

# **RSA**Conference2022

San Francisco & Digital | June 6 – 9

SESSION ID: **PART1-W08**

## **Open XDR: A Strategy for Evolving Security Needs**

**Rakesh Shah**

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

***TRANSFORM***



# 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.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

© 2022 AT&T Intellectual Property. AT&T and globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners

# 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

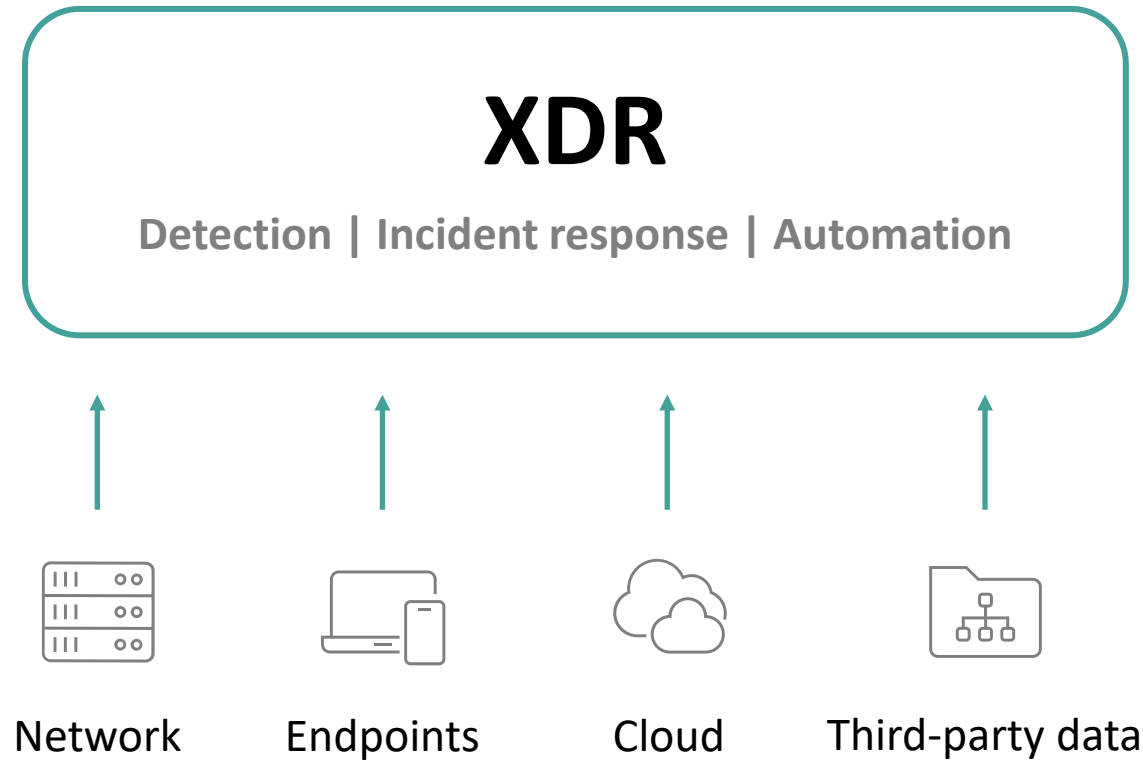
# What is XDR?

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



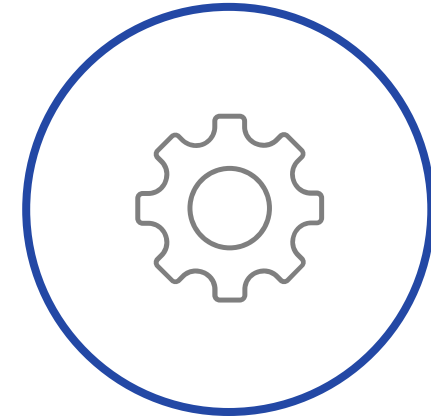
## Business

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



Increase visibility  
and information gathering

Boost threat intelligence;  
improve security analytics



Increase detection accuracy  
and time to detection

Automate and orchestrate  
select workflows and process



Improve response and  
recovery



# The road to XDR



**EDR**

Endpoint Detection  
and Response



**NDR**

Network Detection  
and Response



**XDR**

Extended  
Detection  
and Response



**MDR**

Managed  
Detection  
and Response



**MXDR**

Managed Extended  
Detection and Response

# 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**

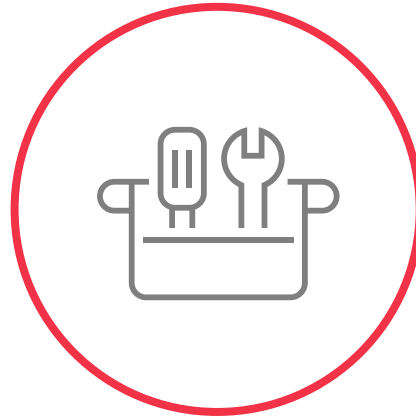
5

**Embrace digital  
transformation**

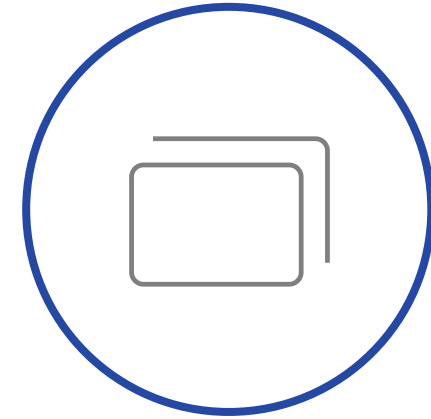
# The benefits of open XDR



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

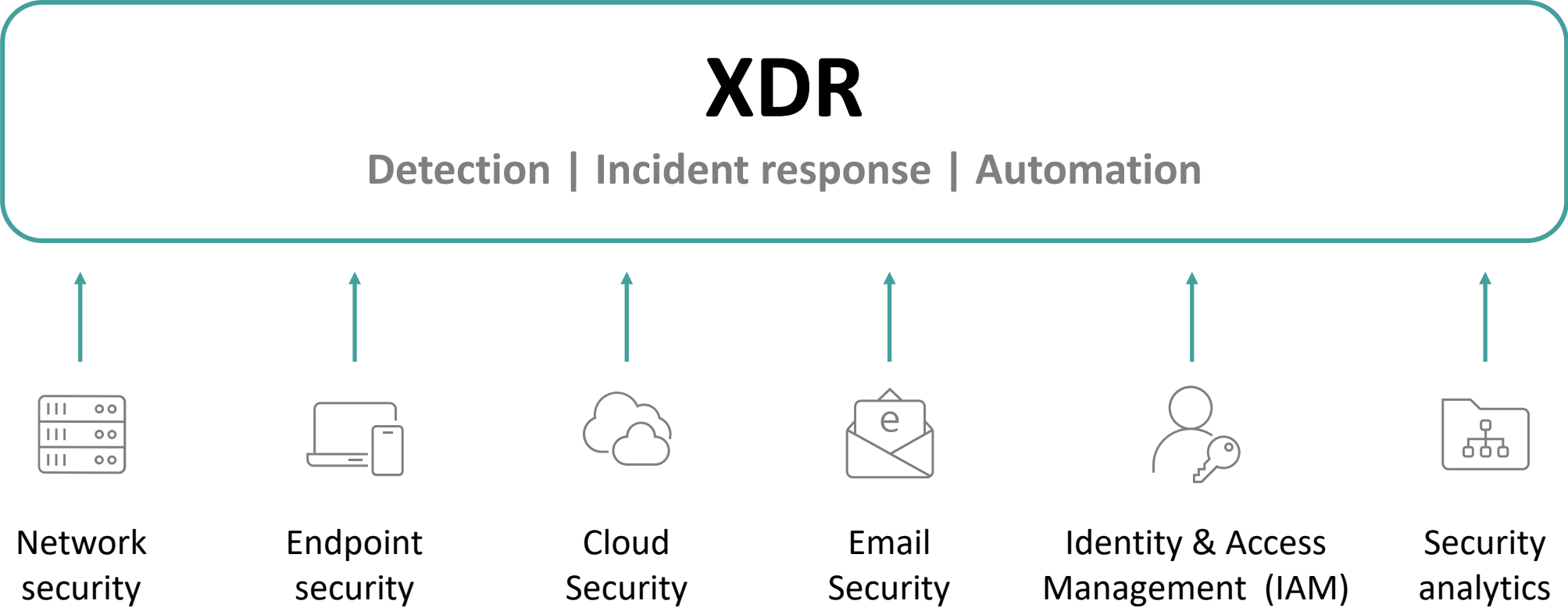
- Translate raw log data into normalized events for analysis

## 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



**RSA**®Conference2022

# Open XDR in Action





A woman with short dark hair, wearing glasses and a headset, is focused on her work in a modern office or call center. She is seated at a desk with multiple computer monitors. The primary monitor displays a teal background with white line graphs, while the secondary monitor shows a list of data or code. In the background, other employees are visible at their desks, working in a bright, open-plan environment with large windows.

## Scenario 1:

Leverage multiple integrations for more actionable context





Critical Traps

17:51:11 12:43 No matching CFIMs are currently being received.  
17:51:11 12:48 No matching CFIMs are currently being received.  
17:51:11 12:53 No matching CFIMs are currently being received.  
17:51:11 12:58 No matching CFIMs are currently being received.  
17:51:11 13:03 No matching CFIMs are currently being received.  
17:51:11 13:08 No matching CFIMs are currently being received.  
17:51:11 13:13 No matching CFIMs are currently being received.  
17:51:11 13:18 No matching CFIMs are currently being received.  
17:51:11 13:23 No matching CFIMs are currently being received.  
17:51:11 13:28 No matching CFIMs are currently being received.  
17:51:11 13:33 No matching CFIMs are currently being received.  
17:51:11 13:38 No matching CFIMs are currently being received.  
17:51:11 13:43 No matching CFIMs are currently being received.  
17:51:11 13:48 No matching CFIMs are currently being received.  
17:51:11 13:53 No matching CFIMs are currently being received.  
17:51:11 13:58 No matching CFIMs are currently being received.

INTERNATIONAL									
NE	TY	CCD	FDC	TC	COUNT	DOM	AC		
NYCMNYBW55T	RE	441	1860	MSC	80	192	2		
DVNSBMCW01	DE	441	2203	MSC	224	192	2		
ATLNGATL01T	RE	52	2098	QPE	200	-	84		
SNDGCA0787T	RE	52	2098	QPE	168	-	23		
MNTRXLVND08	DE	52	2203	MSC	168	-	23		
WHPLNY0203T	DE	52	2098	QPE	152	86	3		
AMSTNLQWE01	DE	31	2203	MSC	152	85	23		
SNANTXCA02T	RE	52	2098	QPE	120	86	35		
PITBPADG09T	RE	52	2098	QPE	88	-	14		
ALBQNMMA02T	DE	52	2098	QPE	88	86	6		
SHOKCA0296T	DE	86	1992	EBF	80	81	1		
SCRMCA0404T	DE	52	2098	QPE	64	86	4		
NYCMNYBW55T	DE	52	2098	QPE	64	86	3		
NYCMNYBW55T	DE	441	1980	ADF	56	-	1		

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?



# **RSA**Conference2022

# Thank you!

**@ATTcyber**

**AT&T Cybersecurity**

