How to Discuss MDR with your Customer



Discovery Questions

1. **Are you able to monitor security across your IT systems and users 24x7? When an incident occurs, who is responsible to fix it?**
2. **What's the risk if your data and infrastructure become unavailable?**
3. **Can you detect security events across the entire IT stack, including cloud, identity, and users? How do you monitor and respond to security incidents?**
4. **How long does it take to respond to a security incident like ransomware?**
5. **What does your security investment look like today?**
6. **Do you have cybersecurity audits, compliance requirements or industry standards you need to meet?**
7. **What cybersecurity challenges are you experiencing? What do you need to achieve in the next 12-24 months?**

Objections

- **Cybersecurity Solutions are expensive and difficult to manage.**
  Comcast Business MDR offers an affordable and scalable solution with tiered pricing based on the number of monitored endpoints, not on data volume or storage, which helps businesses manage costs.

  All of our MDR packages include 24x7 cybersecurity monitoring, investigation, and threat response provided by the Comcast Business Security Operations Center (SOC) so you don't have to invest in or manage your own in-house program.

  Our service takes the complexity out of cybersecurity. You can depend on us for a fully managed MDR service, but also get co-managed access whenever you need it.

- **We already have in-house IT security.**
  Excellent! Having an in-house IT security team is invaluable. However, MDR complements your existing team by providing a layer of expertise and continuous monitoring that can be hard to maintain in-house.

  Our MDR service acts like a force multiplier for your own security team, offering specialized skills in threat detection and response around the clock. This is crucial because cyber threats evolve rapidly and can occur at any time, often outside of regular business hours.

Objections (cont.)

- **We've never experienced a significant cyberattack. I don't see the need for MDR services.**
  It's great to hear that you've been safe from significant attacks, but the threat landscape is constantly evolving, and past performance is not indicative of future safety.

  Cyber threats are becoming more sophisticated and can affect any business, often with devastating consequences. In fact, 9 out of 10 enterprises have security risks they don't already know about.

  Our MDR service not only helps to detect and respond to attacks but also works proactively to prevent potential threats from becoming actual breaches. It's about ensuring readiness and resilience, minimizing risk, and protecting your business's reputation and continuity before an incident occurs.

- **We already have endpoint security. Why do I need MDR?**
  I'm glad you do. Most companies are using some sort of EPP/EDR capability.

  But endpoint protection isn't enough: today's threats happen across the full IT stack, including applications and databases, email and endpoints, cloud and server infrastructure, identity, users, and the network.

  Traditional endpoint protection and EDR only protects your endpoints and servers, while Comcast Business MDR provides full-spectrum threat monitoring and detection across your entire IT environment.

- **We already have EDR from Comcast Business.**
  Comcast Business MDR is designed to work in tandem with our EDR solution to provide a layered defense-in-depth approach against cyber threats. Our EDR and MDR solutions are integrated to work better together.

  EDR focuses on detecting and eliminating threats on individual endpoints, while MDR provides a broader view across applications and databases, email and endpoints, cloud and server infrastructure, identity, users, and the network.

  Implementing both of our solutions together offers real-time protection, helping reduce the potential damage caused by a breach.

- **What's the difference between Comcast Business MDR and Rapid7?**
  Our solution combines Rapid7's security analytics platform with the Comcast Business Security Operations Center (SOC) and our own threat intelligence to deliver best-in-class MDR services.

  Unlike Rapid7, Comcast Business MDR includes custom detection rules, custom automation, and managed user behavior analytics (UBA). With Rapid7, customers are wholly responsible for managing their own user security alerts.

  Rapid7 provides a gold-plated service. With Comcast Business MDR, tiered pricing means you purchase only what you need.

- **I can purchase MDR from a generic Managed Security Service Provider (MSSP).**
  Many MSPs and MSSPs employ IT generalists. The Comcast Business SOC is staffed with cybersecurity specialists who are deeply focused on and skilled in threat detection & response.

  The analogy I like to give is that our MDR service is staffed with fighter pilots while generic service providers are often staffed with commercial pilots. When you're facing a cyber threat, it's best to have the experts on your team, otherwise something is more likely to turn into a security incident.

  In that case, any savings you'd have from using a lower cost MDR service will be lost.

©2024 Comcast. CB-How-to-Discuss-MDR-with-your-Customer-One-Sheet_7.24