behavior and stop an attack before the attacker reaches their objective.

XDR requirements include skilled threat analysis, interpretation, and actionable services. These services provide the building blocks for threat hunting but don't specifically require the offering. To understand exactly what proactive services you can expect, it's important to ask direct questions.

Suggested Questions

- [ ] Do you offer proactive threat hunting services?
- [ ] How often do you check our organizational environment for potential threats?
- [ ] What level of visibility do you provide our team with dashboards and other visual aids?
- [ ] What data sources do you use for crowd-sourced threat intelligence?
- [ ] Do you investigate all types of threats?

YOUR CHECKLIST FOR CHOOSING AN XDR PROVIDER

IDENTIFY THE CONTRACT TERMS

Different XDR vendors utilize various methods to onboard clients. Some might offer an introductory rate, a free trial, or limited services at a lower price. Others might provide all of the services you're seeking but with hidden costs or retainer fees. While your contract should provide an explanation of the services you'll receive for a specific price, it might fail to offer the detail you need to grasp the breadth of the security features offered. Make sure you have adequate time to read the complete terms of the contract and ask questions until you feel comfortable with your level of understanding.

Suggested Questions

- [ ] How long are the terms of the contract applicable?
- [ ] Am I getting an introductory rate? If so, when will it change, and by how much?
- [ ] What exactly is being provided for this price?
- [ ] What happens when our contract is up for renewal?
- [ ] Will you raise rates without notification?
- [ ] What does the base contract include, and are there other services I have to pay extra for?
- [ ] Do any services require a retainer?

YOUR CHECKLIST FOR CHOOSING AN XDR PROVIDER

ADDRESS THE VENDOR'S ABILITY TO MEET YOUR UNIQUE NEEDS

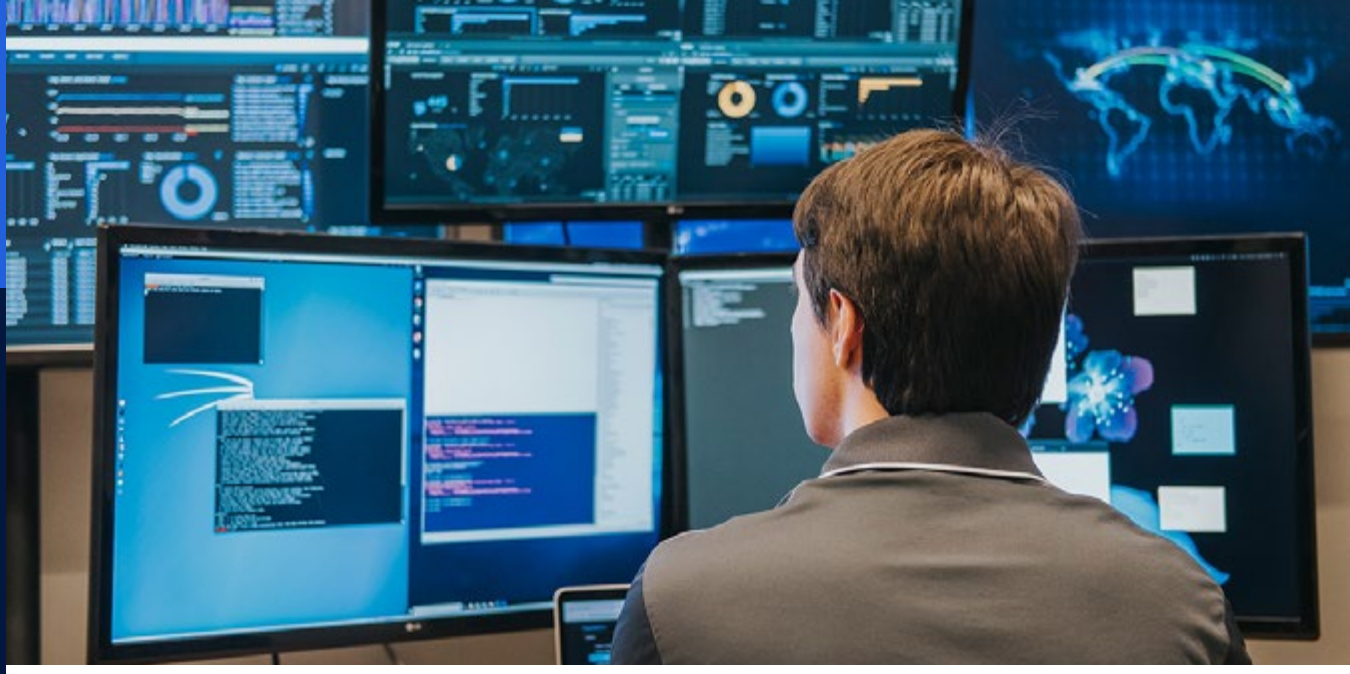
XDR services are designed to be customizable in a way that suits the needs of organizations of all sizes across multiple industries. The level of customizability provided by a vendor is pivotal to successfully working with your internal team and meeting specific industry standards.

XDR is designed to be an extension of your existing security efforts with tools and services provided by professionals. For organizations with no internal security team, an XDR vendor should be able to offer a complete security plan. Some vendors offer little or no customization, providing every client with the same generic solution. If a cookie-cutter fix isn't likely to address your security concerns, it's important to ask about the level of customizability you can receive.

Suggested Questions

- [ ] How do your services work with our existing security efforts?
- [ ] Do you provide custom options for complete security plans?
- [ ] Will you be able to make changes if our team grows or shrinks?
- [ ] What are you doing to customize our security plan to meet our unique organizational needs?
- [ ] Do you go beyond out-of-the-box cybersecurity offerings to close potential security gaps?
- [ ] Can you provide an example of ways you've adapted your service to your customers' requirements?

CHECKLIST FOR CHOOSING AN XDR PROVIDER



DETERMINE THE ADDED VALUE PROVIDED BY THE XDR PROVIDER

When you pay for managed services of any type, you should be able to recognize the value that goes above and beyond what you could achieve on your own. It should be redundant to ask a security provider if what they bring to the table will actually improve your level of cybersecurity. Yet, it's possible the services offered by some providers won't improve your situation. To determine whether the services provided will address your cybersecurity concerns, it's essential to ask for examples of what they add.

Suggested Questions

- [ ] Will you provide visibility and protection beyond what we already have?
- [ ] How do your services address our goals and concerns?
- [ ] Will your services improve organizational cybersecurity posture?
- [ ] Can we accomplish what you offer at a lower price?
- [ ] What kind of reporting do you provide to describe the effectiveness of your services?
- [ ] What measurements do you use to prove your services are working?

MAKING THE RIGHT CHOICE FOR YOUR CYBERSECURITY NEEDS

Entering the world of managed cybersecurity can be confusing. Our goal is to demystify the process and help organizations find the security they need to protect against modern threats and relieve the stresses placed on internal teams. BitLyft Air goes beyond traditional XDR services to provide our customers with expert-level protection at a fraction of the price of increasing your internal team.

BENEFITS OF XDR WITH BITLYFT AIR

Direct Access

You get direct access to the dedicated cybersecurity team that knows your environment, technology, and unique organizational goals.

Extension of Your Team

We stay in sync with you through iterative team calls, reporting, and check-ins. We're always a message or call away, and there to stop a threat at any time of day.

Lightning Fast Response

We protect your network with greater speed through software automation. Humans can be fast, but software is faster in remediating threats and handling manual tasks.

Never Complacent

We constantly keep up with the rapidly changing security and IT environment so your cybersecurity stays effective.

Scalability

We scale as you need us. We offer enterprise-grade cybersecurity within reach for any size organization in a recurring monthly subscription.

Expert Guides

We help you meet your organizational goals and reduce the burden of compliance by providing visibility and guidance.

XDR IN ACTION

Ready to see BitLyft XDR in action? Click on the button to the right to schedule a free, thirty-minute demo.

SCHEDULE A FREE DEMO

www.bitlyft.com

BitLyft
Cybersecurity

517-220-0990