CSA GCR cloud security alliance GREATER CHINA REGION ® | 亚信安全

CSA研讨会

XDR的无限可能

数字时代

数据驱动安全
——从分析到检测与响应

刘志诚

CONTENTS

01 XDR诞生的原因

02 XDR群雄逐鹿

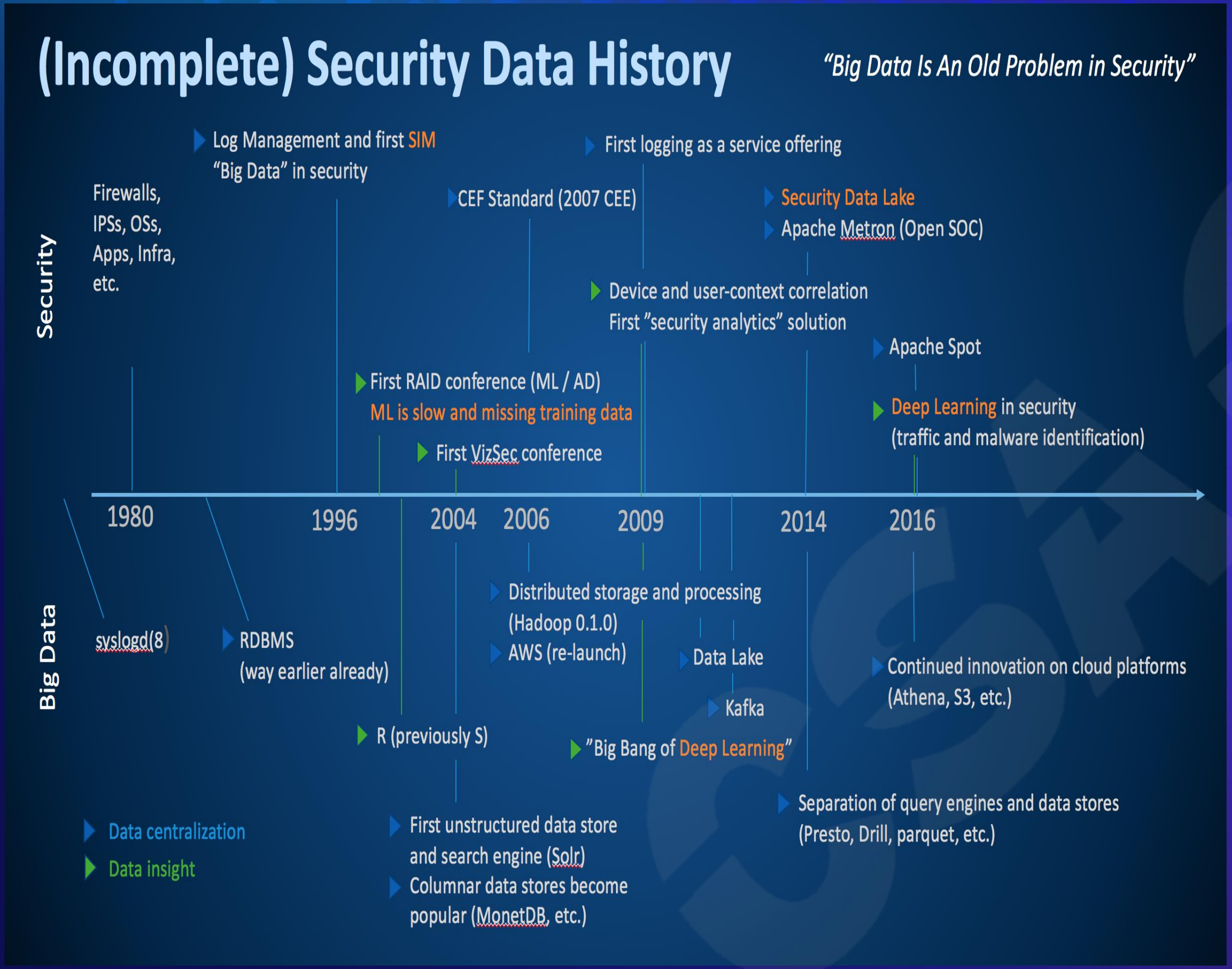
03 XDR需要克服的困难

04 XDR适逢其时

05 XDR的未来

/01 XDR诞生的原因

数据驱动安全发展历程



(Incomplete) Security Data History

"Big Data Is An Old Problem in Security"

Security:

- Firewalls, IPSs, OSs, Apps, Infra, etc.
- Log Management and first SIM "Big Data" in security
- CEF Standard (2007 CEE)
- First logging as a service offering
- Security Data Lake
- Apache Metron (Open SOC)
- Device and user-context correlation First "security analytics" solution
- Apache Spot
- First RAID conference (ML / AD) ML is slow and missing training data
- First VizSec conference
- Deep Learning in security (traffic and malware identification)

Big Data:

- syslogd(8)
- RDBMS (way earlier already)
- Distributed storage and processing (Hadoop 0.1.0)
- AWS (re-launch)
- Data Lake
- Kafka
- Continued innovation on cloud platforms (Athena, S3, etc.)
- R (previously S)
- "Big Bang of Deep Learning"
- Separation of query engines and data stores (Presto, Drill, parquet, etc.)
- First unstructured data store and search engine (Solr)
- Columnar data stores become popular (MonetDB, etc.)

- Data centralization
- Data insight

■ 数据作为安全能力的核心生产力，至关重要

■ 单数据源的静态数据，日志是第一代安全产品的基础

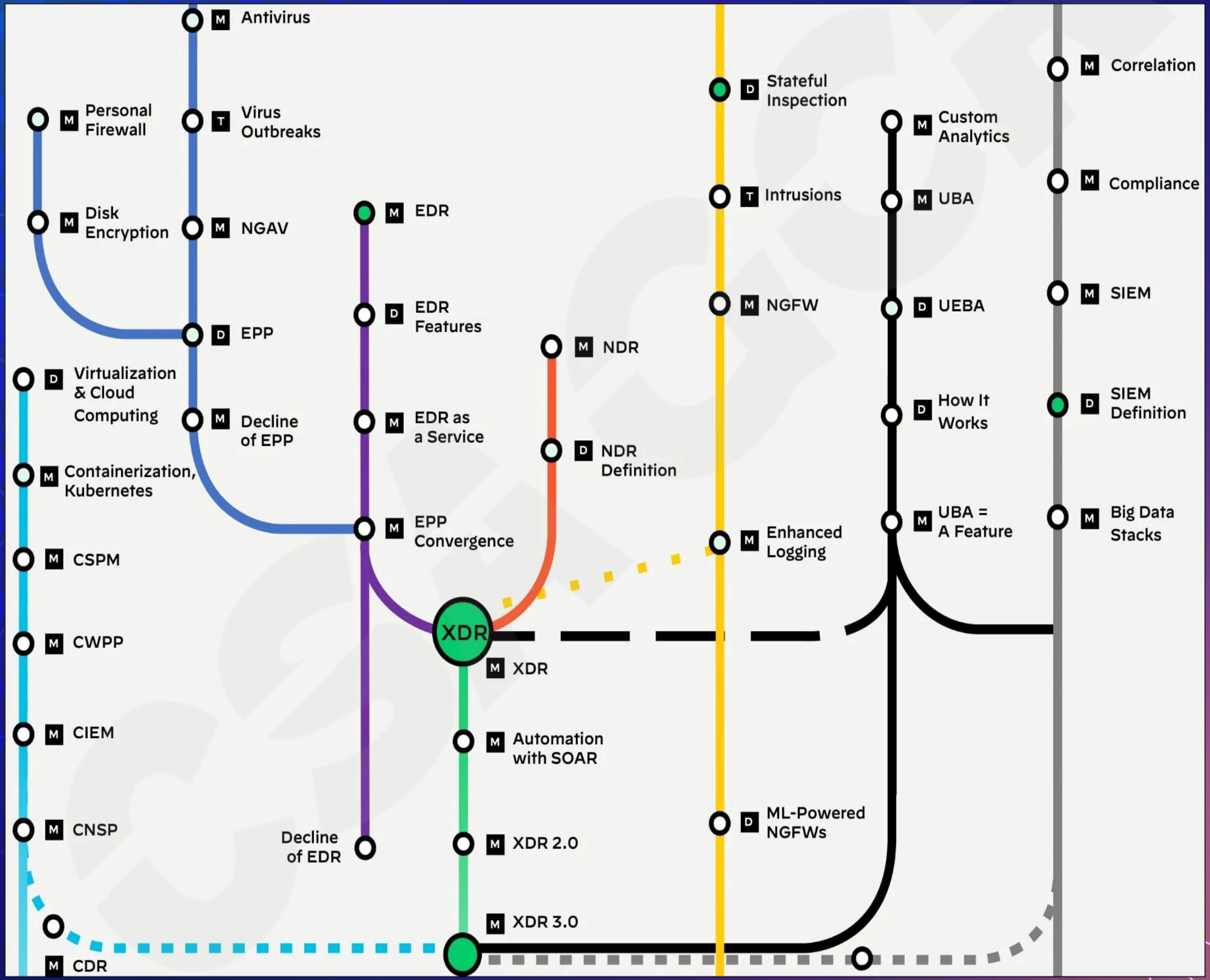
■ 多数据源的静态数据结合人工处置分析形成第一代安全运营平台SOC

■ 网络流量作为动态数据形成态势感知类产品

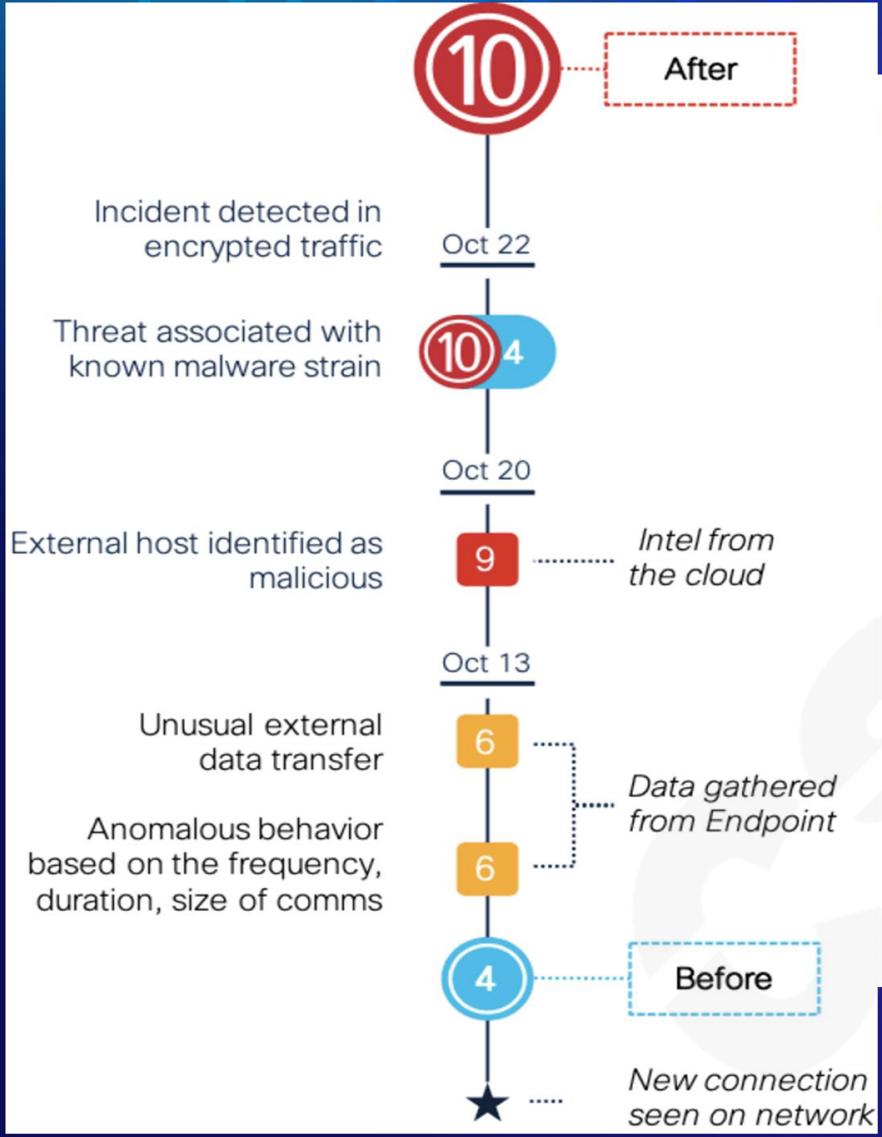
■ 整合多源静态、动态数据的人工智能分析形成异步第二代安全运营平台SIEM

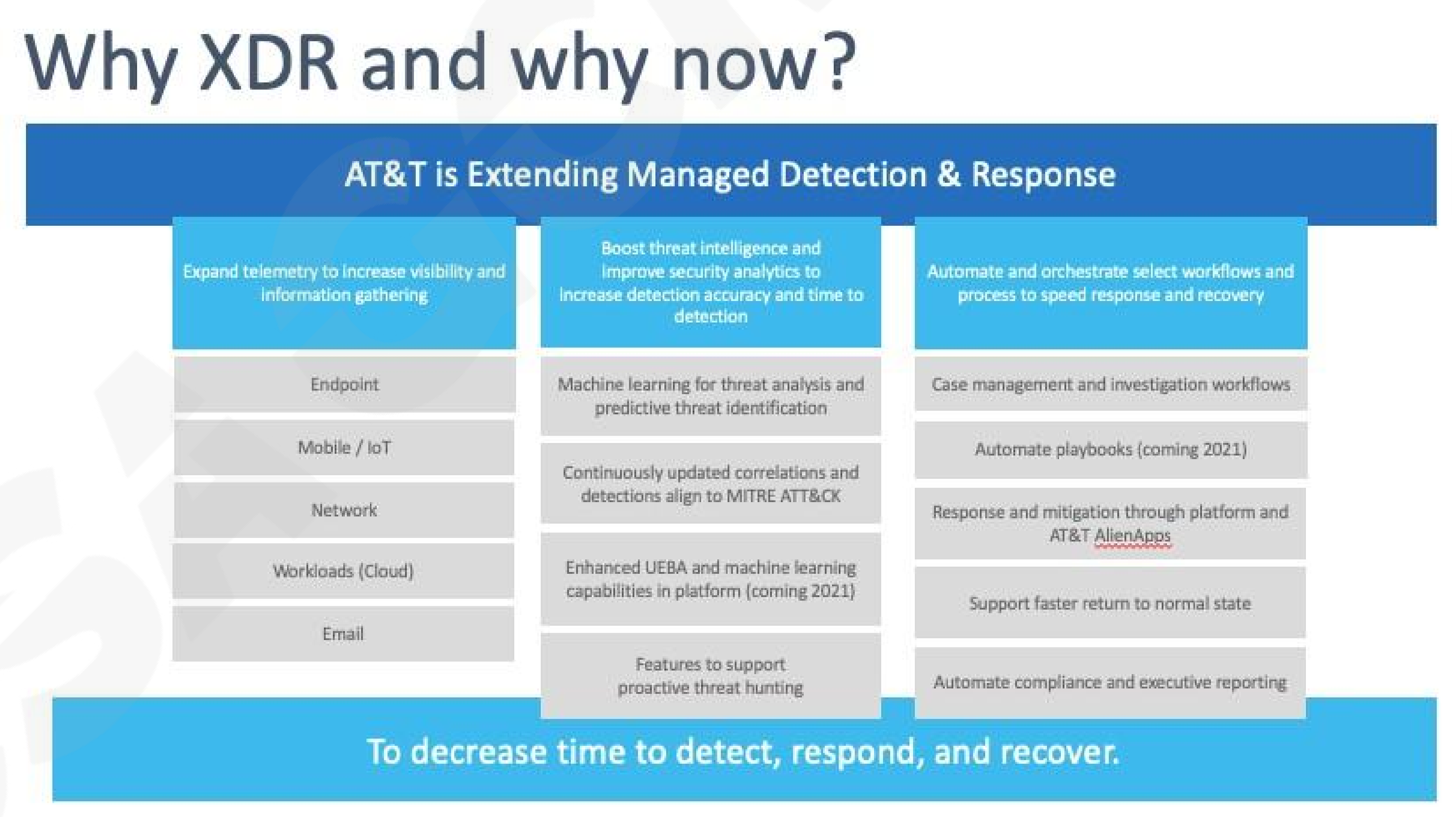
■ 多源静动态内外部数据人工智能分析的实时同步自动化编排（SOAR）与应用形成了XDR

XDR是安全产品进化的产物



XDR是数据驱动安全发展的必然


10
After
Incident detected in encrypted traffic
Oct 22
Threat associated with known malware strain
10
4
Oct 20
External host identified as malicious
9
Intel from the cloud
Oct 13
Unusual external data transfer
6
Anomalous behavior based on the frequency, duration, size of comms
6
Data gathered from Endpoint
4
Before
New connection seen on network



Why XDR and why now?

AT&T is Extending Managed Detection & Response

Expand telemetry to increase visibility and information gathering

- Endpoint
- Mobile / IoT
- Network
- Workloads (Cloud)
- Email

Boost threat intelligence and improve security analytics to increase detection accuracy and time to detection

- Machine learning for threat analysis and predictive threat identification
- Continuously updated correlations and detections align to MITRE ATT&CK
- Enhanced UEBA and machine learning capabilities in platform (coming 2021)
- Features to support proactive threat hunting

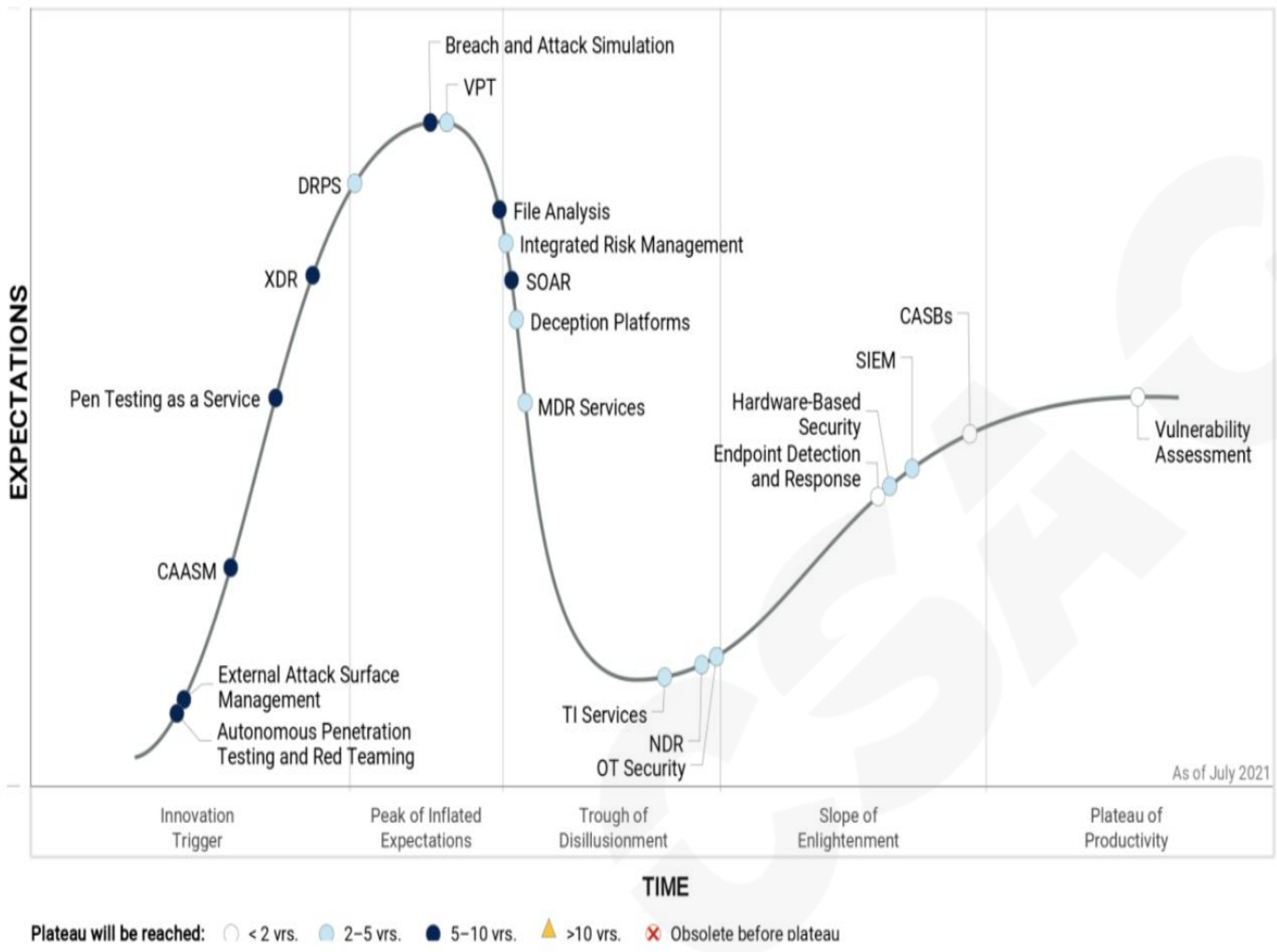
Automate and orchestrate select workflows and process to speed response and recovery

- Case management and investigation workflows
- Automate playbooks (coming 2021)
- Response and mitigation through platform and AT&T AlienApps
- Support faster return to normal state
- Automate compliance and executive reporting

To decrease time to detect, respond, and recover.

/02 XDR群雄逐鹿

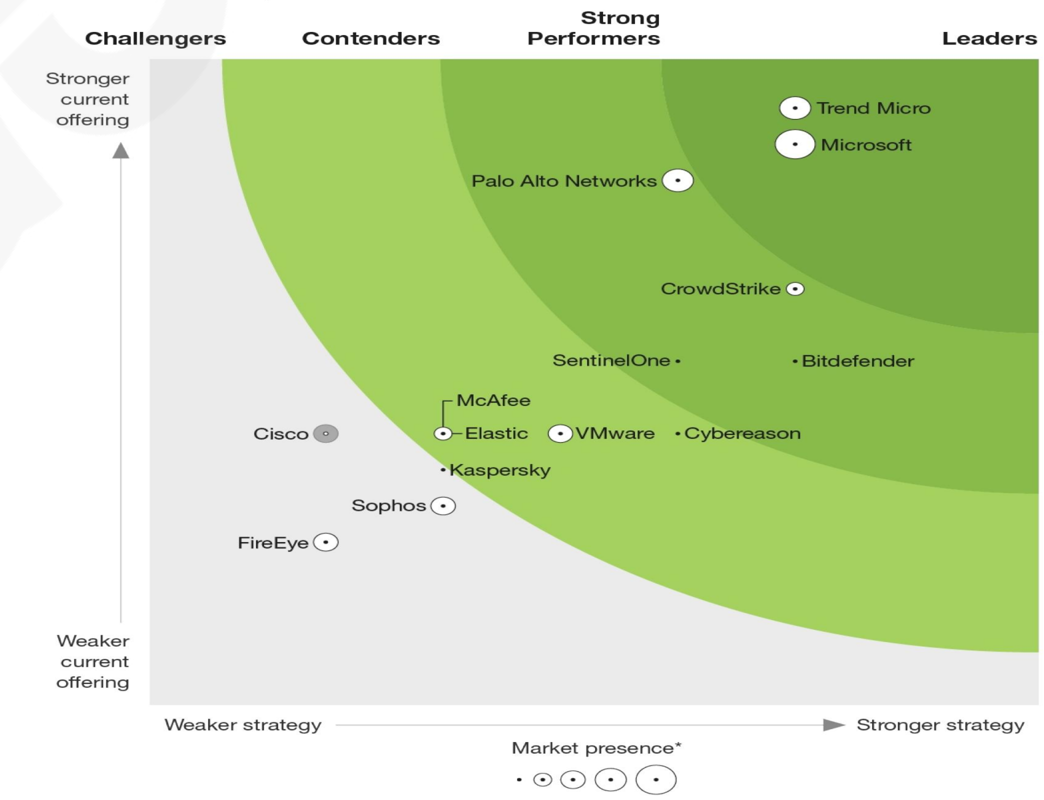
XDR成为安全的热点



THE FORRESTER NEW WAVE™

Extended Detection And Response (XDR) Providers

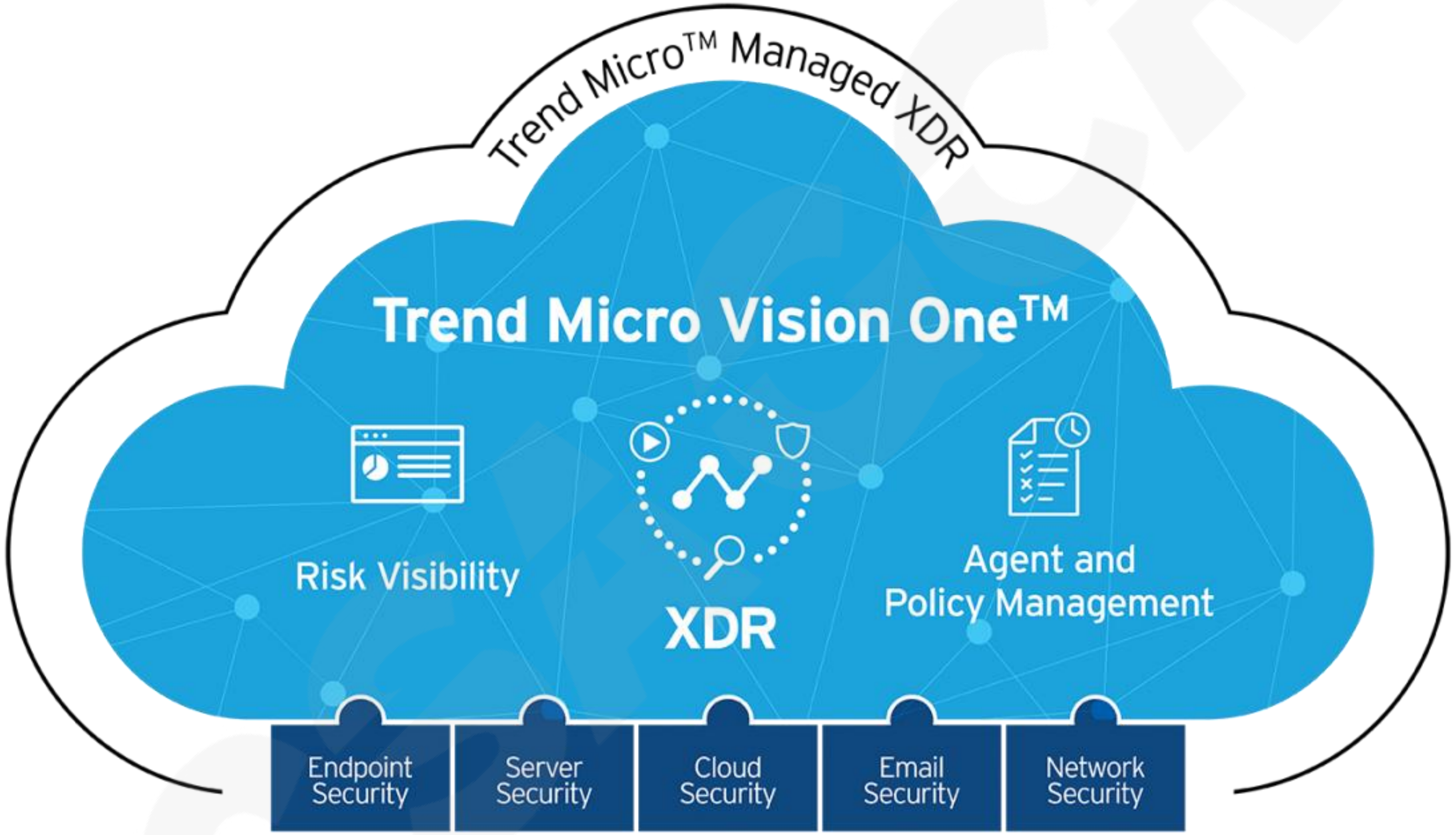
Q4 2021



*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Trend XDR


Trend Micro™ Managed XDR
Trend Micro Vision One™
Risk Visibility
XDR
Agent and Policy Management
Endpoint Security
Server Security
Cloud Security
Email Security
Network Security