SEAL THE DEAL

A TALK TRACK FOR SELLING XDR SECURITY TO YOUR BOSS

INTRODUCTION

You've done the research. Modern cyber threats are a danger to your organization that can't be controlled by your current efforts. You know you need the help. XDR is the best, and the most affordable, option to improve the cybersecurity of your business. Still, you haven't yet faced the real challenge. How do you convince your boss? This guide will outline the most common roadblocks and objections encountered by IT managers when trying to articulate the need for XDR to management within their company.

TOP 10 ROADBLOCKS WHEN GETTING APPROVAL FOR XDR

Roadblock #1

Leadership doesn't understand the technology.

Whether you're trying to describe an XDR solution to a company leader with minimal knowledge about cybersecurity as a whole or an IT professional with ample tech knowledge that is unfamiliar with XDR, this can be a major hurdle. To clearly define the benefits without patronizing your audience, it's a good idea to prepare more than one explanation of the technology supplied by a comprehensive Extended Detection and Response solution.

Responses For Someone Who is Not Tech-Savvy

Short Answer: While many cybersecurity tools are designed to address a single issue, Extended Detection and Response is a combination of modern tools and human response bundled into a single platform for fully integrated and complete protection.

Long Answer: While many cybersecurity tools are designed to address a single issue, Extended Detection and Response is a combination of modern tools and human response bundled into a single platform for fully integrated and complete protection. XDR is a group of services provided by a remote security center that provides log collection, detection of threats, an incident investigation by experienced professionals, and active response.

XDR works by providing an organization with an advanced set of tools and software customized to the needs of the company and ongoing support from a remote security operations center (SOC) fully staffed with experienced professionals. Since the tools are preconfigured and designed to work together, the company receives a solution that immediately improves your company's cybersecurity posture. Ongoing protection means outsourced cybersecurity offerings can grow with the company and change with organizational needs.

How it Works

- Automated tools are optimized to collect data that describes the traffic and activity within your network.
- Machine learning works to create a description of "normal" behavior within your organization.
- After creating a baseline of normal behavior, machine learning can identify abnormal behavior to generate threat alerts.
- These alerts are prioritized based on the type of threat, its potential impact, and other factors to eliminate the manual tasks associated with false alerts.
- XDR providers work with you to explain the scope of the incident and what actions need to be taken to contain it.
- A remote team of cybersecurity experts assigned by your provider investigates the incident and identifies the hacker's point of entry and the extent of access into the company's network.
- Following the investigation, cybersecurity professionals provide guidance on existing vulnerabilities and how to eliminate them to avoid a similar attack.

- Additional ongoing services provided by the XDR vendor's off-site SOC include threat hunting to identify sophisticated attacks that have evaded other security controls and training to your staff on how to effectively use the XDR service.
- The team provides assistance with remediation after an attack like restoring files that were deleted or corrupted and resetting passwords. Full remediation efforts will be provided to return your systems to a good known state.

Responses For Someone Who is Tech-Savvy, But Unfamiliar With XDR

Short Answer: Extended Detection and Response (XDR) is an end-to-end cybersecurity solution designed to protect against the sophisticated, discreet threats used by modern-day hackers.

Long Answer: Instead of investing in more tools with redundant activities and poor integration, XDR provides a fully integrated platform that addresses cloud migration, user credential theft concerns, limited IT/cybersecurity team headcount, and active attacks.

XDR provides:

- Immediate results with a preconfigured cybersecurity stack
- 24/7 monitoring and assistance provided by experienced cybersecurity professionals in a remote SOC
- Services that can complement existing cybersecurity efforts or provide a complete, customized cybersecurity solution
- Services that address log collection, threat detection, analysis, investigation, and response

The service works through the use of:

- Log management with SIEM
- Endpoint detection and response integrated with the SIEM
- AI for proactive threat protection and alert prioritization
- UEBA for recognition of suspicious behavior likely to indicate an insider threat or credential theft
- Integrated network monitoring for complete visibility through user-friendly dashboards visible to your internal team and your vendor's remote SOC
- Expert-level analysts that act as an extension of the internal team

How it Works

Step 1: eXtend

Our intelligent systems extend your security efforts by collecting, monitoring and correlating log data 24/7.

Step 2: Detect

Alerts and warnings are analyzed before remediation steps are taken.

Step 3: Respond

Our team works with you to resolve the issue. Then, solutions are developed to prevent future attacks.

Recommended Reading: XDR Security 101: Understand Its Power, Unleash Its Potential

Roadblock #2

Leadership Believes XDR is Too Expensive.

Many companies are recovering from pandemic losses and facing the effects of ongoing economic uncertainty. As a result, any budget request is more likely to seem expensive. XDR is actually a solution that can help your organization save money upfront with the elimination of immediate expenses and over time with scalable, effective protection that grows with your network and evolves with the growing threat landscape.

Short Answer: XDR is actually the most cost-effective solution and pays for itself.

Long Answer: Instead of a single tool, XDR provides a group of services and the ongoing assistance of a fully staffed remote security operations center. Whether the company needs a complete solution or services that expand cybersecurity efforts XDR provides a custom solution that provides the services you need without extras you don't.

XDR reduces costs related to internal hiring by eliminating recruiting and hiring costs by providing 24/7 assistance from a remote SOC. It allows the company to increase cybersecurity headcount and address the need for 24/7 monitoring and response without affecting the internal team. XDR allows you to outsource and automate redundant manual tasks that free up your IT and cybersecurity professionals to accomplish more with less time.

Since it works on a monthly subscription, XDR limits the immediate budget strains that most solutions require. For example, there are little to no upfront costs for XDR services. The service is scalable, so you don't have to invest in services your company hasn't grown into yet. Since the service includes the use of outsourced tools and software, costs related to outdated infrastructure and tools won't become a problem in the future. XDR is a powerful, cost-effective solution that grows with your organization.

XDR REDUCES OVERALL SECURITY COSTS BY ELIMINATING THE FOLLOWING EXPENSES

- ✓ Salaries for cybersecurity professionals
- ✓ Cost of cybersecurity tools
- ✓ Initial optimization and time to value
- ✓ Training expenses
- ✓ Compliance costs
- ✓ Remote work implementation costs
- ✓ The cost of a breach or attack
- ✓ The cost of burnout
- ✓ The cost of dwell time
- ✓ Maintaining 24/7 monitoring and response

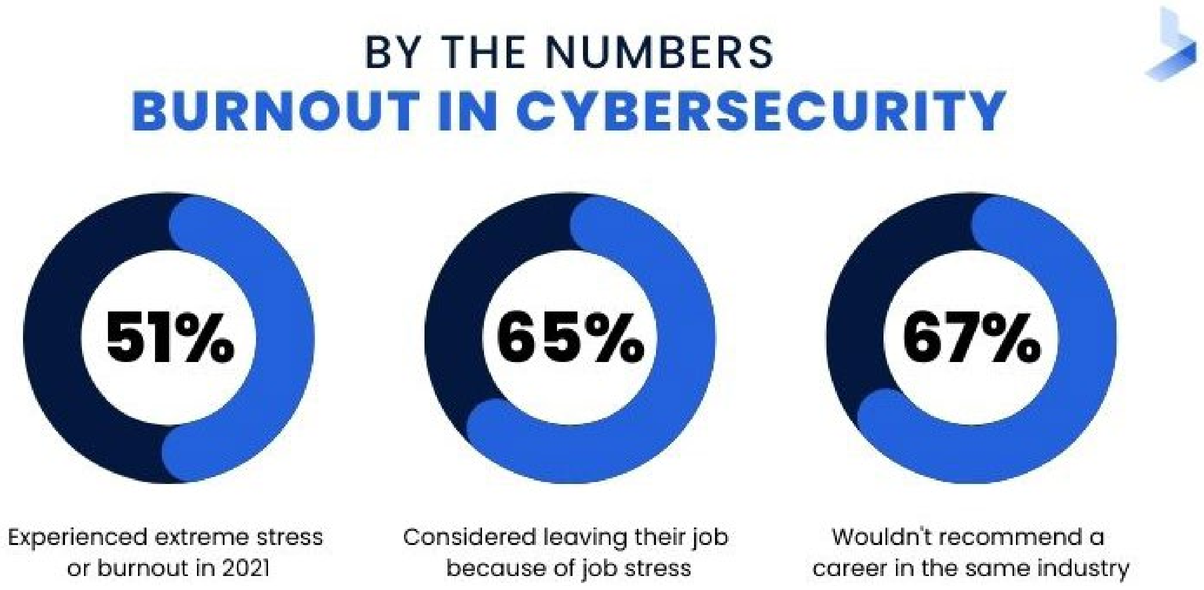
Recommended Reading: Budget Breakdown: 10 Ways XDR Actually Saves Businesses Money

Roadblock #3

Leadership Assumes You Can Do the Work Yourself.

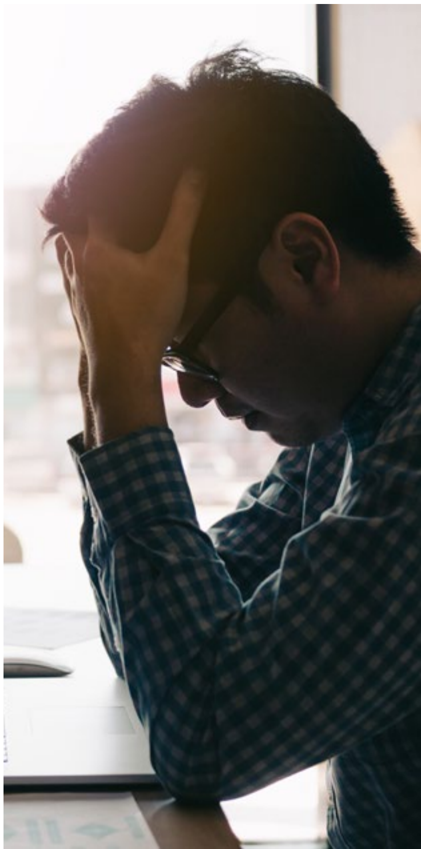
Burnout is a critical problem in the cybersecurity industry. Among professionals currently working in the industry, 51% experienced extreme stress or burnout in 2021, and 65% considered leaving their job because of job stress. Only 33% would recommend such a career to others and the same number would also likely discourage people from entering the industry.

Short Answer: Burnout is common among cybersecurity professionals, and you get an entire team of cybersecurity experts with BitLyft.



Long Answer: Cybersecurity professionals are working in an extremely stressful environment and often taking on more work and longer hours as a result of talent shortages. 65% of cybersecurity professionals have considered leaving their job because of job stress within the past year. As burnout leads to turnover, the remaining security professionals face even more work.

Burnout is a work-related syndrome that leads to negative feelings about one's job and reduced professional efficacy. In the cybersecurity industry, the risk of falling victim to an attack increases considerably when employees are facing stress and fatigue. XDR from Bitlyft provides you with an entire team of experienced cybersecurity experts to monitor your network, detect threats, and provide incident investigation and response as well as threat hunting to recognize impending attacks on the horizon.



Recommended Reading: Eliminate Cybersecurity Burnout with XDR

Roadblock #4

Leadership Believes XDR Won't Provide Enough Benefits/Value.

XDR provides numerous benefits to enhance your cybersecurity posture and benefits that affect your entire organization (like saving time and money).

Short Answer: XDR provides significant value through the services provided as well as the ROI that helps your organization save time and money.

Long Answer: As a turnkey service, XDR immediately improves your cybersecurity posture by addressing potential and existing threats. It addresses the critical functions of cybersecurity, including log collection, threat detection, analysis, investigation, and response. XDR provides end-to-end visibility and protection that covers endpoints like IoT devices and remote workers as well as internal infrastructure and cloud-based apps. These tools can also be optimized to take care of compliance regulations and reports.

The addition of a remote cybersecurity team reduces the need for your internal team to work long hours, and eliminates manual HR tasks associated with recruitment. Since XDR automates redundant tasks and false alerts through prioritization, more time is freed up for other projects.

Roadblock #5

Leadership Just Wants to Hire More Staff.

There are currently about 435,000 cybersecurity job openings in the US. The unemployment rate in the industry is 0%. Hiring more staff for your internal cybersecurity team might be the most difficult solution for any organization.

Short Answer: The talent gap in the cybersecurity industry is ongoing and continually increasing.

Long Answer: Hiring more staff is expensive. It requires time to train new employees on specific tools and procedures within the organization. Plus, the cost of cybersecurity personnel is increasing daily, and recruitment is becoming more competitive than ever. Hiring a single data analyst can be more expensive than your XDR services, and only provides assistance for 40 hours a week. Even worse, there's no guarantee that the new recruit will stay with the company after receiving critical training.

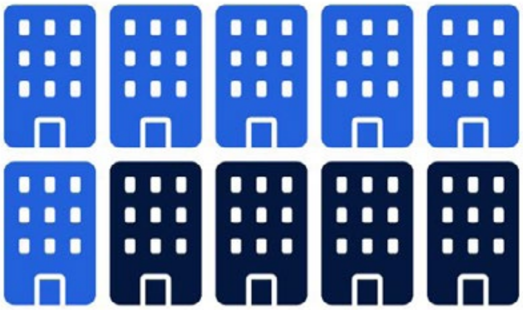
XDR provides tools and professional assistance from a remote team of professionals at a cost lower than that of a single annual salary. Services are scalable to adapt to network changes and company growth, so the organization won't have to adjust to major expense shifts in the future.

Roadblock #6

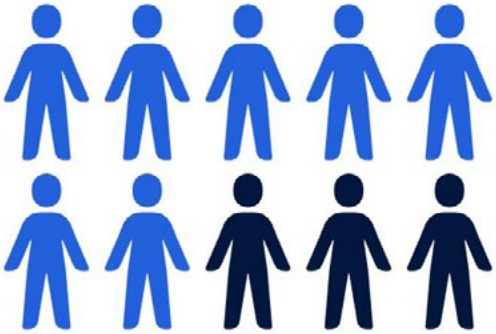
Leadership Doesn’t Think the Company is at Risk.

When it comes to cybersecurity, data doesn’t lie. Every company of every size in every industry is at risk.

Short Answer: 64% of organizations have suffered from some form of cyberattack and 66% of CISOs don’t know if their team is prepared to respond to an attack.



64% of organizations have suffered from some form of cyberattack.



66% of CISOs don’t know if their team is prepared to respond to an attack.

Long Answer: For organizations across all industries, it’s no longer a matter of if a cyberattack will occur, but when. A breach will cost more than the protection you need to protect your network and it could shut down your business.

All information has value. A single click when one network user responds to an email can result in a catastrophic ransomware attack. Perimeter defense is no longer enough to keep out advanced persistent threats.

The average time to discover after a hacker infiltrates a company network is more than 200 days. This means the company network could currently be in the midst of an active attack and not even know it.

THE AVERAGE TIME TO DISCOVER AFTER A HACKER INFILTRATES A COMPANY NETWORK IS MORE THAN 200 DAYS.

Recommended Reading: Recession Proof Your Business in Five Steps: Cybersecurity Edition

Roadblock #7

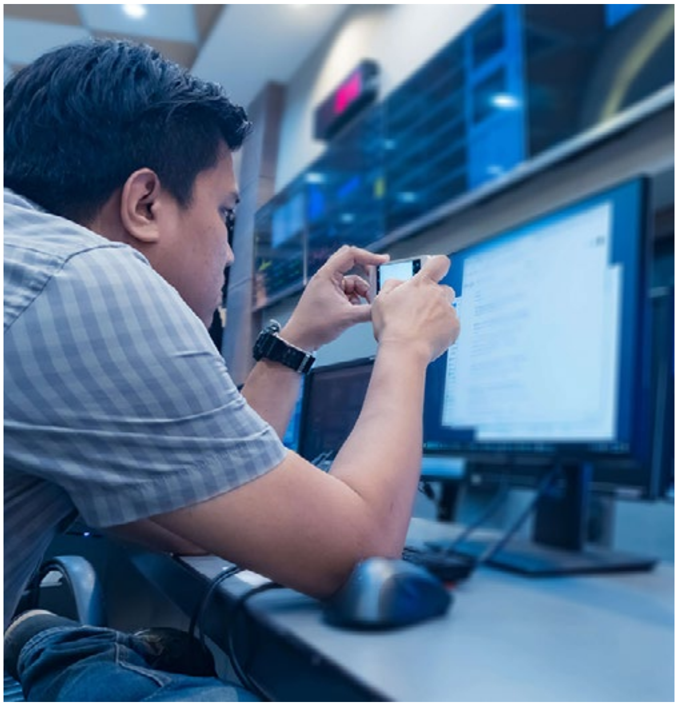
Leadership Doesn't Want to Learn a New System.

Learning a new system can cause a temporary disruption to internal performance and production, but it is usually resolved quickly. Furthermore, modern tools are typically more effective and eliminate ongoing issues caused by outdated tools and procedures.

Short Answer: Technology is advancing at a rapid pace and it's an absolute requirement to keep up.

Long Answer: Legacy systems simply don't have the capabilities required to respond to modern complex cyber threats. The response system an organization has in place has a direct effect on the immediate costs of a breach. When automation and security AI are fully deployed, organizations pay up to $3.81 million less to recover from an attack than those without it.

XDR is designed to offer immediate time to value and provides ongoing support from a remote team of professionals. Since the technology is preconfigured and customized to each organization, there is no waiting period for time to value.



Although network users might need a short period of time to adjust to new procedures, the integrated nature of XDR will likely eliminate redundant security requirements necessary with legacy systems.

Solutions provided by XDR will also eliminate manual tasks and reduce false alerts, providing more free time for the internal team. Instead of a clunky outdated system that requires more work for each user, the streamlined nature of a new system will require less work and effort from all network users almost immediately.

WHEN AUTOMATION AND SECURITY AI ARE FULLY DEPLOYED, ORGANIZATIONS PAY UP TO $3.81 MILLION LESS TO RECOVER FROM AN ATTACK THAN THOSE WITHOUT IT.

Recommended Watching: The Top 6 Cyber Security Tools You Need for 2022 and Beyond

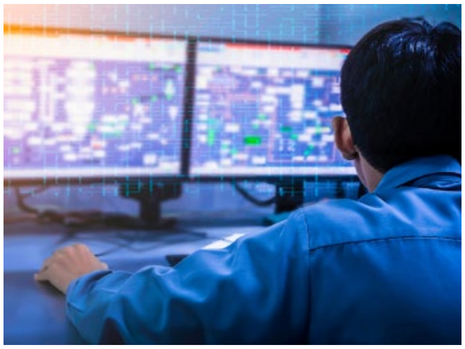
Roadblock #8

Leadership Believes That XDR Will Take Too Much of Your Time.

XDR requires less time from your organizational leaders, network users, and IT/security professionals instead of more.

Short Answer: Obtaining XDR for the company will actually free up time for all network users and take significant pressure off of IT and cybersecurity professionals.

Long Answer: XDR is designed to be a customizable solution that acts as an extension of existing cybersecurity efforts or provides a complete cybersecurity solution. With the use of automated tools and ongoing assistance from a remote team of experts, XDR will eliminate wasted time and improve overall network function.



How it Works: 7 Ways XDR Helps Organizations Save Time

1 An integrated tech stack eliminates the time spent overseeing a large group of tools that aren't designed to work together.

2 Modern tools and technologies that work together eliminate the need for network users to complete redundant security requirements when completing daily tasks.

3 Automated tools that utilize artificial intelligence and machine learning automate tasks that take hours to complete manually.

4 Tools can be optimized to include compliance requirements and the necessary reports for audits, eliminating the manual compliance tasks usually completed by internal cybersecurity professionals.

5 Threat prioritization eliminates redundant and false alerts by only sending relevant alerts with contextual information to the internal team.

6 XDR services include automated and human-centered response actions that reduce attacker dwell time within the network to significantly reduce or even eliminate downtime in the event of an attack.

7 The inclusion of a remote security operations center eliminates time spent on cybersecurity recruitment and retention methods.

Recommended Reading: 9 Signs It's Time to Implement XDR in Your Business

Roadblock #9

Leadership Doesn't Want to Outsource Business to a Company.

For a company that is accustomed to utilizing internal personnel only, outsourcing critical services can be a major hurdle that seems potentially unsafe. Navigate this conversation cautiously, and work to reassure company leaders that your choice is a valid one.

Short Answer: Outsourcing cybersecurity requirements doesn't mean you have to give up full control.

Long Answer: BitLyft is also 100% US based and you'll get to talk to real people. You can begin with a meeting to assess cybersecurity goals and concerns and learn what outsourced XDR services can provide. The XDR services offered are designed to be an extension of organizational cybersecurity, so internal teams can have as much or as little interaction as desired. Since the service is billed on a monthly basis, there is no major upfront investment that ties you to a specific tool or service.

Outsourcing can also create flexibility the organization can not achieve alone. Recent events have taught everyone that it's essential to always expect the unexpected. Yet, no company can afford to invest in protection for every potential scenario. Outsourced XDR offers scalability and the ability to adopt new tools or services as needed. This means the company can be more prepared for unexpected events without investing in services, tools, or products that might never produce the expected ROI.

Although outsourcing seems like investing in another company. It's actually an opportunity to invest more time and money into the organization.

Scalable solutions that can be customized allow security teams to control costs and save money. The cost of hiring internal cybersecurity professionals is growing daily. With the rapid pace of changing technology, infrastructure costs will likely present bulk expenses more frequently and limited scalability will require investments that might not be used.

Since outsourcing allows the company to rely on the tools and trained professionals of a different organization, the overall cost is reduced and the organization is subject to fewer responsibilities. When the time and money saved by outsourcing are used elsewhere within the organization, the company can recognize improved performance and growth.

Recommended Reading: Comparing The Most Popular XDR Solutions: An Overview

Roadblock #10

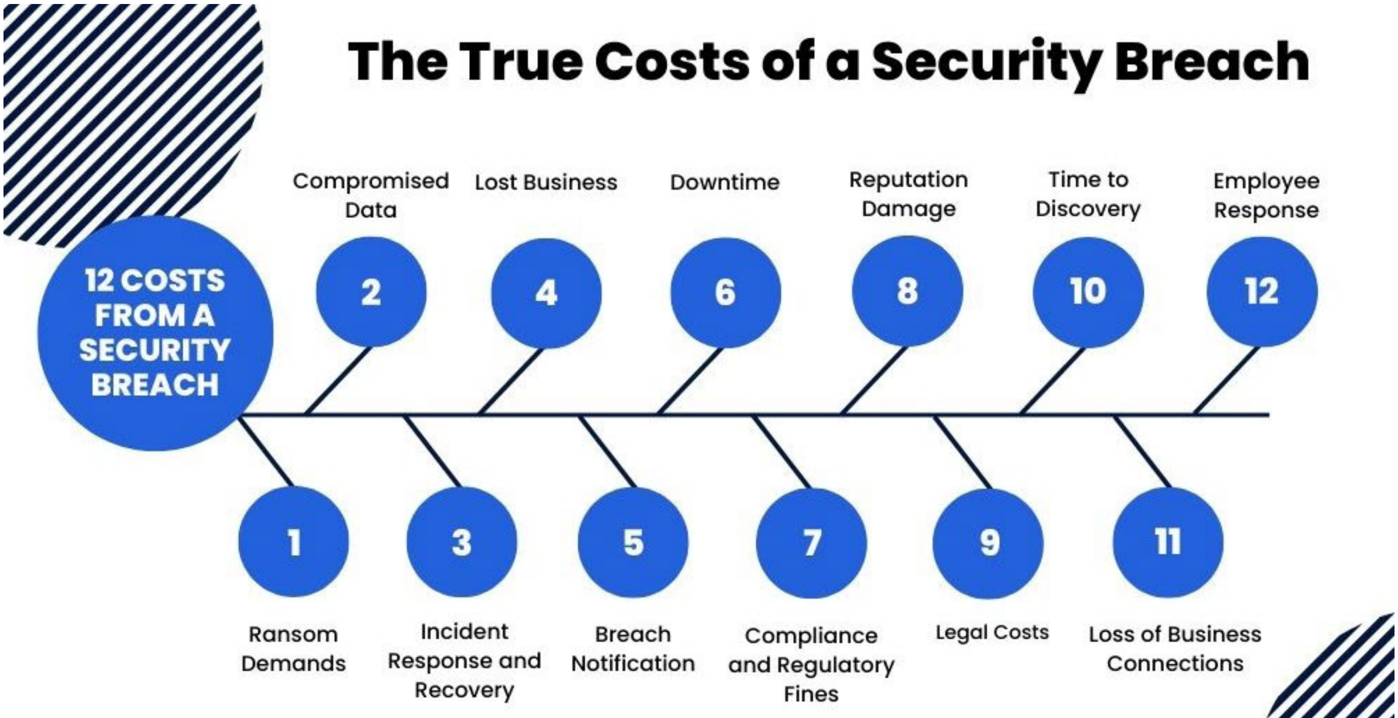
Leadership Believes Their Current Cybersecurity Stack is Enough.

Emerging trends mean the cybersecurity practices you used yesterday probably won't work today. Current technology is aging immediately upon hitting the shelves.

Short Answer: Hackers aren't satisfied with current solutions to exploit company networks.

Long Answer: Ransomware requests aren't staying the same. The cyberattack landscape is constantly growing and changing. The network of any successful business also must continually grow and change to meet the demands of modern consumers. Cyberattacks and related costs are increasing significantly each year. Today's stats won't even keep up with the stats that come out six or even three months from now.

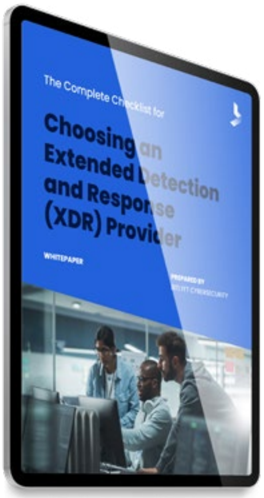
The technology used to generate company-wide advances like remote work and the convenience of IoT devices increases the number of ways attackers can access the organizational network. Attempting to keep up with the advancing threat landscape with new tools and increased cybersecurity headcount will result in substantially higher costs with lower ROI. It's impossible to keep up with today's threats using yesterday's tools. Legacy systems and software offer no manufacturer oversight or updates to address new vulnerabilities as they're discovered by hackers. Essentially, relying on any current solution is like waiting to become a victim of a cyberattack.


The True Costs of a Security Breach
12 COSTS FROM A SECURITY BREACH
Compromised Data
2
Lost Business
4
Downtime
6
Reputation Damage
8
Time to Discovery
10
Employee Response
12
1
Ransom Demands
3
Incident Response and Recovery
5
Breach Notification
7
Compliance and Regulatory Fines
9
Legal Costs
11
Loss of Business Connections

Recommended Reading: The True Costs of a Security Breach

LEARN TO CONVEY THE TOTAL VALUE OF XDR SERVICES TO YOUR BOSS OR MANAGEMENT TEAM

When it comes to modern cybersecurity, XDR is in a class of its own. Although you know the value of cybersecurity and the dangers of a successful cyberattack, it can be difficult to convince others of the immediate threat. At Bitlyft, we know that dealing with budget proposals and company requirements can be the only major hurdle to getting your organization the assistance required to achieve complete cybersecurity. That's why we provide as much information as possible to describe available services and the benefits they can provide.


The Complete Checklist for
Choosing an Extended Detection and Response (XDR) Provider
WHITEPAPER
PREPARED BY
BITLYFT CYBERSECURITY

NEXT STEPS

Once you convince your boss (we know you will) be sure to download the Complete Checklist for Choosing an Extended Detection and Response (XDR) Provider. This handy guide contains nearly 80 questions that will help you prepare for interviews with vendors.

GET THE FREE CHECKLIST

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

BitLyft

Cybersecurity