BitLyft
Cybersecurity

WHITEPAPER

NEXT GEN XDR

Understand its power,
Unleash its potential

www.bitlyft.com

Table of Contents

Recommended Reading:

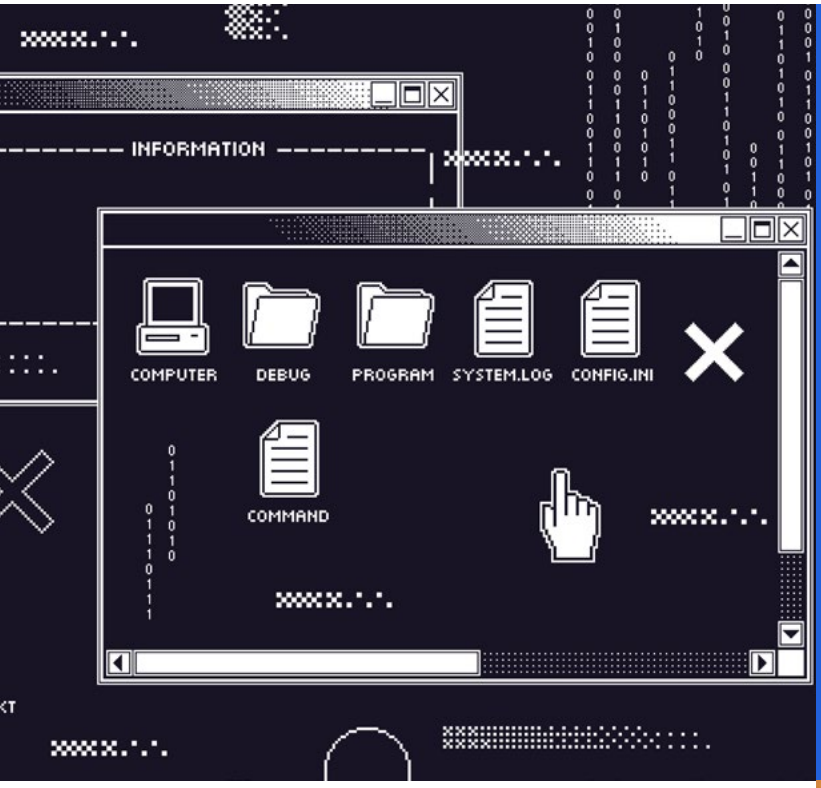
Look for the icon throughout the document for hand-selected recommended reading.

INTRODUCTION

You know your business is at risk. You've seen the headlines, and you understand that cyber threats are a reality. But what can you do to protect yourself? One option is to invest in XDR security.

This comprehensive approach to cybersecurity provides powerful protection, detection, and response capabilities. All of which can keep your business safe from even the most sophisticated threats.

In this guide, we'll explore everything you need to know about XDR security. This will help you make an informed decision about whether it's right for your business.



A BRIEF HISTORY OF CYBERSECURITY

In the early days of computing, security was not a major concern. Computers were big, expensive machines that were used primarily by governments and large businesses. As such, there wasn't much incentive for criminals to target them.

But as computers became smaller and more affordable, they became targets for criminals. Early cybersecurity solutions were designed to protect against these new threats. But as the threats evolved, so too did the solutions.

Today, we face a wide variety of cyber threats, from viruses and malware to phishing attacks and ransomware. And while there are many different types of cybersecurity solutions on the market, not all of them are equally effective at protecting against these threats.

THE CURRENT STATE OF CYBERSECURITY

Businesses in all industries have been forced to adapt to a landslide of changes over the last few years. Some of the most common challenges currently faced by security teams include:

- Keeping Up With New Tech Developments
- Maintaining Compliance
- Preparing for the Post Pandemic Workplace
- Recruiting and Retaining Talent
- Managing Cybersecurity
- Preparing for Attacks
- Tool Sprawl
- Artificial Intelligence and Machine Learning
- Aging Systems and Software
- Decreasing Budgets and Increasing Workloads

Extended Detection and Response

Over the next five years, the XDR landscape is expected to grow by a whopping 20%. Businesses recognize the importance of better security to protect them from the significant fallout of data breaches and cyberattacks. That's where XDR security comes in.

XDR provides robust, top-notch security solutions to keep your data safe. With XDR you can rest assured that your data is well-protected from any potential threats. If you have no idea what XDR solutions can do for your business, read on to learn more.

What is XDR?

XDR is a security solution that integrates multiple security tools and technologies. This approach provides a more holistic view of your security posture and can help you more quickly identify and respond to threats.

The goal of XDR is to improve detection rates, shorten the mean time to detection (MTTD), and reduce false positives. By integrating EDR and SIEM, XDR can provide a more complete picture of your environment and help you detect threats that would otherwise go undetected.

Additionally, XDR can automate the investigation and response process, which can help save time and resources. Implementing an XDR solution can be a complex undertaking, but the benefits of this approach make it well worth the effort.

How Does XDR Work?

Most XDR solutions follow a three step process.

1.) Identify/Detect

XDR systems help to identify anomalous behavior that is indicative of a threat. They also provide insight into the security of an organization.

2.) Investigate

After identifying a threat, the XDR security system investigates and determines the course of action. It then investigates the nature of the threat and how to deal with it.

3.) Respond

Once the system identifies the source of the threat, it takes action to neutralize it. This involves blocking network traffic from the source, quarantining the affected files, or taking action to prevent its spread.

Three Steps of XDR

Next-Gen XDR

What is Next-Gen XDR?

Next-Gen XDR is a new approach to cybersecurity that combines the best features of several different technologies. This approach provides a more comprehensive view of your security posture and can help you more quickly identify and respond to threats.

Next-Gen XDR is an integrated platform that brings together data from multiple sources, including EDR, SIEM, and SOC. This platform uses artificial intelligence to correlate this data and provide insights into your security posture.

This approach can help you more quickly identify and respond to threats, as well as improve your overall security posture, and we will showcase the benefits of Next-Gen XDR in this article.a complex undertaking, but the benefits of this approach make it well worth the effort.

How Does Next-Gen XDR Work?

Next-Gen XDR solutions are designed to address the most common pain points that businesses face. They offer enhanced benefits such as:

Easy Deployment and Flexibility

Next-Gen XDR solutions are designed to be easy to deploy and manage—even for businesses with limited IT resources. Next-Gen XDR solutions are also highly scalable and can be customized to meet the unique needs of any business.

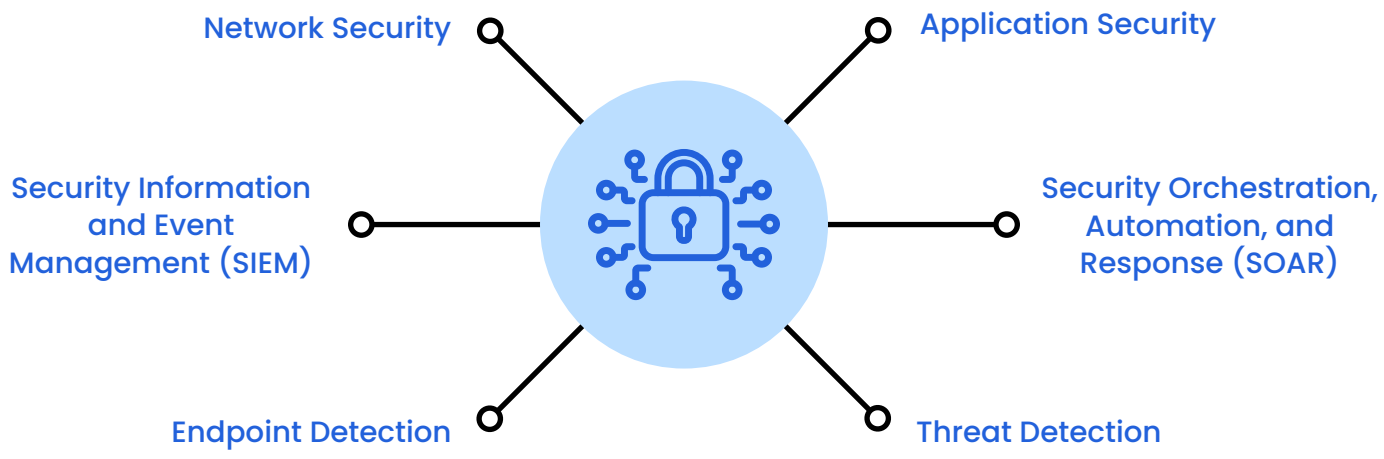
Comprehensive and Automated Techniques

Next-Gen XDR solutions offer a complete view of your security posture. They do so by integrating advanced security tools and technologies, like machine learning, into a single platform. This allows for real-time threat response.

NEXT-GEN XDR IS A NEW APPROACH TO CYBERSECURITY THAT COMBINES THE BEST FEATURES OF SEVERAL DIFFERENT TECHNOLOGIES INCLUDING EDR, SIEM AND SOC.

XDR Security Features

Your chosen XDR platform should include a variety of features offering comprehensive data protection. Some of these features include:



Disadvantages of Traditional XDR Security

Now that we've looked at some of the benefits of Next-Gen XDR, let's take a look at some of the disadvantages of traditional XDR security.

1. Lack of Integration

One of the biggest disadvantages of traditional XDR security is its lack of integration. This is because traditional XDR security relies on multiple disconnected products and silos of data within those products. This can make it difficult to get a complete picture of your security posture and can slow down threat detection and response.

To overcome this disadvantage, many organizations are now turning to next-generation XDR solutions that offer complete integration. Next-generation XDR solutions are designed to work together from the ground up, sharing data and insights across the entire platform.

This allows you to get a complete view of your security posture and speeds up threat detection and response.

2. Inefficient Threat Detection and Response

As enterprises become increasingly reliant on digital technologies, they are also becoming more vulnerable to cyberattacks. To address this growing threat, many organizations have adopted a security approach known as extended detection and response (XDR).

XDR security is a unified platform that combines multiple security solutions, including firewalls, intrusion detection and prevention systems, and endpoint security. While XDR security offers many benefits, it also has some disadvantages.

One of the biggest disadvantages of XDR security is its efficiency in terms of threat detection and response. This is because traditional XDR security relies on manual processes, which can be time-consuming and error-prone.

Additionally, traditional XDR security often lacks features like machine learning and artificial intelligence, which can help automate threat detection and response. As a result, organizations that rely on XDR security may be at a disadvantage when it comes to detecting and responding to common cyber threats.

3. High Costs

While traditional XDR security can be costly, there are some steps that organizations can take to help reduce costs. One way to do this is to purchase products from a single vendor. This can help to reduce the overall number of products that need to be purchased, and it can also make it easier to manage costs.

Additionally, organizations can look for vendors who offer discounts for purchasing multiple products. Another way to reduce costs is to automate some of the manual processes involved in traditional XDR security. This can help to save time and money by reducing the need for manual work.

Finally, organizations can use open-source tools whenever possible. Open-source tools are often free or low-cost, and they can provide a high level of security. By taking these steps, organizations can help to reduce the costs associated with traditional XDR security.

Disadvantages of Traditional XDR Security (Cont.)

4. Lack of Visibility

Lack of visibility is a common problem with traditional XDR security solutions. This is because these solutions often silo data within multiple products, making it difficult to get a complete picture of your security posture. This can lead to slowed threat detection and response times, as well as an increased risk of missed or false-positive threats.

To combat this problem, many organizations are now turning to next-generation XDR solutions that provide comprehensive visibility into the entire network. These solutions use cutting-edge machine learning and artificial intelligence technologies to constantly monitor network activity and quickly identify potential threats.

As a result, they can provide a much higher level of visibility and protection than traditional XDR solutions.

5. Poor Compliance

One of the potential disadvantages of traditional XDR security is that it can lead to poor compliance in your organization. This is because traditional XDR security silos data within multiple products. This can make it difficult to get a complete picture of your security posture and can slow down threat detection and response.

Additionally, traditional XDR security often lacks features like machine learning and artificial intelligence, which can help automate compliance processes. As a result, organizations using traditional XDR security may find it difficult to meet compliance requirements.

In contrast, next-generation XDR platforms that leverage machine learning and artificial intelligence can help simplify compliance processes and improve overall compliance rates.

6. Limited Protection Against Today's Threats

While traditional XDR security can offer some protection against cybersecurity threats, it has several limitations that leave organizations vulnerable. One of the biggest limitations is that traditional XDR security silos data within multiple products.

This can make it difficult to get a complete picture of your security posture and can slow down threat detection and response. Additionally, traditional XDR security often lacks features like machine learning and artificial intelligence, which can help you more quickly identify and respond to threats.

As a result, organizations that rely on traditional XDR security may be at a higher risk for cyberattacks.

Recommended Reading:

Is Managed XDR for You?
Here's How to Decide

Advantages of Next-Gen XDR Security

Now that we've looked at some of the disadvantages of traditional XDR security, let's take a look at how Next-Gen XDR can help address those disadvantages.

1. Better Integration

Traditional XDR security tools offer a limited view of your organization's security posture. This is because they only collect data from a single source. Additionally, traditional XDR tools lack features like machine learning and artificial intelligence, which can automate threat detection and response.

As a result, Next-Gen XDR offers better integration than traditional XDR security. Next-Gen XDR integrates data from multiple sources and provides a more comprehensive view of your organization's security posture.

Additionally, Next-Gen XDR includes features like machine learning and artificial intelligence, which can help automate threat detection and response. As a result, Next-Gen XDR is a more effective tool for managing your organization's security posture.

2. More Efficient Threat Detection and Response

Just as important as detecting threats is responding to them quickly and effectively. Next-Gen XDR can help you do both of these things more efficiently. By integrating data from multiple sources, Next-Gen XDR provides a more complete picture of your security posture.

This allows you to more quickly and accurately identify potential threats. Additionally, Next-Gen XDR uses machine learning and artificial intelligence to automate threat detection and response. This means that you can respond to threats more quickly and effectively, without having to rely on manual processes.

As a result, Next-Gen XDR can help you improve both your threat detection and response times, making your overall security posture more effective.

3. Lower Costs

As data and threats become more complex, organizations are turning to Next-Gen XDR for security. Next-Gen XDR is a more comprehensive approach to security that can provide better protection and visibility. Additionally, Next-Gen XDR can be less costly than traditional XDR security.

This is because Next-Gen XDR often requires the purchase of fewer products and can be less expensive to operate. Additionally, Next-Gen XDR often integrates with existing security infrastructure, which can help reduce costs.

As organizations continue to face new challenges, Next-Gen XDR will become an increasingly important part of their security strategy

4. Greater Visibility

As organizations increasingly rely on digital systems and data, the need for comprehensive security solutions has never been greater. Next-Gen XDR is a new type of security platform that promises to provide greater visibility into your network and more effectively identify and respond to threats.

Next-Gen XDR integrates data from multiple sources and provides a more comprehensive view of your security posture. This allows you to identify potential threats and take steps to mitigate them before they cause serious damage.

Additionally, Next-Gen XDR includes features like machine learning and artificial intelligence, which can help you more quickly identify and respond to threats.

By implementing a next-generation XDR solution, you can improve your organization's overall security posture and better protect your digital assets from harm.

5. Improved Compliance

Organizations face compliance requirements from a variety of sources, including government regulations, industry standards, and contractual obligations. Meeting these compliance requirements can be a challenge, particularly as they often evolve.

Next-Gen XDR can help improve compliance in your organization by integrating with existing compliance infrastructure and automating compliance processes. Additionally, Next-Gen XDR's machine learning and artificial intelligence capabilities can help you identify and respond to threats.

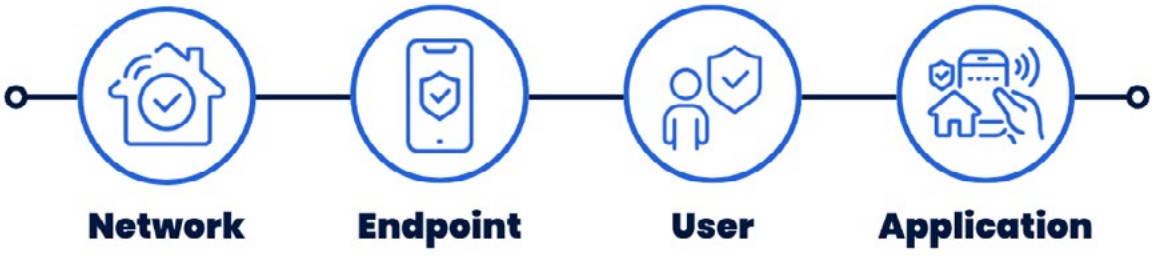
As a result, Next-Gen XDR can play a key role in helping your organization meet its compliance obligations more.

6. Greater Protection Against Today's Threats

As anyone who has followed the news knows, security threats are constantly evolving. What might have been a minor nuisance a few years ago can now pose a serious risk to your business. That's why it's important to have a security solution that can adapt to the changing landscape.

Next-generation XDR (extended detection and response) is designed to do just that. By integrating data from multiple sources and using advanced features like machine learning and artificial intelligence, Next-Gen XDR can provide a more comprehensive view of your security posture.

Additionally, Next-Gen XDR malware protection software is designed to be more agile and responsive, so you can more quickly identify and respond to threats. As the world of security becomes increasingly complex, Next-Gen XDR offers a powerful tool for staying one step ahead of the threats.



XDR vs Other Technologies

What is the Difference Between XDR and SIEM?

At its core, a SIEM platform collects, organizes, analyzes, then stores huge volumes of information. Its primary purpose in doing so is to provide analysis, aid in data storage, and support compliance/reporting objectives. Security analytics is indeed a component of SIEM.

But, this is a feature that has been tacked to many SIEM solutions. The reality is that SIEM security tools require a lot of fine-tuning and trial/error to implement into an enterprise.

If security is just relying on SIEM, then they're usually overwhelmed by the sheer number of alerts coming from the platform. This can cause them to miss important threats when they do appear.

On top of that, SIEM is a passive analytic tool. So, while it can provide alerts, it can't actively do anything to combat the security threats. XDR, on the other hand, is more actively geared toward security analysis.

This is thanks to both AI and automation within the platform, but also the way data is stored on the platform. With SIEM software, the tools work under the assumption that all data is found inside the SIEM platform.

Meanwhile, XDR tools work with data that is stored on any platform. The result is a security system that can not only rapidly detect threats but also proactively find them before they happen.

It helps prioritize which threats are a high priority for the security team, so nothing important slips by.

That's not to say that SIEM platforms don't have a place in security or compliance reporting. They're just not as efficient as XDR solutions at cybersecurity.

XDR tools work with data that is stored on any platform. The result is a security system that can not only rapidly detect threats but also proactively find them before they happen.

XDR vs Other Technologies

What Is the Difference Between XDR and EDR?

With the help of threat intelligence and data analytics, security solutions like EDR and XDR can automate security operations. At the same time, they'll provide the essential endpoint protection and threat detection.

There are numerous options for endpoint security on the market. But, before committing to endpoint detection and response (EDR), it may be worthwhile to learn about the advantages offered by cross-domain XDR solutions.

Capabilities

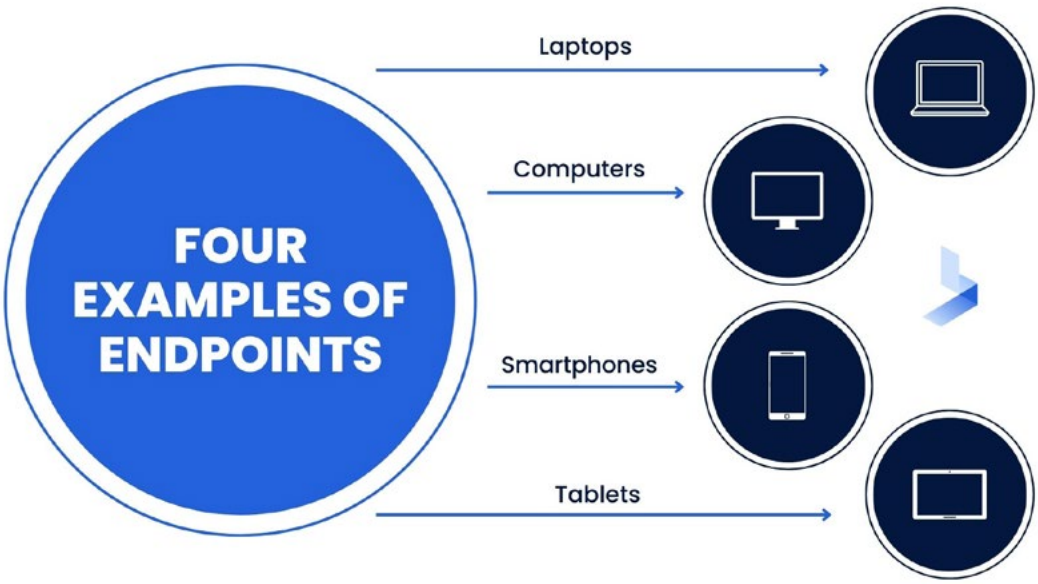
If you're familiar with EDR, you already know that XDR is different. It's a cutting-edge security solution that improves upon previous methods of endpoint protection by offering more advanced features than those found in standard EDR tools.

Although EDR is a vital tool for warding off assaults at the endpoint, it can only defend against threats that are reflected in the data collected from those devices. XDR is a development of EDR that goes beyond the endpoint to guard against and identify attacks using a wide variety of methods by integrating the features of traditional security products like SIEM, UEBA, NDR, and EDR.

To make it easier to investigate and respond, XDR correlates and stitches together this rich data and brings together similar warnings in a centralized user interface.

Limitations in threat visibility, an increase in false positives, and extended investigation timeframes are all possible when using an EDR technology with data collected just from endpoints.

If you're looking to streamline your security processes, XDR solutions may assist by protecting all of your data, not just what's on individual endpoints. XDR helps to automate many of the tasks that are often performed manually by EDR, and it also delivers threat information and analytics straight out of the box.



Recommended Reading:

EDR vs MDR vs XDR: How They Differ and Which One is Right For You

10 Ways XDR Saves Businesses Money

1. SALARIES FOR CYBERSECURITY PROFESSIONALS

In theory, an on-prem SOC is the most effective way to secure your organization's network. Yet, employing and maintaining a full cybersecurity staff is an expensive endeavor for any business. These are the average yearly salaries of cybersecurity team members.

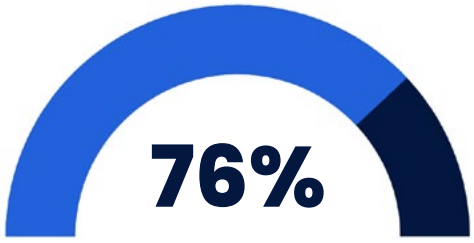
Most companies require as many as four security analysts and engineers to effectively run security operations, making the average cost for yearly cybersecurity staff salary $739,000-$1,708,000.

Unfortunately, these estimates don't include the cost of 24/7 monitoring and employee benefits. It's common for cybersecurity professionals to work long hours, with over half of cybersecurity professionals working more than 40 hours each week and some working up to 90. Yet, even with a full team working a top number of hours, you'd likely need to double your cybersecurity headcount to achieve 24/7 security oversight and response capabilities.

$739,000 to $1,708, 000

The average cost for yearly cybersecurity staff salaries.

Along with your team's salary and benefit requirements, recruitment is a critical cost that can be easily overlooked when calculating the salary of a full-time cybersecurity staff. Over two-thirds (67%) of security professionals say they don't have enough talent on their team. With $465,000 cybersecurity workforce roles unfilled in the US alone, recruitment is fiercely competitive, increasing the cost and time spent by organizations seeking talent.



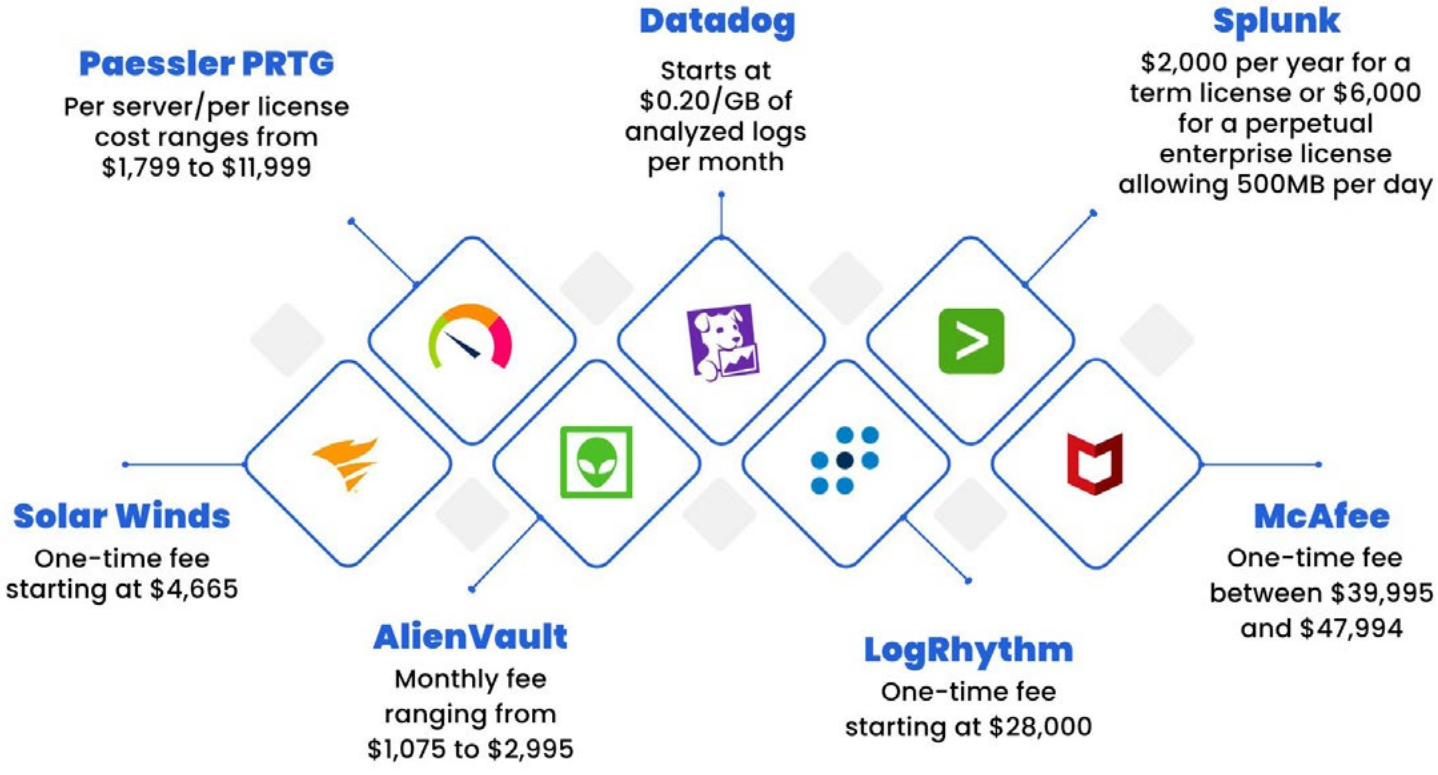
The percentage of security professionals who say they don't have enough talent on their team.

2. CYBERSECURITY TOOLS

On average, organizations employ 29 different cybersecurity tools. Such tools can range from a typical firewall to complex software designed to carry out multiple security tasks. Business organizational networks continually grow and change for a variety of reasons including company growth and new workforce requirements. The cyberthreat landscape is continually growing as well. Because of this ongoing evolution, businesses must constantly upgrade cybersecurity tools to maintain an effective cybersecurity posture. These investments don't come cheap.

For example, SIEM is a pivotal part of any cybersecurity system. When properly optimized and run by experienced professionals, the software provides storage, analysis, reporting, real-time monitoring, correlation, and notifications of and from network log data. SIEM tool prices range from a single fee to per-server, per-license fees, or fees based on amounts of logged data. An exploration of the cost of SIEM tools reveals a considerable investment.

Considering that SIEM is a single tool in your 29-piece cybersecurity toolbox, tool costs can quickly eat up your cybersecurity budget. Even worse, these tools can be rendered ineffective without the funds to cover the cost of implementation, training, staffing, and maintenance costs. Depending on the tools you choose, you may also be facing additional costs for hardware and infrastructure that can exceed the costs of the tools themselves.



The fraction of time it takes for an XDR solution to optimize and provide value vs. other tools.

25%

3. INITIAL OPTIMIZATION AND TIME TO VALUE

Cybersecurity tools and systems are not out-of-the-box solutions that magically solve security issues upon deployment. While tools that utilize machine learning (ML) and artificial intelligence (AI) can accomplish tasks that humans can't complete alone, they are tools designed to be used by professionals.

Modern cybersecurity solutions that collect and parse mass amounts of data, recognize suspicious activity, and launch automated response activities must be optimized to perform properly. Upon purchasing a new tool or system, your team will need to integrate the new software with existing solutions, set a baseline of use cases, and configure alerts.

Full optimization of cybersecurity tools that ingest and analyze data requires your team to identify and group data, weed out unimportant data and unknowns, conduct tests, provide feedback, and configure system reactions to alerts. As the number of log sources and endpoints your business needs to integrate grows, the time and effort spent integrating and optimizing tools increases. This is a process that could take weeks or even months to complete.

Furthermore, if you don't have dedicated cybersecurity specialists familiar with the equipment, you'll likely need to pay a third-party team to optimize software and tools for effective results. Conversely, an experienced XDR provider will take about 25% of the time an organization will take on its own to optimize tools and provide full value.

4. TRAINING EXPENSES

Cybercriminals are innovative, determined, and always learning new ways to breach systems for monetary gain. Technology is advancing faster than ever before. Cybersecurity is not a stagnant profession with a single set of rules that lasts the span of a career. Cybersecurity professionals like security analysts and engineers must participate in ongoing training and upskilling programs to understand new threats, tools, and tactics.

For instance, the Certified Information Security Professional certificate must be renewed every three years by obtaining continuing education. The cost of maintaining the certification is only $85 annually. However, this price doesn't reflect the cost of training for recertification or the approximately 120 hours each professional spends on updated training each year.

Recommended Reading:

Eliminate Cybersecurity Burnout with XDR

5. COMPLIANCE

Large firms report the average cost to maintain compliance can total up to $10,000 per employee. While compliance regulations safeguard against risks, they create a significant burden for IT and security professionals tasked with maintaining them. Federal, state, and local regulations vary by industry and other factors about your business operations. Gartner estimates that by 2023, 65% of the world's population will have its personal data covered under modern privacy regulations. Some of the most common regulations businesses must follow include: HIPAA, GDPR, PCI DSS, CMMC, FERPA, COPPA and GLBA.

To maintain compliance with these regulations, companies must follow specific business operations and record-keeping requirements. As a result, the cost of meeting and maintaining compliance comes from many different sources, including:

Soft costs of preparing for an audit: These costs depend on your current cybersecurity posture and may include preparations necessary to meet requirements, costs of hiring a third-party provider for a gap assessment, costs of devising a security plan, and other costs associated with bringing your organization's security practices up to date.

Hard costs for tools and services: Depending on the size of your company and your current cybersecurity posture, these costs may include tools that provide multi-factor authentication, log monitoring, data backup, etc. Other hard costs when preparing for an audit might include a professional gap assessment or services from cybersecurity professionals to help your organization create new security processes.

Hard costs of a third-party audit: A third-party audit is a professional comparison of your business's security processes to the policies outlined in a specific set of regulations. The cost of such an audit will likely depend on the size of your company, market rates, and the specific regulations involved.

$10,000

The average cost per employee to maintain compliance

$235,000

The average amount a company stands to lose if they face a GDPR non-compliance issue

$100,000

The potential cost of a GLBA violation

The Cost of Non-Compliance

Like most things in cybersecurity, the cost of failure when it comes to compliance can be much higher than the cost of prevention. On average, an organization stands to lose over $235,000 if they face a GDPR non-compliance issue. The maximum civil penalty for violating COPPA is $40,000 for a single individual. While that might seem minuscule if your organization is facing a cost of over $50,000 to achieve compliance, it's important to remember that the fine will be multiplied for every individual involved.

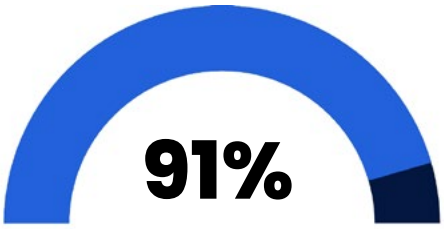
HIPAA violations fall into 4 tiers. Maximum fines per violation in tiers 1-3 are $50,000. For tier 4 violations, $50,000 is the minimum fine per violation. GLBA penalties can result in fines of $100,000 for each violation. Federal non-compliance fines are not the only costs for companies that fail to meet required standards. For instance, violations of CalOPPA (California state privacy laws) can result in a penalty of $2,500 per violation.

The costs of non-compliance do not begin and end with fines. Other lesser known costs of noncompliance include:

- Prison time
- Lawsuits and other legal fees
- Downtime and loss of productivity
- Difficulty in securing capital or financing
- Damage to company reputation
- Lost business partnerships

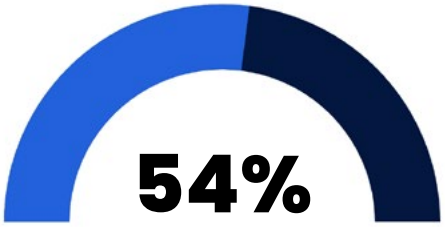
6. REMOTE WORK IMPLEMENTATION COSTS

Pandemic restrictions brought about remote work across practically all industries. Even as restrictions were lifted, successful remote work operations paved the way for a new normal of hybrid workforces for many organizations. 91% of workers in the US working at least some of their hours remotely are hoping their ability to work at home becomes permanent. While 54% are hoping for a hybrid work schedule, 37% would like to work from home exclusively.



Employees hoping to retain some ability to work from home

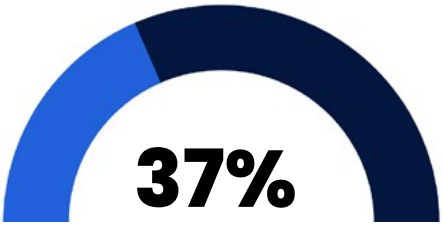
Although employees are comfortable working from home, these extended networks present more cybersecurity vulnerabilities. To provide security against long-term risks, organizations will have to deploy new security controls for remote devices. For companies depending on internal resources alone, expanding efficient security practices to remote workers may require increased headcount within your cybersecurity team and additional tools and software applications to protect remote devices. The cost of cybersecurity for remote and hybrid workforces will depend heavily on the size of your company, the sensitive data that requires protection, and your industry regulations.



Employees who would like a hybrid work schedule

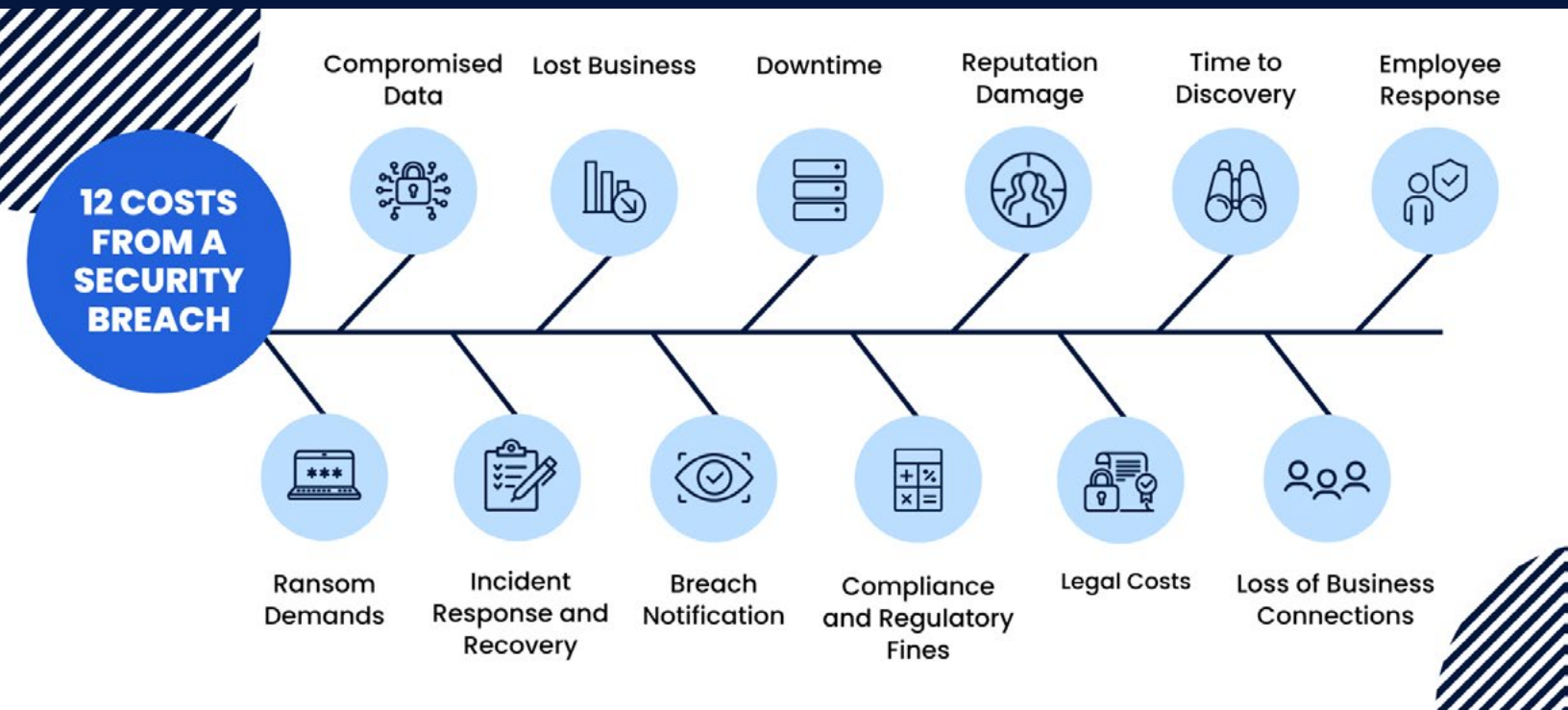
7. THE COST OF A BREACH OR ATTACK

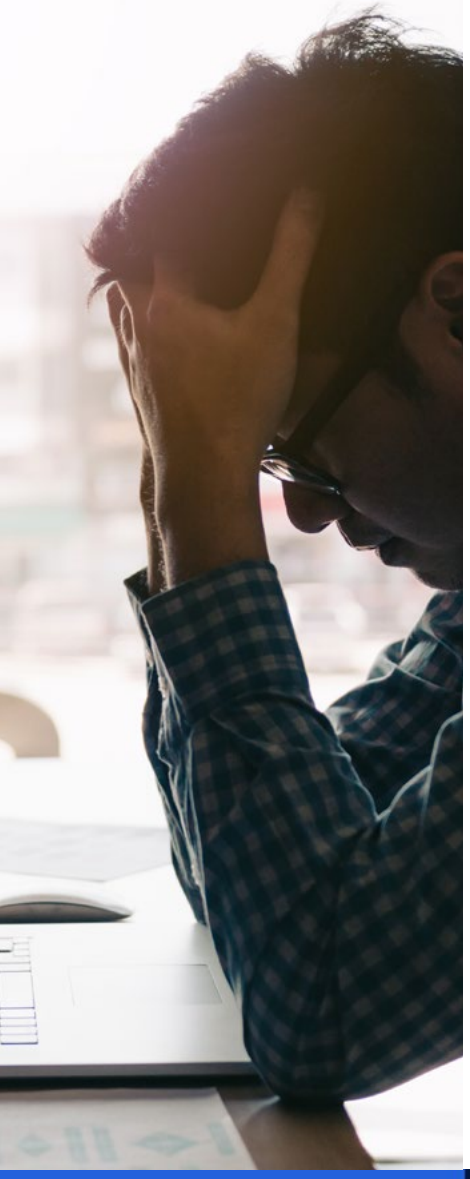
No matter the cost of your cybersecurity investments, one thing is certain. The cost of a breach or other successful cyberattack will be significantly more expensive. The average cost of a data breach in 2021 was 4.24 million, a 10% increase from 2020. Yet, data breaches in the US average around $9.05 million. The average ransom demand is around $220,298. However, requests for outlandishly high payments have more than doubled, with 11% of companies paying $1 million or more. Unfortunately, these startling figures fail to tell the whole story when uncovering the ongoing costs of a cybersecurity attack. Some costs are much more difficult to estimate.



Employees who would like to work from home exclusively

The average ransom demand is $220,298



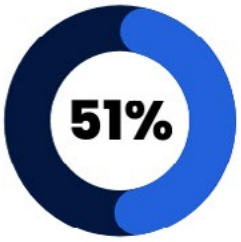


8. THE COST OF BURNOUT

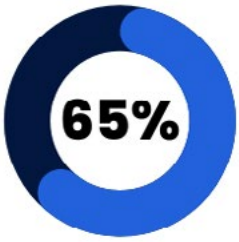
It's no surprise that cybersecurity is a high-stress profession. Security professionals face hundreds of alerts daily, many of them false. With enormous task loads, the job becomes a high-stakes game of risk prioritization where a single mistake can lead to a successful attack. In recent years, increased remote work, the use of IoT devices, and cloud adoption have increased workloads for all levels of cybersecurity professionals. In the meantime, a talent shortage combined with burnout means internal cybersecurity teams are shrinking.

Burnout in cybersecurity is becoming increasingly common. There are currently about 435,000 cybersecurity job openings in the US. The unemployment rate in the industry is 0%. 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.

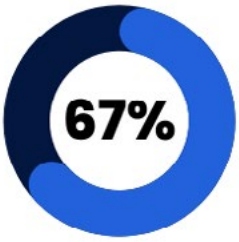
The cost of burnout for businesses depending solely on internal security teams can quickly add up.



Experienced extreme stress or burnout in 2021



Considered leaving their job because of job stress



Wouldn't recommend a career in the same industry

BURNOUT IN CYBERSECURITY

5 Symptoms of Burnout

1. Exhaustion
2. Negative feelings and mental distance toward the job
3. Reduced performance
4. Indifference
5. Turnover

9. THE COST OF DWELL TIME

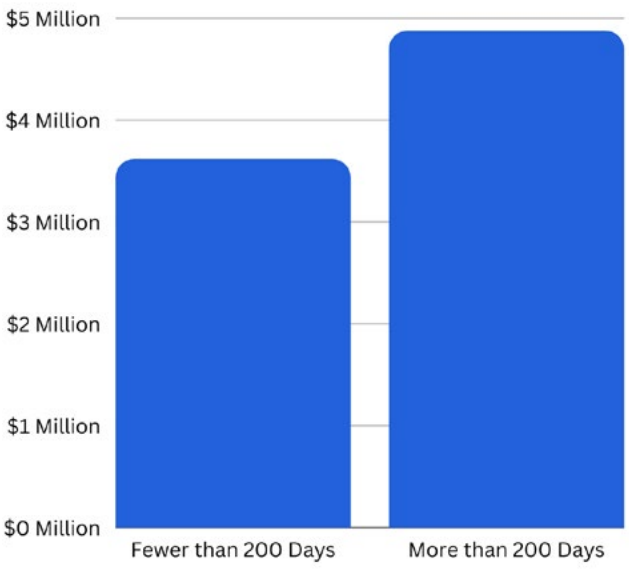
Modern sophisticated cyberattacks rarely use brute force tactics used to breach your organization's external perimeter. Instead, attackers use discrete methods to quietly infiltrate your network and spend time mining data or reaching an objective that will result in bigger financial gains. These slow and low attacks depend entirely on the amount of time an attacker can spend lurking in your network without being noticed. Referred to as dwell time, the time an attacker spends in your network can lead to larger data leaks or credential theft that can increase a hacker's level of authority.

The average time taken for organizations to contain data breaches in 2021 was 287 days. Breaches with a lifecycle of over 200 days had an average cost of $4.87 million compared to $3.61 million for breaches with a lifecycle of fewer than 200 days. Short-staffed security teams or those depending on multiple tools with minimal integration technologies are less likely to have the resources to recognize suspicious behavior within the network, resulting in longer dwell time and the increased likelihood of an attack.

10. MAINTAINING 24/7 MONITORING AND RESPONSE

Cybercriminals don't work office hours. In fact, some of the most successful attacks occur when businesses are closed for the night, weekend, or holidays. As a result, many organizations are beginning to recognize the need for 24/7 cybersecurity monitoring and response. If you're running a fully-staffed SOC, you're probably confident that your business has adequate protection during business hours. Yet, unless your team works 24/7, your organization is unprotected more than half the time.

So, how can businesses close this enormous security gap? If an organization depends on internal resources alone, achieving 24/7 monitoring and response would require an additional security team to work off-hours. Even if both teams worked a maximum of overtime, the business would need to double the budget typically required for an on-prem staff salary. Furthermore, the talent shortage in the industry will likely require high-level salaries and increased benefits for the successful recruitment and retainment of qualified professionals. As a result, your organization would need to increase the budget for recruitment as well.



Breach Lifecycle vs Cost

ROUNDUP: 10 WAYS XDR REDUCES CYBERSECURITY COSTS

Extended detection and response (XDR) is an outsourced cybersecurity option that provides your organization with a security solution customized to the needs of your organization. A collection of services and tools, XDR is a turnkey solution designed to tackle the modern cybersecurity threat landscape and the issues affecting internal IT and security teams of all sizes. XDR is a group of services that offers organizations the protection of an off-site SOC combined with a comprehensive security stack that allows organizations to rapidly detect, analyze, investigate, and actively respond to cybersecurity threats. It also offers many companies a solution that will considerably decrease the upfront and ongoing costs of cybersecurity.

A fully staffed remote SOC is included in the monthly cost of maintaining XDR. Instead of dealing with the increasing recruitment challenges and rising salaries in the industry, you can depend on trained and experienced professionals provided as part of the service.

XDR is cloud-based and scalable to meet the needs of any growing business. This growth can include company growth or the protection required to include the addition of devices, infrastructure, and software required for remote work

XDR is a turnkey solution that includes a preconfigured cybersecurity stack with modern tools and services.

XDR is a fully effective end-to-end solution designed to tackle the complexities of the modern cybersecurity landscape. Utilizing it for your organization means you'll be less likely to become the victim of a successful attack.

As a turnkey solution that provides both tools and assistance from cybersecurity professionals, XDR includes the optimization of tools and software included with the service. Organizations can recognize time-to-value in a fraction of the time.

XDR is customizable to provide a complete cybersecurity solution or act as an extension of your existing efforts. By automating specific services and adding the increased cybersecurity headcount offered by an off-site SOC, you can eliminate many of the causes of burnout in cybersecurity

The remote SOC included with XDR security offers your organization the opportunity to supplement your existing team with experienced professionals that act as an extension of your team. As a result, internal security professionals can gain greater knowledge from working with experienced professionals in your XDR vendor's remote SOC.

Highly effective monitoring and response actions supplied by modern cybersecurity tools and trained experts mean that attackers will have little chance of dwelling in your network for long periods of time without detection

XDR services are tailored to meet the individual security requirements and goals of each organization. While compliance might not be the overarching goal of the service, improved cybersecurity compliance as it relates to your industry can cut some of the major costs associated with cybersecurity compliance maintenance.

XDR works 24/7/365 so your internal team has time to eat, sleep, and go on vacation.

Recommended Reading: 3 Ways XDR Security Improves SOC Efficiency

How to Choose the Right XDR Vendor

When choosing an XDR solution, there are a few things you'll need to keep in mind:

- Your company's specific security requirements
- The features and capabilities offered by different vendors
- The cost of the solution

It's important to find an XDR solution that meets your company's specific security requirements. There are many different vendors and solutions on the market, so you'll need to do your homework to find one that's right for your business.

You should also consider the features and capabilities offered by different vendors. Some vendors may offer more comprehensive solutions than others. Be sure to compare the features of each vendor to find one that best meets your needs.

Finally, you'll need to consider the cost of the solution. XDR solutions can be expensive, so you'll need to make sure the benefits justify the cost.

Must-Have Features for Your Future XDR Provider

When evaluating XDR vendors, there are a few key features you should look for:

- The ability to integrate with your existing security infrastructure
- Comprehensive detection and response capabilities
- An easy-to-use interface
- 24/7 customer support

The vendor you choose should be able to integrate with your existing security infrastructure. This will ensure that the solution works seamlessly with your other security tools and systems.

The vendor's solution should also have comprehensive detection and response capabilities. This will allow you to quickly identify and respond to threats.

The interface of the vendor's solution should be easy to use. You shouldn't need a lot of training to be able to use the tool effectively. Additionally, the vendor should offer 24/7 customer support in case you have any questions or run into any problems.

XDR security is a powerful tool that can help businesses improve their overall security posture. By choosing the right XDR vendor and implementing a comprehensive security strategy, you can keep your business safe from cyber threats.

Recommended Reading:

The Complete Checklist for Choosing an Extended Detection and Response (XDR) Provider

Comparing XDR Vendors

SHOPHOS XDR

OVERVIEW

The Sophos platform provides some of the most comprehensive services of all the XDR vendors on our list. For one thing, it has a fully optimized XDR security array, with synchronized cloud data.

It also leverages next-generation tech like AI, secure firewalls for remote workers, and anti-ransomware options to provide full security.

FEATURES

- The Cloud Optix threat response platform constantly monitors cloud infrastructure
- The Intercept X Endpoint, provides excellent endpoint protection
- Malware and threat detection systems use deep-learning AI algorithms
- Offers a suite of WiFi, email, and mobile security programs

MCAFEE XDR SOLUTIONS

OVERVIEW

McAfee is a solution both for private home users as well as businesses. McAfee also offers MVISION, a threat detection and elimination system that lives on the cloud.

As for pricing, you can request a free demo for McAfee's Enterprise solution, and a free one-month trial comes standard for Windows PC.

The Family plan includes a $39.99 one-year subscription for 10 devices. You can also opt for the Single Device individual plan, at $29.99 per year for one device.

FEATURES

- Offers 24/7 monitoring, threat detection, and in-depth threat investigations
- Device-to-cloud security
- The MVISION cloud-based platform to monitor and automate your extended detection and response strategy.
- Offers a number of pricing plans tailored to suit individual or business needs
- Antivirus and security backups for both cloud and endpoint

CISCO XDR

OVERVIEW

Cisco's XDR platform is called Cisco SecureX.

As with McAfee's MVISION solution, Cisco SecureX lives on the cloud and allows you to orchestrate a versatile security setup that accords with your company's needs. Similar to Symantec, to purchase SecureX you'll need to locate a Cisco partner, who will then work with you on a pricing plan.

FEATURES

- Analytics programs
- Automated workflows
- Nearly 200 out-of-the-box integrations
- Expert guidance
- Top-tier threat intelligence through the Cisco Talos team of security experts

PALO ALTO NETWORKS XDR PLATFORM

OVERVIEW

Palo Alto Networks offers the Cortex XDR platform, which affords comprehensive threat detection and response. Perfect for small to large businesses, this XDR platform works at the cloud, network, and endpoint nodes of the threat chain.

Cortex XDR comes in two tiers, the Cortex XDR Prevent and the Cortex XDR Pro. Contact the sales officers at Palo Alto Networks to learn about the detailed price points of both services.

FEATURES

- Integrated responses, automated analysis, and some of the best threat detection and prevention in the business
- Offers a host of managed detection and response services (MDR)
- AI-based analytics are optimized to detect evolving threats
- A veritable defensive bulwark of Next-Gen firewalls, endpoint security measures, and detection algorithms
- Machine-learning programs create behavioral profiles and stop new threats in their tracks

CYNET XDR

OVERVIEW

Cynet is an excellent platform for both small and large businesses.

It works as an Autonomous Breach Protection platform, which provides some of the most impregnable XDR technology. The system can discover and eliminate many threats, using next-generation antivirus (NGAV), user entity and behavior analytics (UEBA), and network traffic analysis.

Cynet has free 14-day trials, with more detailed quotes available for their pricing plans.

FEATURES

- Works overtime to analyze all network endpoints to search for active malware and other threats
- Has the flexibility of sophisticated programs to make rapid decisions
- Manual and automated remediation for files, hosts, and networks
- The ability to track infiltration and deception methods by planting false passwords, data files, and monitoring network connections
- Automated remediation technology allows the platform to continuously gather and monitor threat levels throughout the network

SYMANTEC XDR

OVERVIEW

Symantec is among the best XDR systems on the market, with a good reputation among users.

As far as its performance capabilities, Symantec is fully able to detect and resolve threats using its advanced suite of features. This includes powerful detection software and analytical programs, and AI-guided security systems.

The purchase plan for Symantec XDR requires your business to select a partner or distributor based on region and country.

FEATURES

- Detection protocols are continually updated by Symantec researchers to respond to new threats
- EDR console offers access to expert advice and guidance
- The system is customizable so you can automate certain routine and repetitive tasks
- Pricing is typically available at around $70 per year for a license

BitLyft AIR®

OVERVIEW

BitLyft AIR® offers holistic protection against cyber threats—at a fraction of the price. Our all-inclusive cybersecurity platform combines innovative automation with the power of people to provide unparalleled protection.

BitLyft AIR® combines four powerful threat protectors—security incident and event management, security operations center, security orchestration, automation and response, and central threat intelligence—to offer unbeatable protection from cyberattacks.

FEATURES

- Helps your business meet its detection and response goals through the guidance of expert support staff
- Provides access to a support team that is familiar with your business, goals, and threat environment
- Unique software automation is designed for a swift response as soon as a threat is detected
- Versatile scalability allows you to upgrade your services and protection as your business grows
- Hundreds of automations save security teams countless hours

Affordable Pricing for Every Business*

Every business deserves protection against cyber threats. That is why we've created one of the most competitive pricing structures on the market. And we're not afraid to share it.

Plan Name	Troposphere	Stratosphere	Mesosphere	Enterprise
BitLyft AIR® Platform *(Price per month)*	$1,899	$2,099	$6,499	Starts at $10,499
Professional Service Onboarding *(*Starts at)*	$500*	$2,000*	$5,000*	Starts at $5,000
Features				
Number of Users to Protect	Unlimited	Unlimited	Unlimited	Unlimited
Integration Data Retention	21 Days	45 Days	60 Days	365 Days
Data Retention for Alerts Triggered and Incident Response	365 Days	365 Days	365 Days	365 Days
Reporting	Basic		Advanced	
Maintenance and Support	8 AM – 5 PM M–F Standard		8 AM – 5 PM M–F Priority	
Built-in Automations and Orchestrations	3	10	25	Starts at 80
BitLyft Essential Rules	Tied to integration turned on		60	Starts at 80
Number of Integrations	1	3	5	Starts at 10

*Pricing is subject to change at any time without prior notice.

Read to see BitLyft AIR® in action?

Click on the button to schedule a free demo.

BOOK A FREE DEMO


BitLyft
Cybersecurity