What is XDR?

XDR is not a single product. A true XDR platform should include both front-end solutions (countermeasures like endpoint, DLP, etc.) and back-end solutions (intelligence & orchestration capabilities that allow customers the ability to automate low-level threats to focus on what’s most important).

A SaaS-based, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations systems.”
— Gartner

Challenges in Security Operations addressed by XDR

<table>
<thead>
<tr>
<th>Average number of security tools</th>
<th>Number of security alerts daily</th>
<th>Time required to triage a single alert</th>
<th>Average time it takes to discover a breach</th>
<th>Average time it takes to respond to a breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>70</td>
<td>10K</td>
<td>30min</td>
<td>75days</td>
<td>30days</td>
</tr>
</tbody>
</table>

Buying Audience

<table>
<thead>
<tr>
<th>Security Operations</th>
<th>Security Administrations</th>
<th>Chief Security Officers</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Director/Analyst Architect/Engineer)</td>
<td>(IT Director/Security Engineer /Analyst)</td>
<td>(Other Titles: CISO, VP/Director of Security)</td>
</tr>
</tbody>
</table>

Top XDR Discovery Questions and Conversation-Starters:

Tell me about your plans to implement an XDR architecture.
- Follow up with, "What does XDR mean to you?"

Tell me about your security team processes:
- How are threats prioritized?
- If a new threat emerges, will your team know whether your cybersecurity defenses are prepared to safeguard against the threat?
- How does your SOC team investigate threats?
- What is your mean time to detect/respond to a threat?
- Does your security architecture help retain your security talent?

What part of an XDR architecture is currently most important for you?
- Follow up with, "Is that XDR element working well in your environment today?"

Do your security technologies integrate well enough to quickly enable a threat response?
- Does the integration drive better security outcomes for your organization?
- Where do you look to investigate a threat?
- Do you pivot to multiple technologies to understand a threat?
- Do you have too many alerts to investigate?
- How are your alerts prioritized?
Who is Trellix?

FireEye and McAfee Enterprise merged to form Trellix: A fresh cybersecurity firm determined to redefine the future of cybersecurity with a mature XDR platform.

Trellix XDR Solution

Open and Native XDR platform • Over 650 Integrations
Cloud Native • Built to be an XDR platform • Advanced Threat Intel
Machine Learning Native • Automation and Orchestration

A Living security solution.

Learning & Adapting

Our living XDR ecosystem harnesses the power of AI/ML to adaptively strengthen detection, plus responds in real time to active threats, so your business continues as usual.

Native & Open

Our flexible, scalable platform with open APIs integrates seamlessly with your existing technologies, to deliver maximum visibility, control, and vendor choice.

Expert & Embedded

Our experts monitor and research threats and campaign activities, producing insightful and actionable threat intelligence on threat actors and their behavior.

Questions about Trellix? Email your Trellix Channel Partner Relationship Manager

Learn More about Trellix!

- www.trellix.com
- Video Brief: Introducing Trellix
- Blog: Is XDR for You?
- Trellix Insights: Step Ahead of Your Adversaries with Proactive Security
- Solution Brief: Trellix XDR

Visit Trellix.com to learn more.