RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART1-W08**

Open XDR: A Strategy for Evolving Security Needs

Rakesh Shah

Senior Director Product Management and Development
AT&T Business
@ATTcyber

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

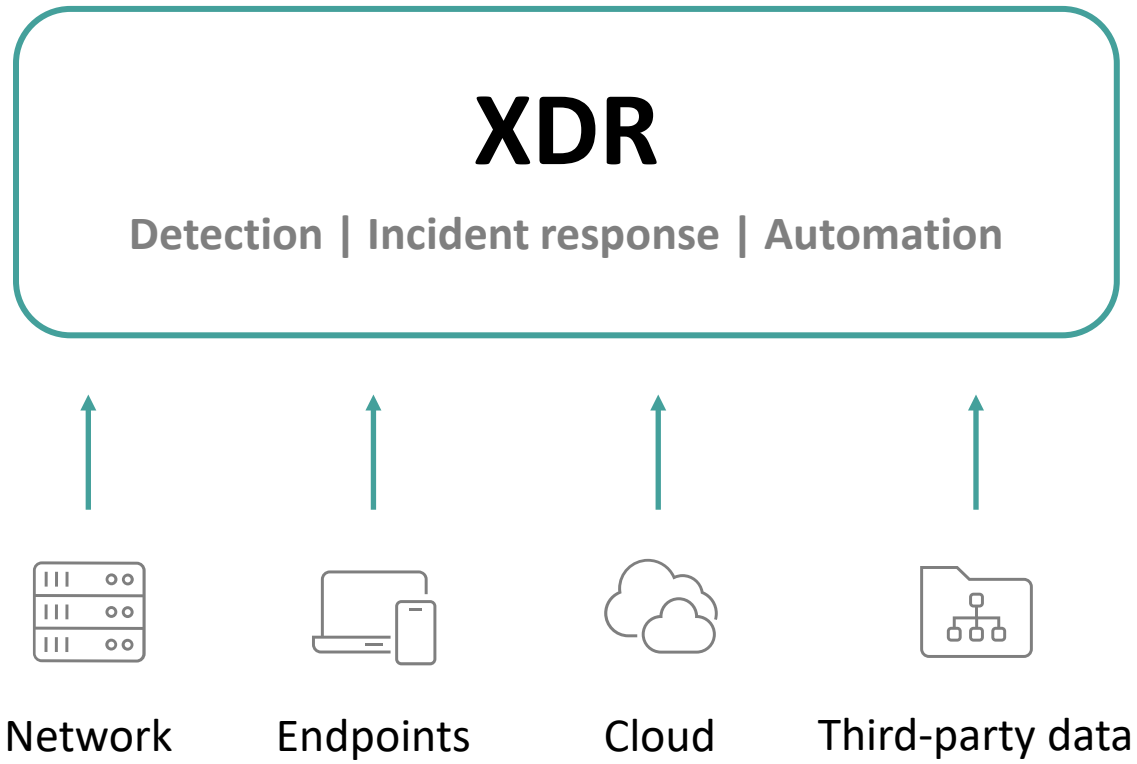
Agenda

- What is XDR?
- What is driving the need for XDR?
- Why XDR, and why now?
- The road to XDR
- The benefits of open XDR
- Stronger, smarter integrations
- Open XDR in action

What is XDR?

Whatever you want it to be . . .

So, what is XDR?



XDR is a **new approach** to detection and response.

What is driving the need for XDR?

Security teams are drowning from defense in depth

Disparate security point products

Overwhelming number of alerts

Difficulty in conducting investigations

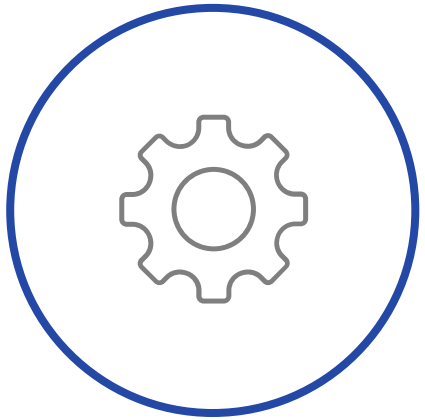
How an XDR solution can help reduce risks

Business

Increase efficiency with scalable, flexible, and **existing solutions**

Technology

Deep integrations with **best-of-breed** security vendors to identify threats



Operations

Investigate threats more effectively with **current tools**

Why XDR, and why now?

Increase efficiency in security operations and help improve time to detect, respond, and recover

Expand telemetry	Boost threat intelligence; improve security analytics	Automate and orchestrate select workflows and process
Increase visibility and information gathering	Increase detection accuracy and time to detection	Improve response and recovery

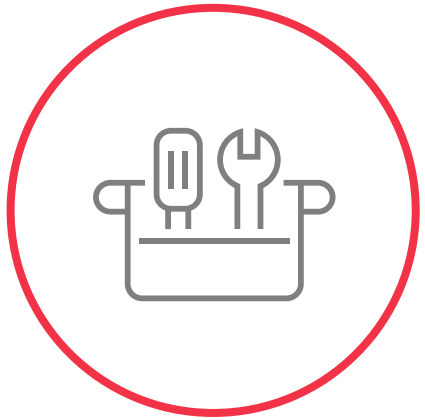
The road to XDR

Use cases

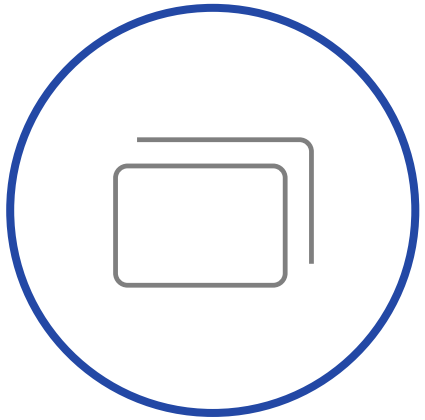
1. Prevent malware and ransomware on your endpoint
2. Detect and respond to attackers in your network
3. Unified view into your security posture
4. Augment your security team
5. Embrace digital transformation

The benefits of open XDR

Automated threat detection and incident response



No need to rip and replace



Single pane of glass

Stronger, smarter integrations

While businesses are looking for the easy button with XDR, it can be challenging to go all-in with a single security platform

- Integrating best-in-breed partners will leverage existing investments
- API integrations extend and adapt to your cyber defenses

The need for deep integrations

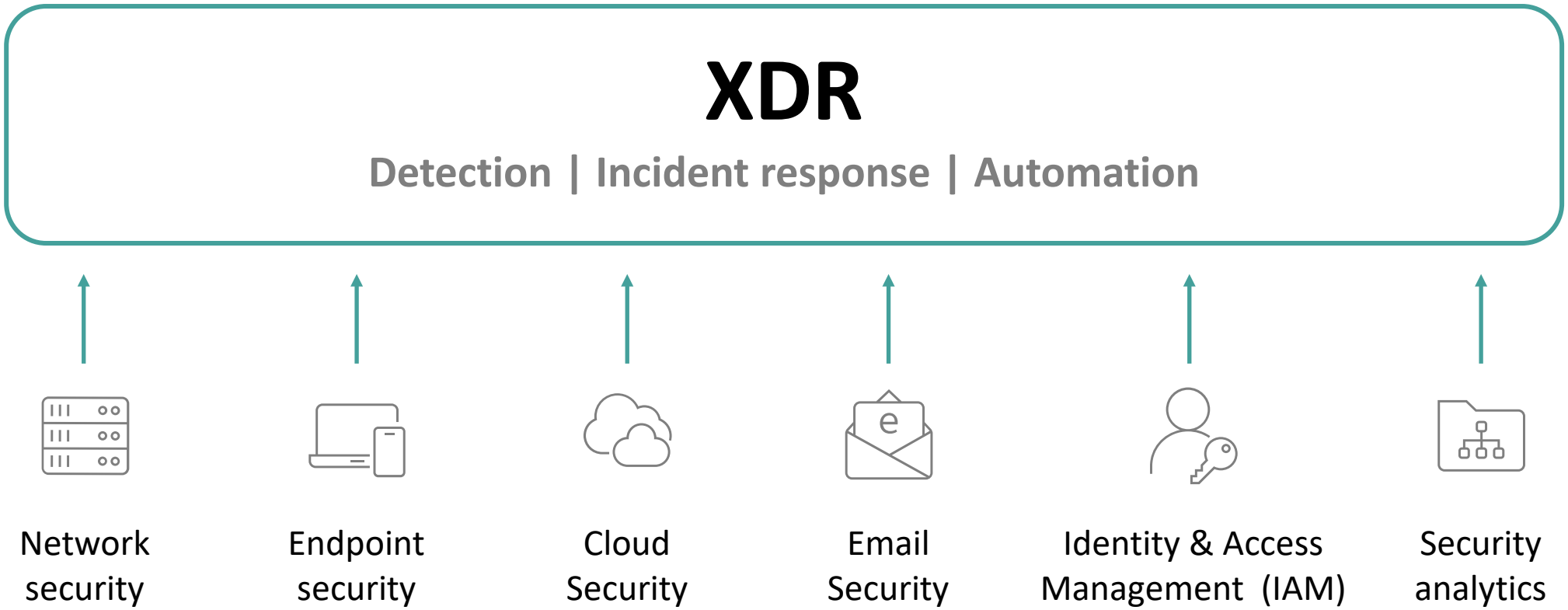
Basic integrations

- Translate raw log data into normalized events for analysis

Deep integrations

- Translate raw log data into normalized events for analysis
- Collect and enrich log data
- Perform threat analysis
- Coordinate response actions
- Provide security orchestration
- Access to built-in dashboards

Key integrations by category



RSAConference2022

Open XDR in Action

Scenario 1:

Leverage multiple integrations for more actionable context

Scenario 2:

Gain visibility across your environment

Scenario 3:

Faster time
to respond

Importance of Managed Services

- Bringing together technology, infrastructure, and expertise
- Helping to implement complex solutions
- Incident response planning

Planning for your XDR Strategy

- What outcomes are you driving for?
- What does your current security stack look like?
- Does the vendor's roadmap align to your strategy?
- Will you need help deploying the solution?

RSAConference2022

Thank you!

@ATTcyber

AT&T Cybersecurity