QRadar XDR

level 2 client presentation

Chip Wagner
Worldwide QRadar XDR Sales Leader
wagnerdo@us.ibm.com

The era of the advanced threat

>50% of technical U.S. executives cited state-sponsored cyberattacks as their #1 concern

What NIST zero trust architecture says about threat management

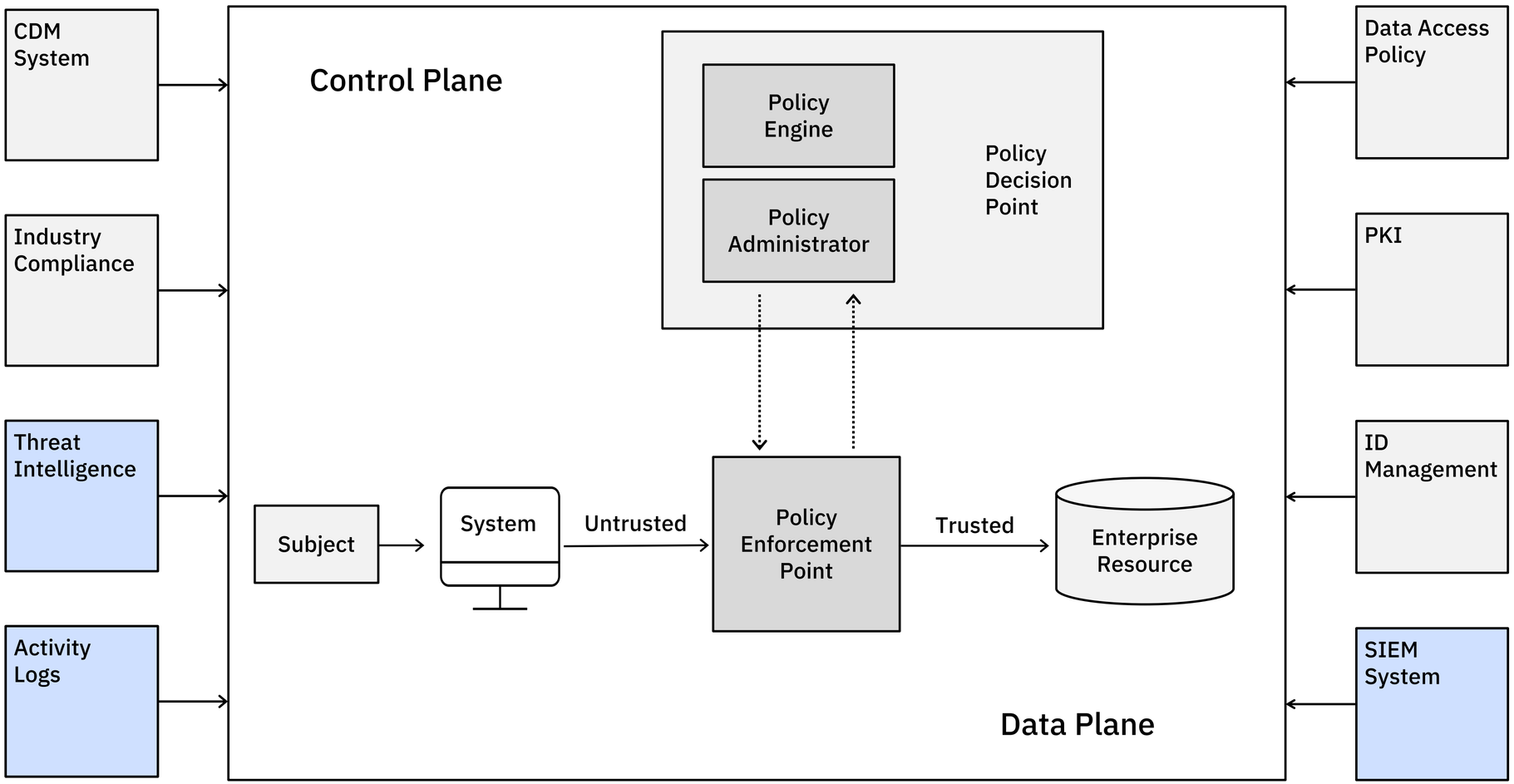
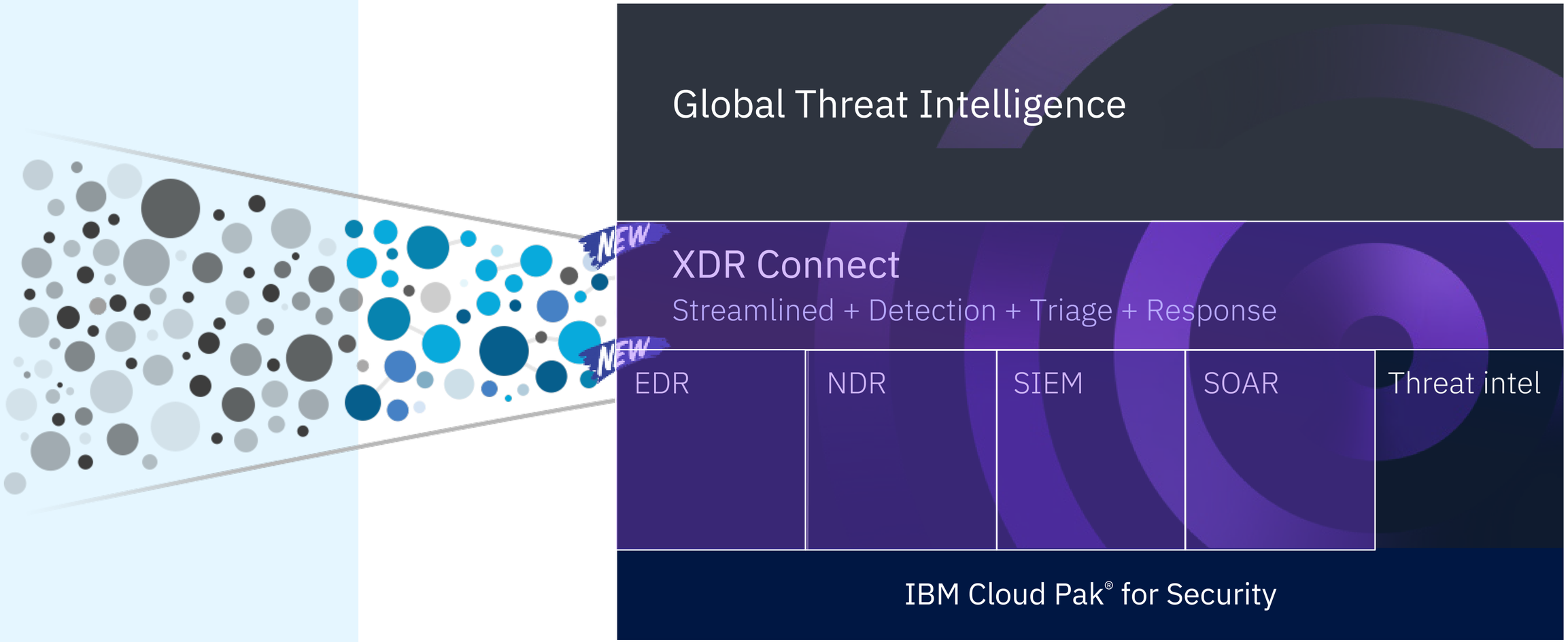


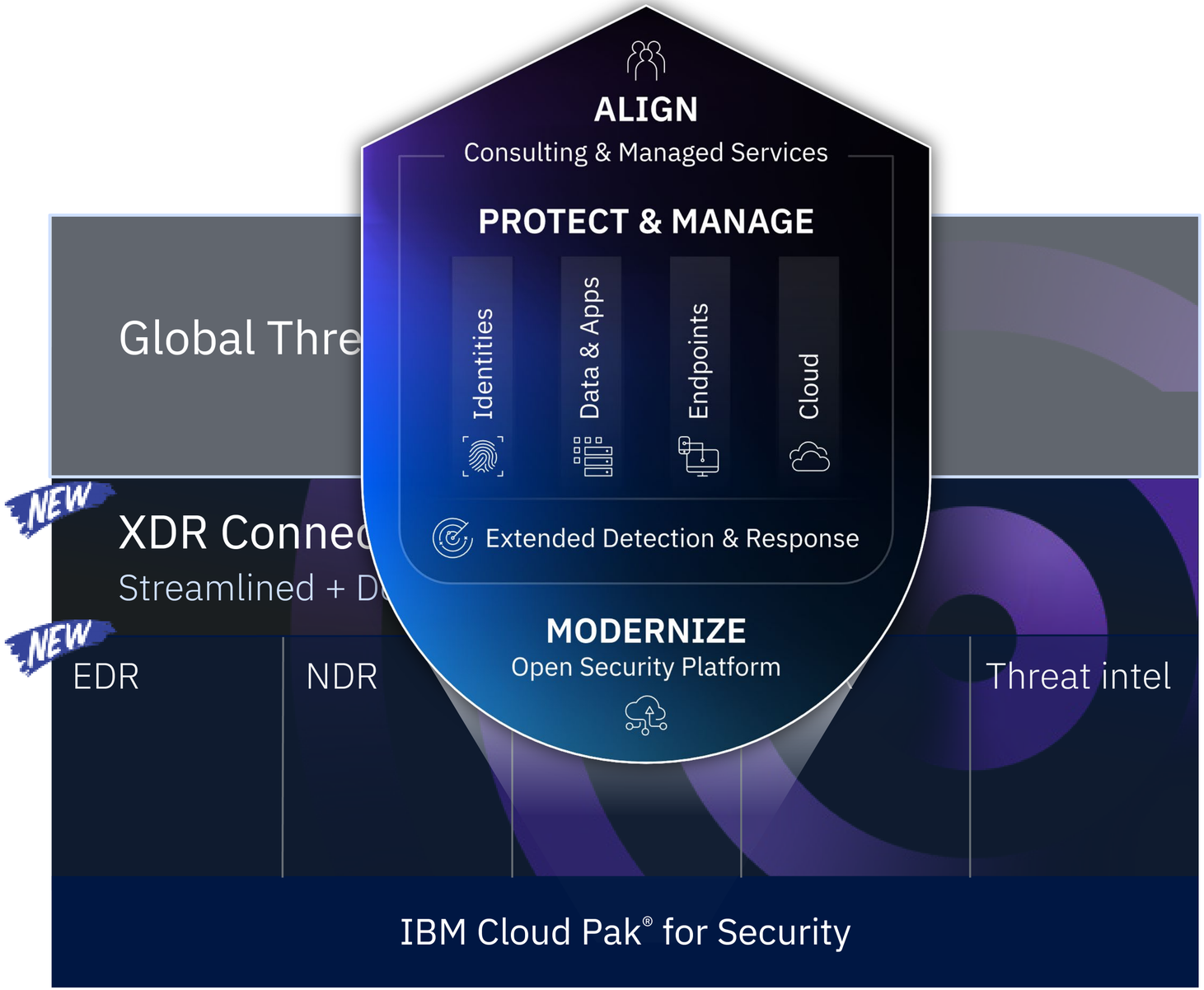
Figure 2: Core Zero Trust Logical Components

Threat management, evolved



X-Force Global Threat Intelligence

Global visibility + advanced analytics = Global Threat Intelligence



QRadar NDR

– Behavioral analytics

– Next-gen forensics

– Automated network learning

QRadar SIEM

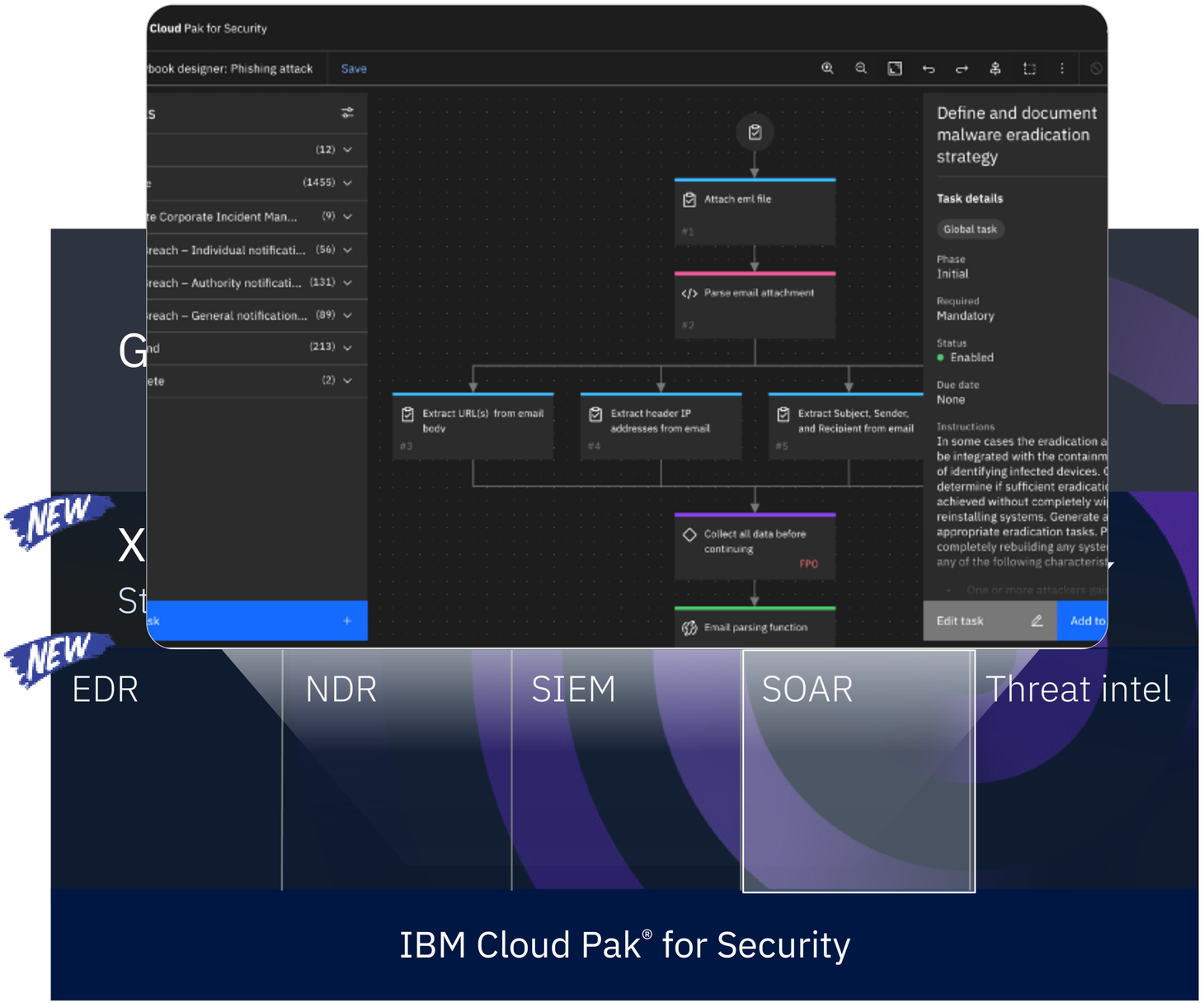
– Advanced analytics

– Advanced correlation

– Simplified visibility

QRadar SOAR

- Streamlined orchestration
- Streamline legal notifications
- Enterprise artifact analysis

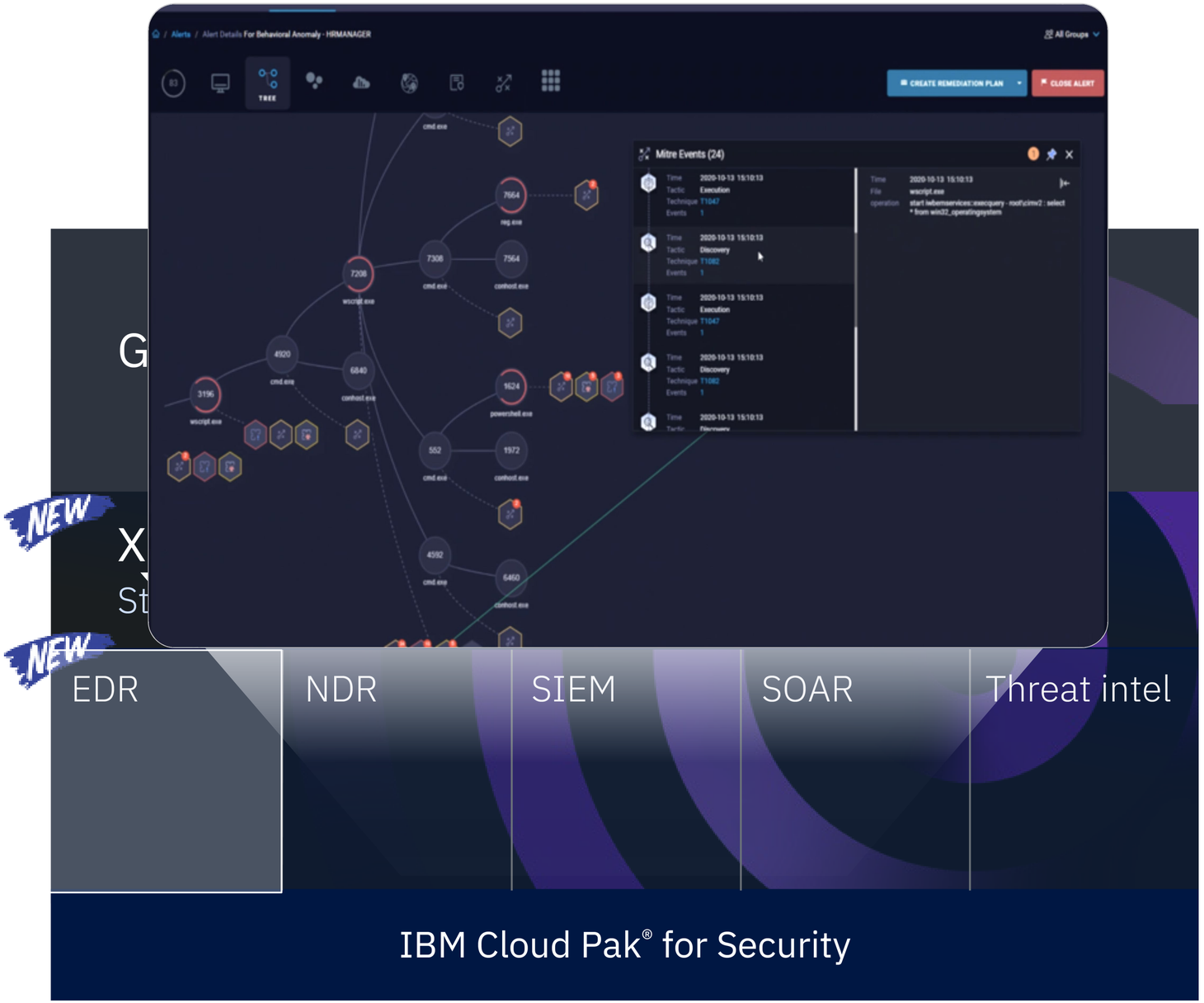


QRadar EDR

– Tamper resistant

– Autonomous threat detection

– Stops ransomware

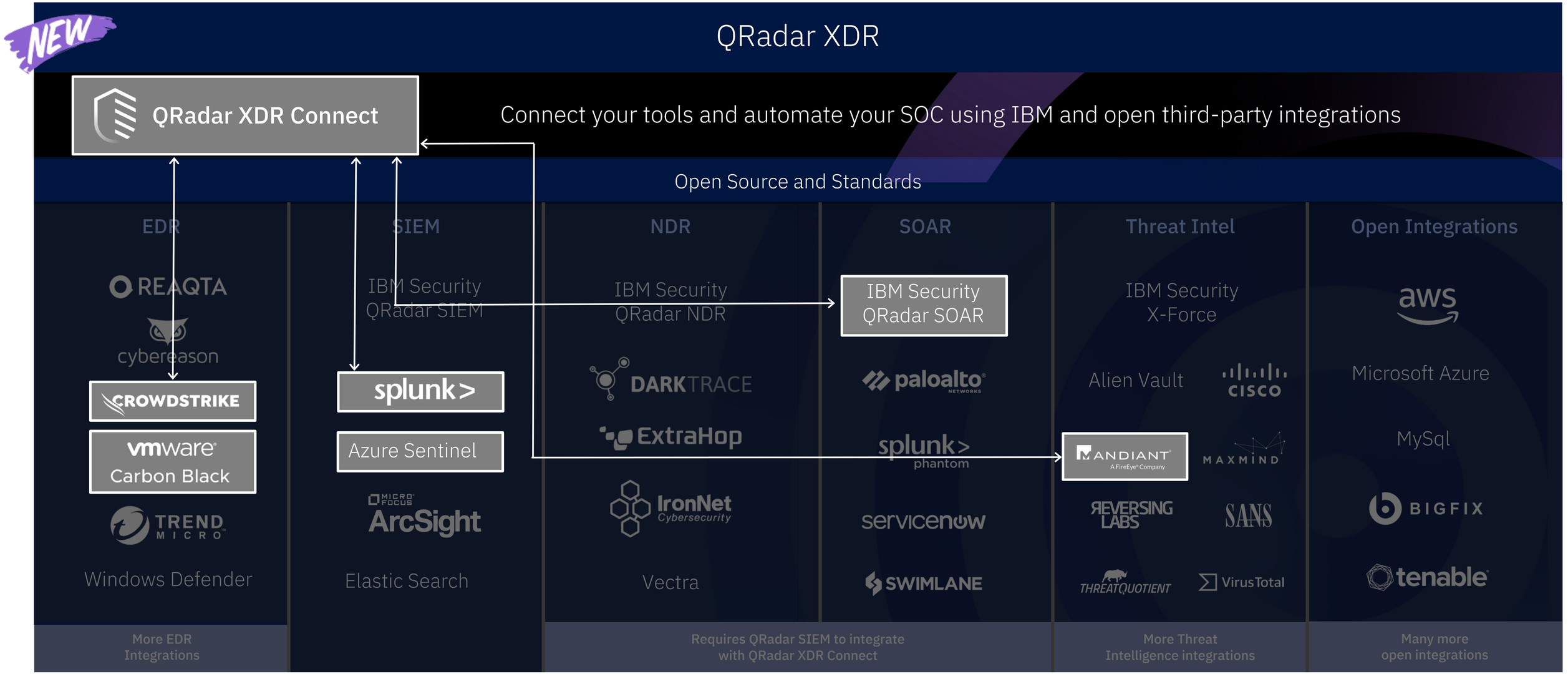


QRadar XDR Connect

– Supports native or hybrid XDR

– Interconnects key components of a threat practice

Simplifying threat management (native or hybrid XDR)



Evolved to solve

Improve operational efficiency by providing tools to more easily ingest data and better manage the system

Advanced analytics to accurately detect critical threats against users, networks, systems and applications

Streamline workflows to help analysts make faster, well-informed escalations decisions

Mission:
Enable clients to accurately and efficiently detect and manage threats to help mitigate the risk of data exposure and business disruption