



Native XDR vs. Open

What's the difference and why it matters to you

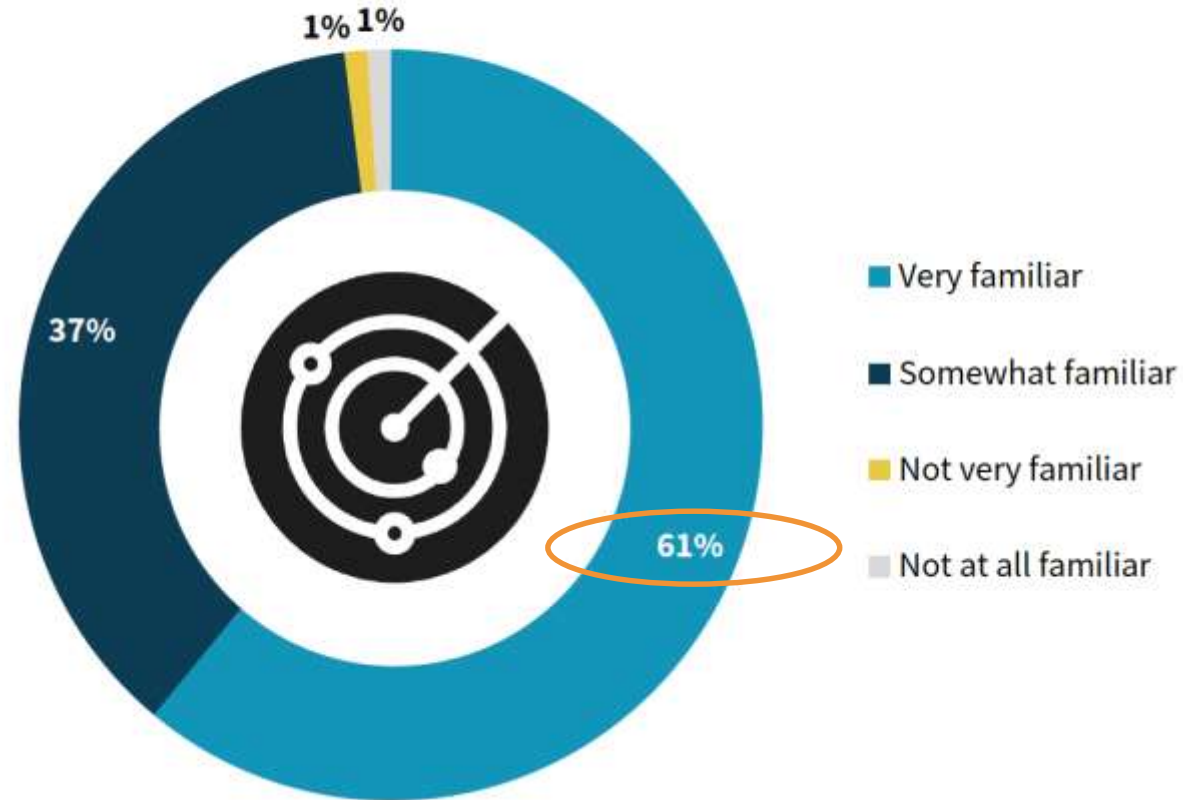
IT SA Nuremberg 2022
Stand 6-203

AGENDA

- XDR: Native vs. Open
- Why Stellar Cyber

XDR Market Awareness

Familiarity with XDR technology.



In ESG's 2020 research, only 24% of security professionals were very familiar with XDR

XDR Market Growth

50%

Of businesses are interested
in a fully managed XDR

48%

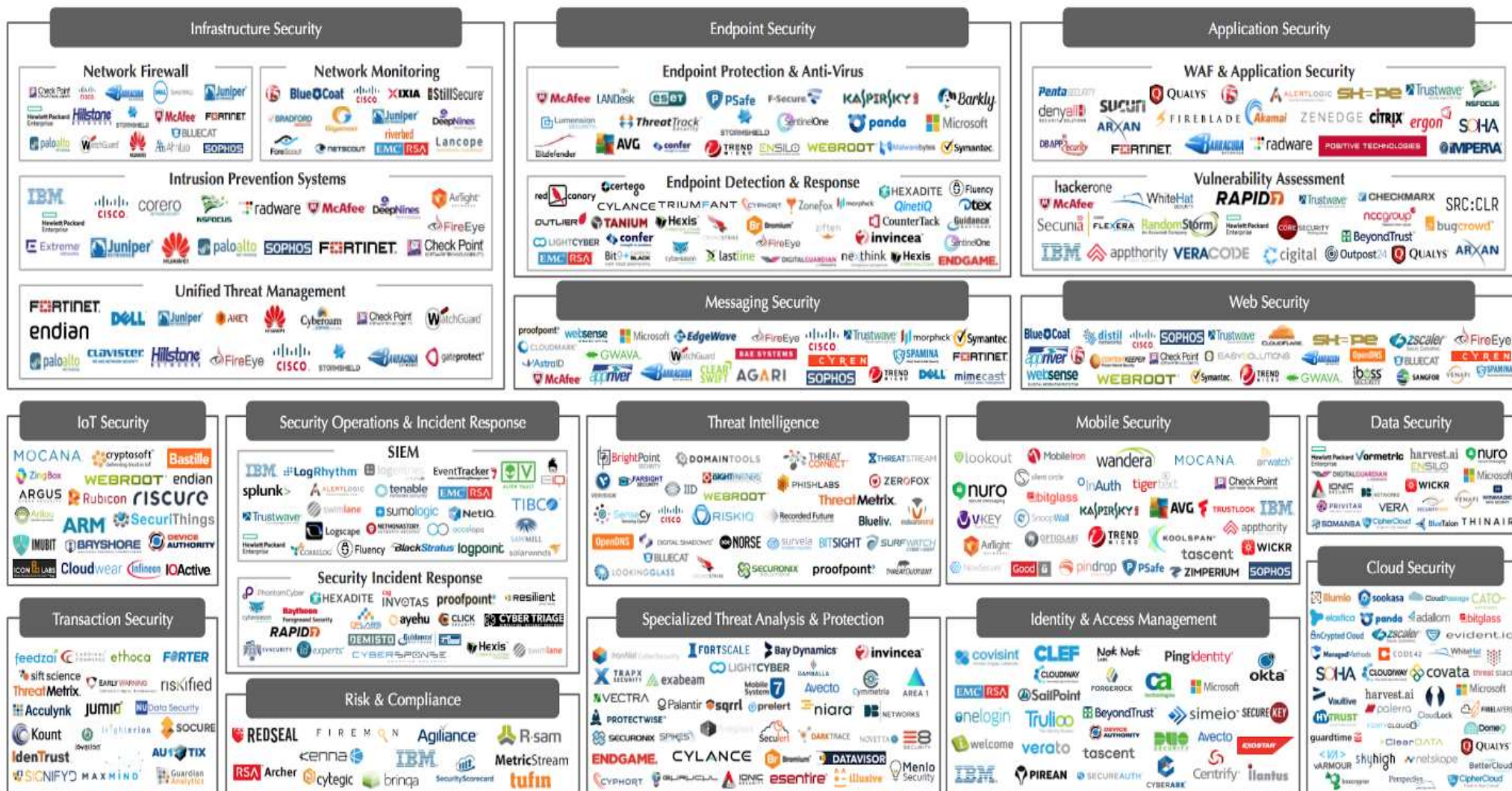
Will be replacing individual
controls with integrated XDR
solutions.

43%

Would focus on implementing XDR
solutions in support of threat detection
and response capabilities for cloud-
based workloads and SaaS applications.

Impact of XDR on the Modern SOC, ESG Research, Nov 2020

Why Your Organization Needs Open XDR / XDR



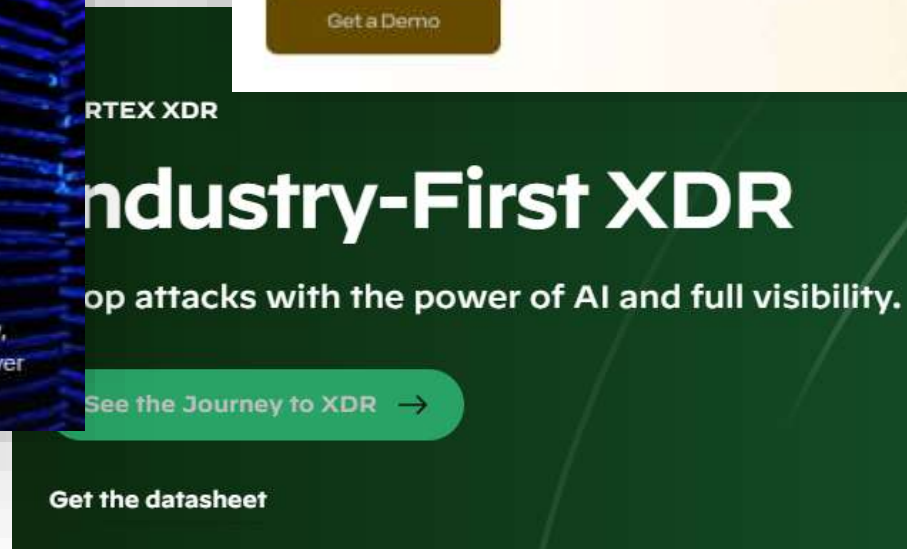
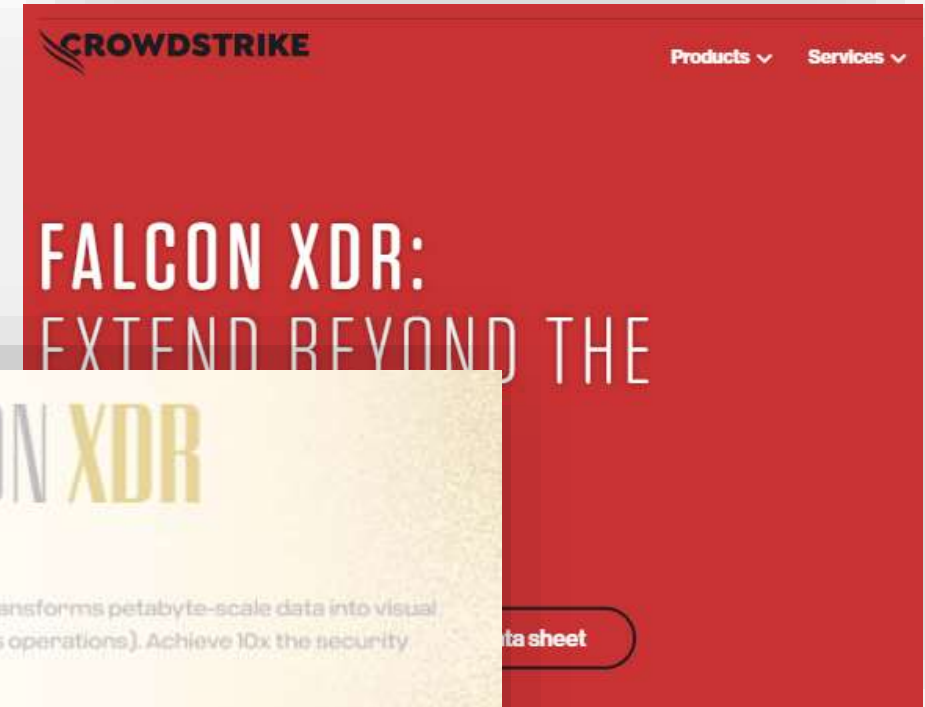
Source: Momentum Partners.



XDR: Native vs. Open

Security Vendors Jumping In

- Native XDR plays
- Customer acquisition focused
- Driving vendor adoption



XDR – Extended Detection & Response

Gartner's No. 1 Security & Risk Trend for 2020

"XDR solutions are emerging that automatically collect and correlate data from multiple security products."

"The primary goals of an XDR solution are to increase detection accuracy and improve security operations efficiency and productivity."

Gartner®

FORRESTER®

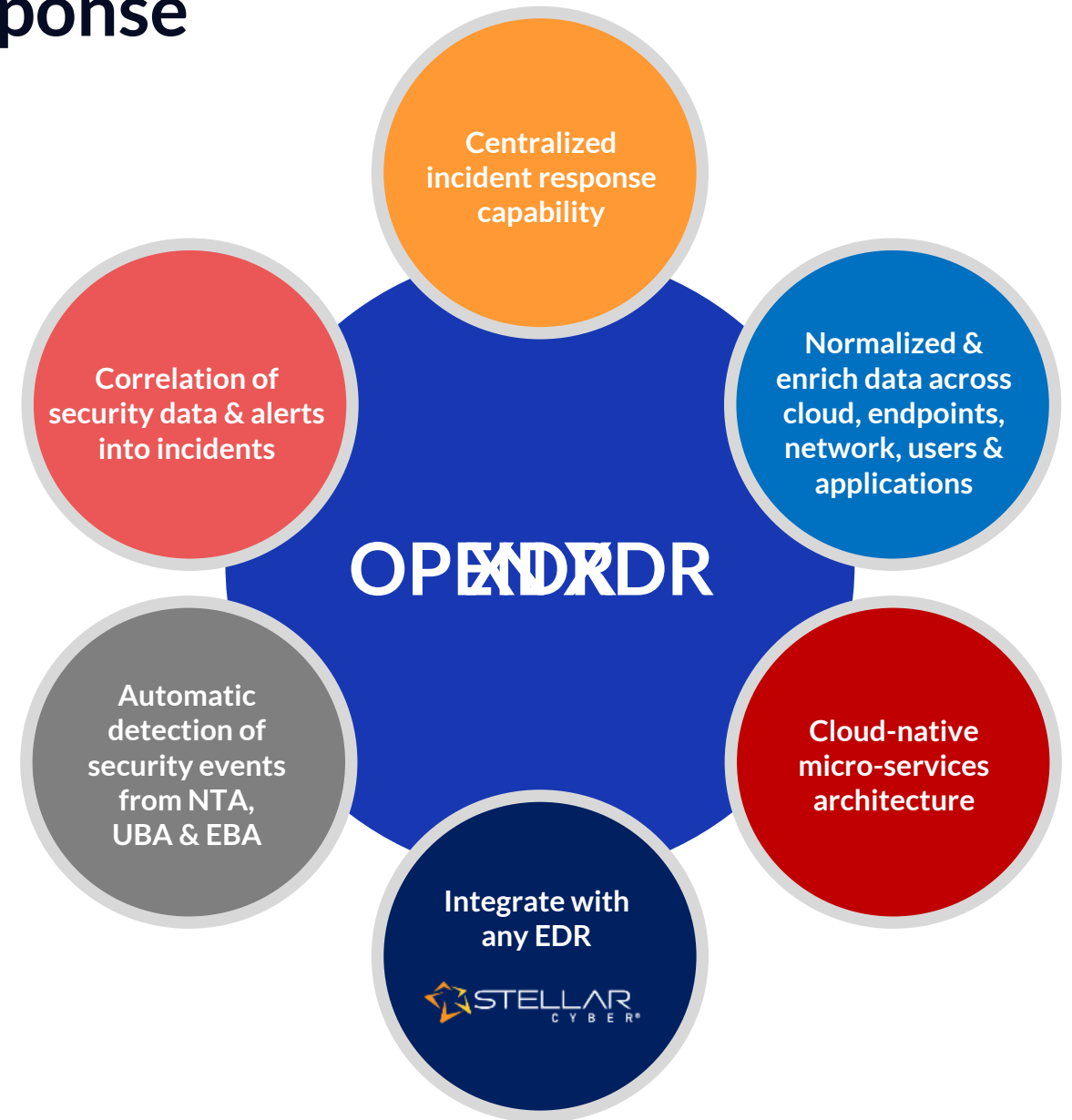
ESG
Enterprise Strategy Group

IDC

OMDIA
Brought to you by Informa Tech

451 Research®

STELLAR
CYBER®



What is XDR?

- Platform that normalizes, correlates telemetry from security products
 - Endpoint, network, cloud, email, workspace, SSE
 - Centralized data lake for telemetry storage, processing
- Unifies security analytics, incident correlation
 - Detection plus Correlation ML, combining weak signals from multiple components into stronger signals of malicious intent
- Automates data triage, playbooks, hunting
 - Centralized command of automated response functions of security products

What it should do

- Improve efficiency and effectiveness in Security Operations
 - Identify threats, detection and response workflow
- Support automation of detection and response of security products
 - Endpoints, firewalls, cloud, containers, identity, Email, SASE
- Advanced analytics and machine learning
 - Attack surface visibility and machine-speed correlation
- Integrate with IT operations and service delivery tools
 - ITSM, PMM, PSA

Native XDR

- Evolved endpoint centric approach - *Forrester*
- Integrations and cross control response on vendors backplane
- Benefits:
 - Simplify buying,
 - Native integrations,
 - Vendor consolidation
- Risks:
 - Vendor lock-in
 - Competitor integrations
- Ideal for smaller, lower operational maturity

Open XDR

- Open Platform – Composable Security
- Integrations with security vendors
- Combines key SOC function in platform
- Cross control response and ML on Open platform
- Benefits:
 - Any security vendor
 - Composable security architecture
 - Flexibility
- Risks:
 - Acquisition

Why Open XDR

- Onboard any technology
- Tool Consolidation
- Unifies cross-control response
- Reduce Manual Work & SOC Burnout
- Composable security architecture



Why Stellar Cyber

Stellar Cyber– NextGen Security Operations Platform– See Us @ Stand 6-203

- Over 4,000 customers globally
- Market leading technology partnerships
- 400+ security vendor integrations



Open approach ensured
investments leveraged



Stellar Cyber short
listed as top 20 security
analytics platform



Editor's Choice XDR
2022



CRN's Tech Innovator
Award 2021



Stellar Cyber
is a standout for
XDR projects



Stellar Cyber offers
pervasive protection
with its XDR platform



Best Cybersecurity
Solution 2022



Astor's Gold Award
Winner 2021



Stellar Cyber improves
SOC efficacy, efficiency
and productivity



Futuriom 40 - Market
Leader 2022



TMCnet Cyber Security
Award 2021





www.stellarcyber.ai
See us @ Stand 6-203