



Ten Questions an MSSP Should Ask their Customers About XDR (with Answers)

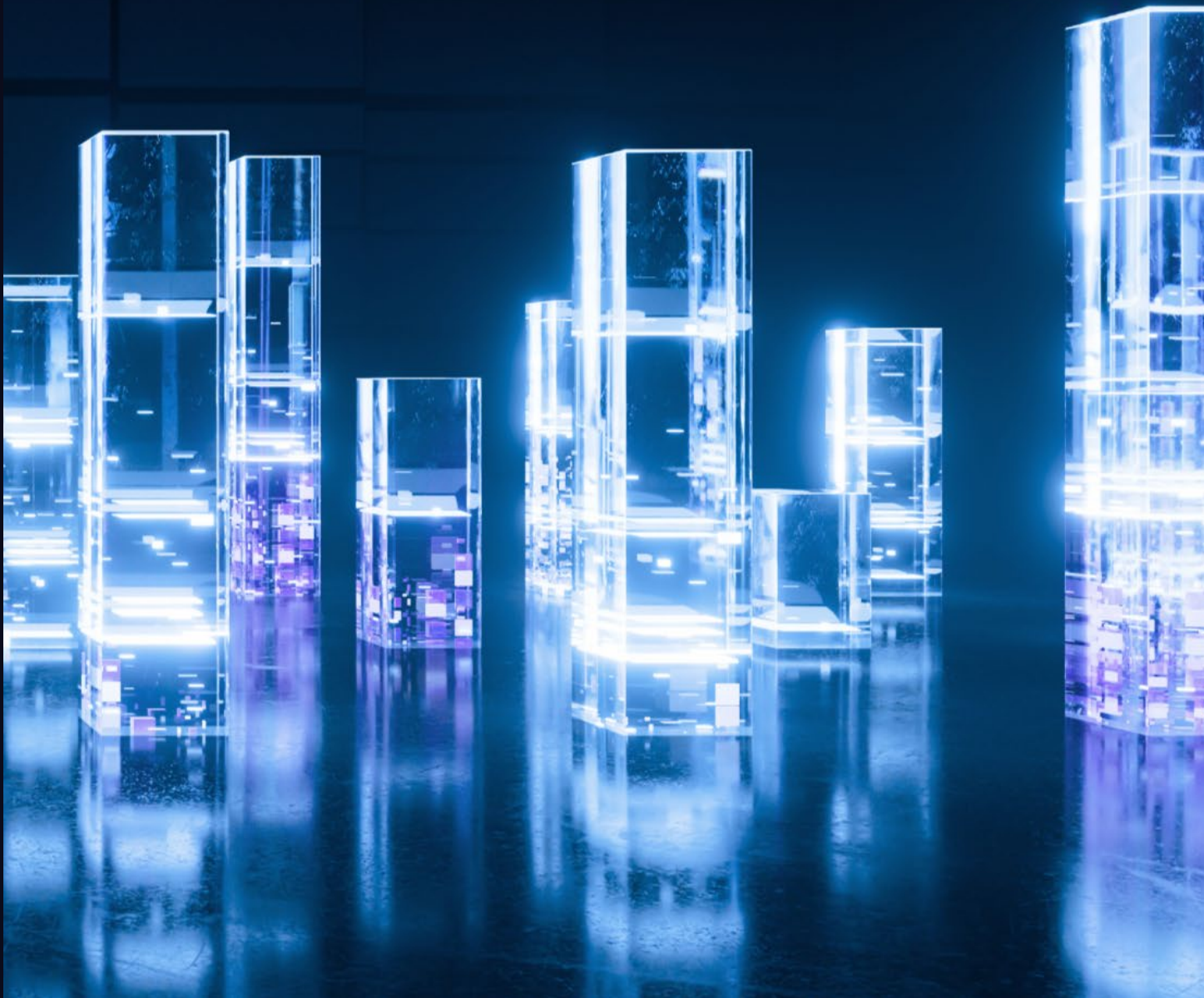


Table of Contents

Introduction	3
What Problem Does XDR Solve?	4
What Are the Challenges Your Customers Face When Implementing XDR?	5
Five Things to Look for in an XDR Solution	6
Ten Questions an MSSP Should Ask their Customers About XDR (with Answers)	7
Conclusion	11
Tomorrow's Threats Require a New Enterprise Security Paradigm	12





63%

Of organizations report EDR as a core capability within the endpoint security solution.

(ESG, "XDR: Spawning a Disruptive Modernization of Cybersecurity")

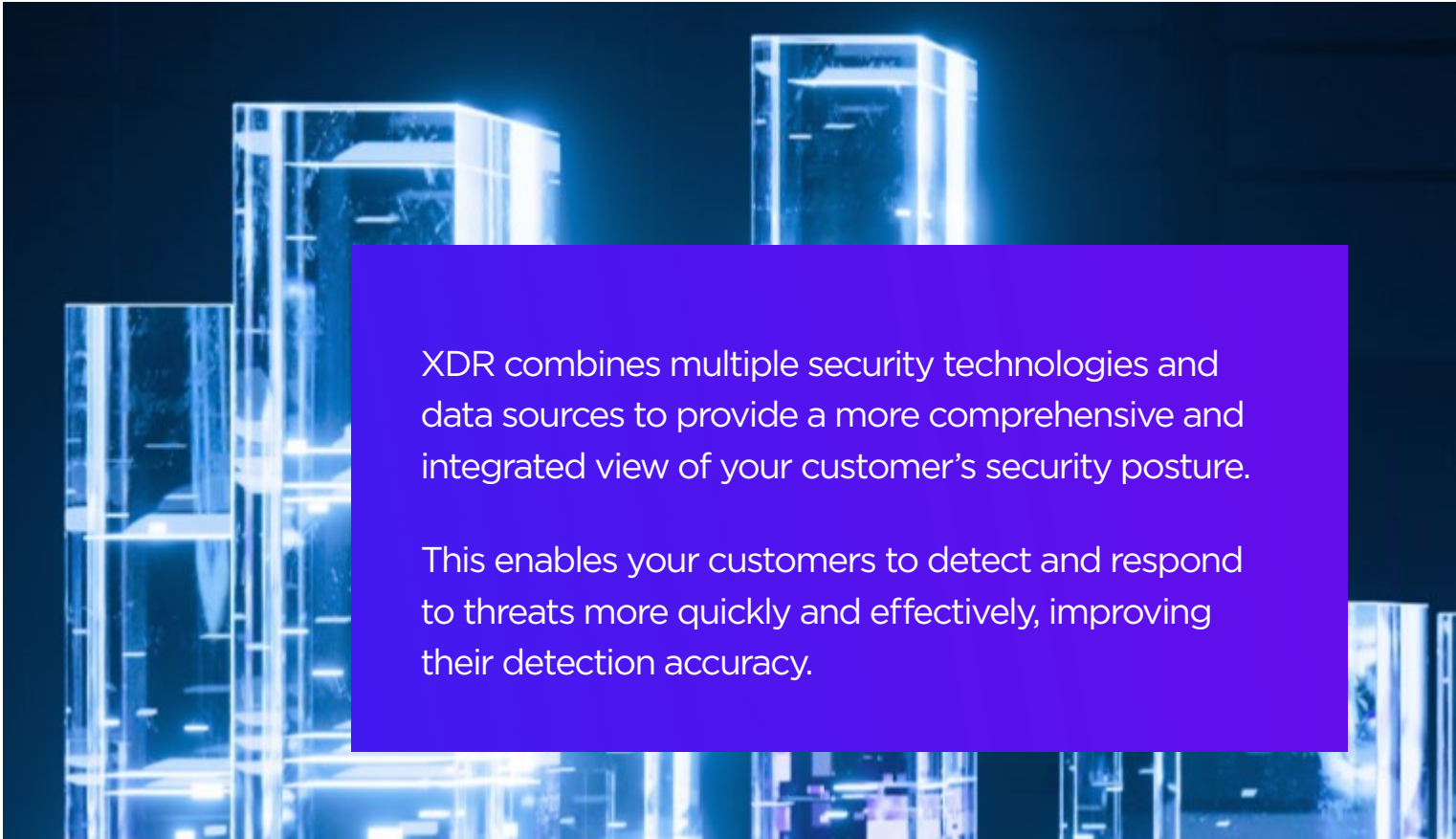
As an MSSP, staying informed about the latest security technologies and approaches to protect your customers from cyber threats is important. A technology that has recently gained significant attention is XDR, or Extended Detection and Response.

XDR provides a comprehensive and integrated approach to security, combining multiple technologies and data sources to detect and respond to threats more effectively than traditional AVs, EPP or EDR security solutions.

In this white paper, we provide ten key questions that an MSSP should ask their customers about XDR to help them understand the benefits and potential drawbacks of implementing this technology in their organizations.

What Problem Does XDR Solve?

XDR solves the problem of inadequate and fragmented security solutions. Traditional security solutions often focus on a single technology or data source, such as antivirus software or intrusion detection systems. This can leave gaps in customer's security posture and make it difficult to detect and respond to threats effectively. XDR addresses this problem by combining multiple security technologies and data sources to provide a more comprehensive and integrated view of your customer's security posture. This enables your customers to detect and respond to threats more quickly and effectively, improving their detection accuracy. This can help your customers reduce the impact of security incidents and minimize their potential losses from security breaches.



XDR combines multiple security technologies and data sources to provide a more comprehensive and integrated view of your customer's security posture.

This enables your customers to detect and respond to threats more quickly and effectively, improving their detection accuracy.

What Are the Challenges Your Customers Face When Implementing XDR?

There are several challenges customers may face when implementing XDR, including:

1. Cost and complexity

XDR solutions can be more expensive and complex than traditional security solutions, requiring time, money, and expertise to implement and manage effectively.

2. Integration with existing security technologies and processes

XDR benefits from integrating with customer's existing security technologies and processes, which can be challenging and require effort and resources to implement.

3. Expertise and training

XDR may require a high level of expertise and training for staff to use and manage effectively, which can be challenging for your customers with limited security resources or expertise.

4. Resistance to change

Implementing XDR may require significant changes to customer's security infrastructure and processes, which can be met with resistance from staff or other stakeholders.

To overcome these challenges, MSSPs should plan and prepare for XDR implementation, engage and communicate with all relevant stakeholders to gain support and buy-in for the XDR implementation, and provide training and support to ensure that staff is equipped to use and manage the XDR solution effectively.

Five Things to Look for in an XDR Solution

When evaluating XDR solutions, there are several key factors to consider, including:

- 1.** An XDR solution should comprehensively cover a customer's security posture, combining multiple security technologies and data sources to provide a more complete and integrated view of potential threats and vulnerabilities. Look for solutions that provide open XDR, like SentinelOne. Open XDR provides your customers with the flexibility and control they need to customize and optimize their security posture and enables them to combine SentinelOne's advanced XDR capabilities with their existing security tools and processes. This allows customers to integrate their security technologies and data sources with SentinelOne's XDR solution.
- 2.** An XDR solution should provide real-time visibility into security incidents and threats, enabling customers to respond more quickly and effectively to potential threats. SentinelOne's XDR solution uses machine learning and other advanced technologies to give customers real-time visibility into their security posture and the ability to detect and respond to threats more effectively. This can help customers reduce the impact of security incidents and minimize their potential losses from security breaches.
- 3.** An XDR solution should use advanced technologies, such as machine learning and data analysis, to improve threat detection accuracy and reduce false positives. SentinelOne's XDR solution uses machine learning and data analysis to identify potential threats and anomalies and filter out false positives. This can help customers improve the accuracy of their threat detection and focus their resources on the most serious threats. SentinelOne's XDR solution also includes behavior analysis, which can provide customers with additional insights and context to help them identify and respond to potential threats more effectively.
- 4.** An XDR solution should be able to integrate with customer's existing incident response processes and procedures to enable more efficient and effective threat response. SentinelOne's XDR solution includes incident response automation and data breach detection features, which can help customers respond more quickly and effectively to potential threats and incidents.
- 5.** An XDR solution should be scalable and flexible to support the customer's growth and evolving security needs. It should also be able to integrate with a customer's existing security technologies and processes to provide a seamless and integrated security solution. SentinelOne's XDR solution is designed to support customers' growth and evolving security needs and can be easily scaled up or down to meet changing requirements. SentinelOne's XDR solution is also open and flexible, allowing customers to integrate their existing security technologies and data sources with SentinelOne's XDR capabilities. This enables customers to customize and optimize their security posture and provides them with the control they need to ensure the security and resilience of their critical assets and data.

Ten Questions an MSSP Should Ask their Customers About XDR (with Answers)

1. **What is XDR, and how does it differ from traditional security solutions?**

XDR is a new approach to security that combines multiple security technologies and processes to provide a more comprehensive and integrated approach to visibility, threat detection and response across your entire estate.

This differs from traditional security solutions, which typically focus on a single security technology or processes, such as antivirus software or intrusion detection systems. XDR provides a more holistic view of a customer's security posture by combining multiple data sources and security technologies to identify and respond to threats more effectively.

2. **How does XDR integrate with our existing security infrastructure and processes?**

XDR is designed to integrate seamlessly with a customer's existing security infrastructure and processes. This typically involves integrating XDR with existing security technologies and data sources, such as firewalls, endpoint protection, and network security tools, to provide a more comprehensive view of a customer's security posture.

XDR can also be integrated with existing incident response processes and procedures to enable more effective and efficient threat response. Additionally, XDR can be integrated with security operations centers (SOCs) and other security teams to provide real-time visibility and actionable insights into security threats and incidents.

3. **How does XDR help us detect and respond to security threats more effectively?**

XDR helps customers detect and respond to security threats more effectively by combining multiple security technologies and data sources to provide a more comprehensive view of a customer's security posture. This allows XDR to identify potential threats that may be missed by traditional security solutions that focus on a single technology or data source.

Further, XDR provides real-time visibility into security incidents and threats, enabling security teams to respond more quickly and effectively. XDR also uses machine learning and other advanced technologies to improve threat detection accuracy and reduce false positives, helping customers focus their resources on the most serious threats.

4. What are XDR's key features and capabilities, and how do they benefit our customer?

XDR's key features and capabilities include:

1. XDR combines multiple security technologies and data sources to provide a more comprehensive view of a customer's security posture.
2. XDR provides real-time visibility into security incidents and threats, enabling security teams to respond more quickly and effectively.
3. XDR uses machine learning and other advanced technologies to improve the accuracy of threat detection and reduce false positives.
4. XDR can be integrated with existing incident response processes and procedures to enable more efficient and effective threat response. These features and capabilities can benefit customers by providing a more comprehensive and integrated approach to security, enabling them to detect and respond to threats more quickly and effectively and improving the accuracy of their threat detection. This can help customers reduce the impact of security incidents and minimize their potential losses from security breaches.

5. How does XDR help us reduce false positives and improve the accuracy of our threat detection?

XDR uses machine learning and other advanced technologies to improve threat detection accuracy and reduce false positives. By combining multiple security technologies and data sources, XDR can provide a more comprehensive view of a customer's security posture and identify potential threats that may be missed by traditional security solutions that focus on a single technology or data source.

In addition, XDR uses advanced algorithms and data analysis techniques to identify and filter out false positives, helping security teams focus on the most serious threats. This can help customers reduce the time and resources spent on investigating false positives and enable them to respond more effectively to real threats.

6. What is the total cost of implementing and maintaining an XDR solution, and what is the expected return on investment?

The cost of implementing and maintaining an XDR solution will vary depending on factors such as the size and complexity of a customer's security infrastructure, the number and types of security technologies and data sources integrated with XDR, and the level of support and services required from the XDR vendor.

In general, XDR solutions can be more expensive than traditional security solutions due to their advanced technologies and capabilities. However, customers can expect a return on investment from XDR through improved threat detection and response, reduced losses from security incidents, and increased compliance with industry regulations and standards.

With SentinelOne, you can calculate your expected value from implementing XDR. This is done by answering a few questions: how many analysts do you directly employ? How many security incidents per year does your customer respond to? What is your mean time to investigate and remediate an incident? How many user endpoints, physical servers and virtual servers does your customer manage, and more.

Find the calculator here:



7. How does XDR support compliance with industry regulations and standards?

By combining multiple security technologies and data sources, XDR can provide customers with the visibility and control needed to meet various regulations and standards requirements. XDR can also provide customers with real-time visibility and incident response capabilities to quickly and effectively respond to security incidents and prevent data breaches. This can help customers avoid the financial and reputational risks associated with non-compliance with industry regulations and standards.

SentinelOne Singularity XDR provides customers with the comprehensive and integrated security capabilities they need to meet the requirements of various industry regulations and standards. The solution combines multiple security technologies and data sources, including endpoint protection, network security, and cloud security, to give customers real-time visibility into their security posture and the ability to detect and respond to threats more effectively.

SentinelOne XDR also includes incident response automation, data breach detection, and regulatory compliance reporting, which can help customers meet the requirements of regulations and standards such as HIPAA, PCI DSS, and GDPR.

These features and capabilities can help customers avoid the financial and reputational risks associated with non-compliance with industry regulations and standards.

8. What expertise and training are required for our staff to effectively use and manage an XDR solution?

The expertise and training required for staff to effectively use and manage an XDR solution will depend on the specific solution and the customer's security infrastructure and processes.

In general, XDR solutions are designed to be user-friendly and require minimal training for staff to use and manage. Most XDR vendors offer training and support services to help customers get up and running with their XDR solution and ensure that their staff is properly trained and equipped to use the solution effectively.

Many XDR solutions include features such as threat intelligence feeds, automated incident response, and intuitive user interfaces, which can help reduce the level of expertise and training required for staff to effectively use and manage the solution.

9. How do XDR support collaboration and information sharing between different teams and departments in our customer?

XDR can support collaboration and information sharing between different teams and departments in a customer by providing a centralized platform for managing and sharing security information.

XDR solutions typically include security dashboards, reporting, and alerting, which can provide different teams and departments with the information they need to collaborate and respond to security threats and incidents more effectively.

Additionally, XDR solutions can be integrated with other security and IT systems, such as SIEMs and ticketing systems, to enable seamless information sharing and collaboration across different teams and departments. This can help customers improve their overall security posture and reduce the impact of security incidents.

10. Are there any potential drawbacks or limitations to implementing XDR, and how do we mitigate these risks?

There are potential drawbacks and limitations to implementing XDR, including the cost and complexity of the solution, the level of expertise and training required for staff to use the solution effectively, and potential integration challenges with existing security technologies and processes.

To mitigate these risks, customers should work with their MSSP to carefully evaluate their security needs and requirements and choose an XDR solution that suits their specific needs and infrastructure. Customers should also ensure their MSSP has the expertise and resources necessary to effectively implement and manage an XDR solution and plan for any potential integration challenges; and ensure they have access to the training and support services needed to effectively use and manage the solution.

Conclusion

As an MSSP, it's important to stay up-to-date on the latest security technologies that can help protect your customer from cyber threats. XDR provides a more comprehensive and integrated approach to security by combining multiple technologies and data sources to detect and respond to threats more effectively.

If you're considering implementing XDR for your customer, be sure to ask about the potential benefits and drawbacks. By combining endpoint, network, and application telemetry, XDR can provide security analytics to win that race through enhanced detection, triage, and response. If you'd like to know more about SentinelOne's Singularity Platform, contact us or request a demo.

Learn More About SentinelOne's Singularity XDR and Cyber Security

- [The Dangers of Social Engineering | How to Protect Your Customer](#)
- [Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results](#)
- [Building Blocks For Your XDR Journey, Part 4 | The Value of Security Data](#)

Tomorrow's Threats Require a New Enterprise Security Paradigm

SentinelOne provides one platform to prevent, detect, respond, and hunt ransomware across all enterprise assets. See what has never been seen before. Control the unknown. All at machine speed.



Autonomous EPP + EDR

Real-time detection and remediation of modern attacks at the endpoint, at machine speed, and without human intervention.



Unprecedented Visibility

Contextualize and identify threats in real-time. Storyline™ technology reduces manual effort and automatically strings together related events in an attack storyline.



Frictionless Threat Resolution

Patented Storyline™ enables 1-click remediation and rollback to accelerate recovery to real-time. Storyline Active Response or STAR™ provides proactive detection and response. For threat hunters and responders, remediation is integrated as a standard EDR response.



Simplified Experience

One agent consolidates security functions and reduces agent count. One console unifies administration of devices and cloud workloads. Fast to deploy. Easy to manage.



Exceptional Customer Experiences

Customers are our #1. The proof is in our high customer satisfaction ratings and net promoter scores that rival the globe's best companies.



SentinelOne Vigilance

Get answers, not alerts, with our managed detection, investigation and response service.

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

Get a Free Demo

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

**MITRE
GENUINITY**

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

**Gartner
peerinsights™**
4.9 ★★★★★

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne



TEVORA
PCI DSS Attestation
HIPAA Attestation

Contact us

sales@sentinelone.com

+1-855-868-3733

About SentinelOne

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

Are you ready?

sentinelone.com