

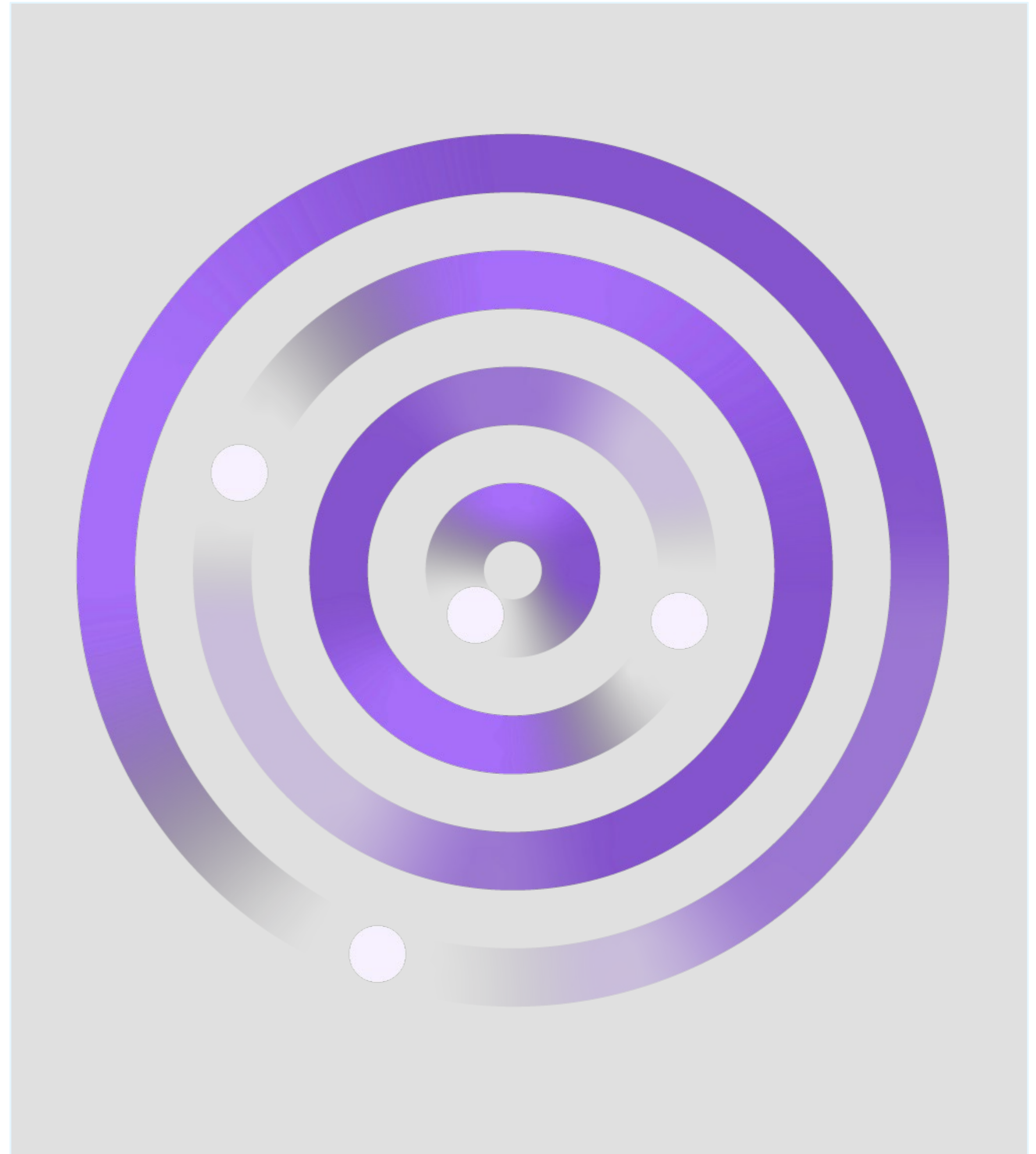
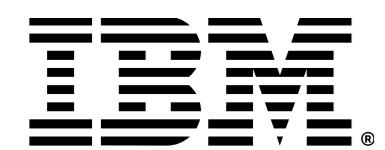
QRadar XDR

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

>50%

What NIST zero trust architecture says about threat management

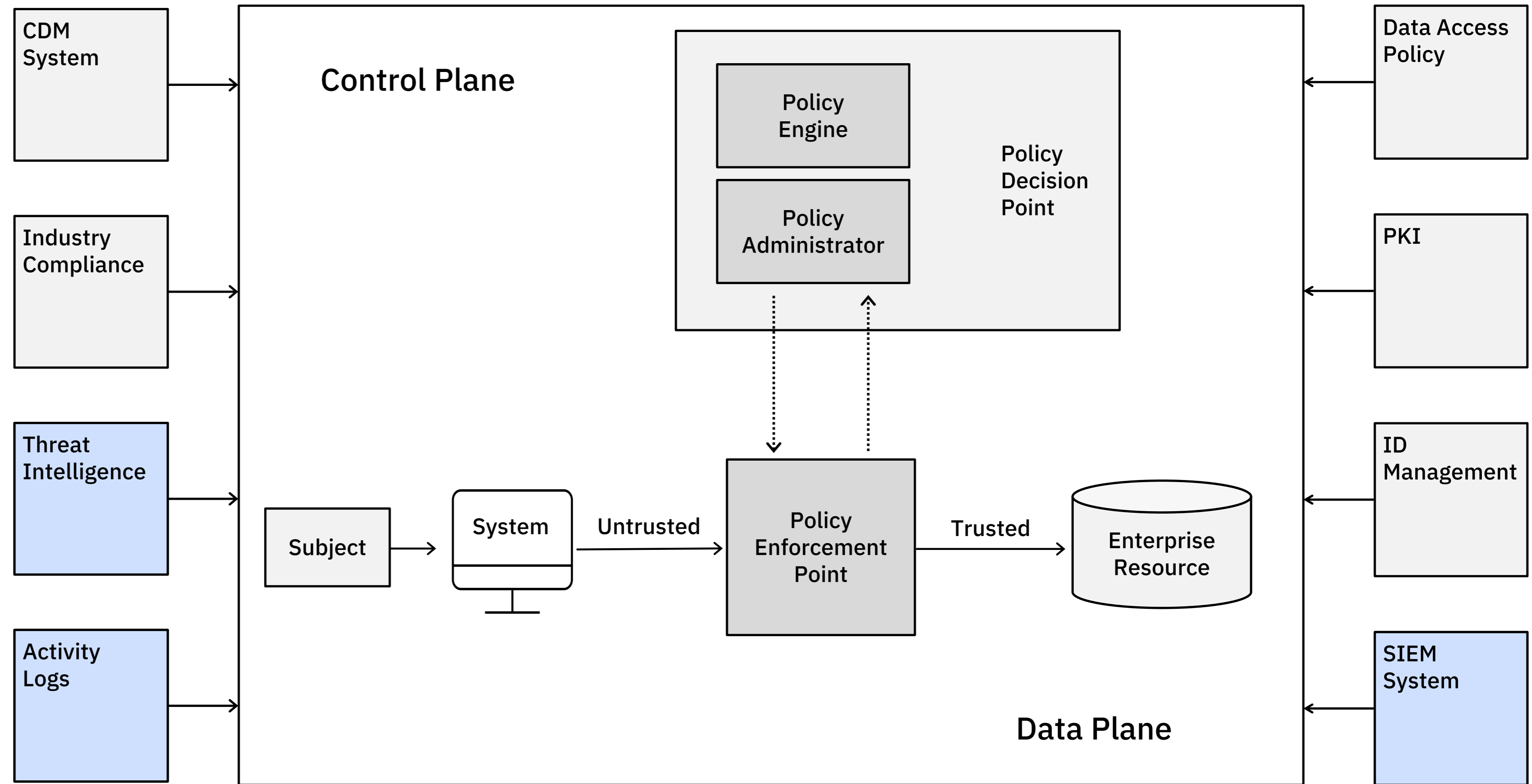


Figure 2: Core Zero Trust Logical Components

Threat management, evolved

Global Threat Intelligence

XDR Connect

Streamlined + Detection + Triage + Response

NEW
EDR

NDR

SIEM

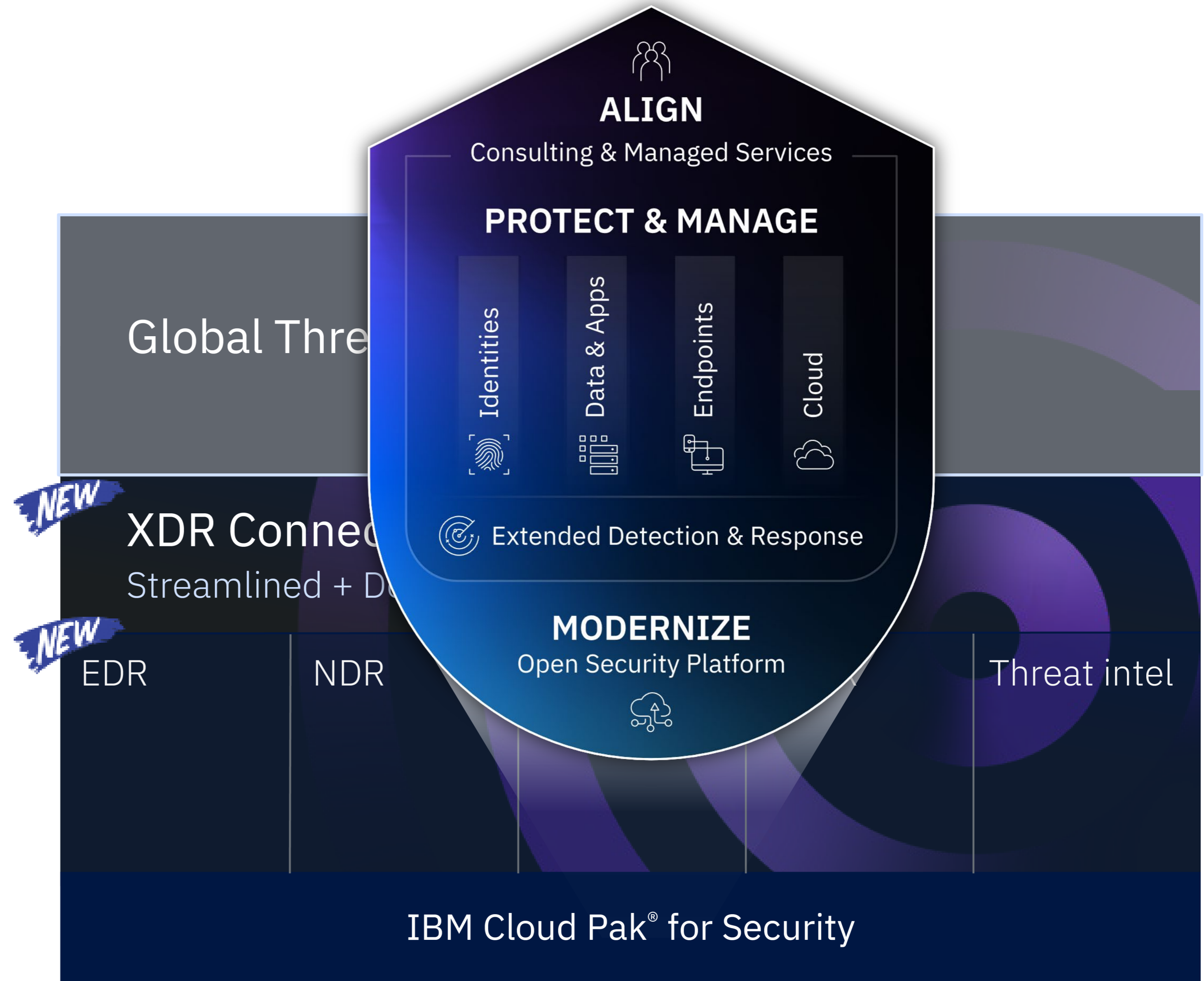
SOAR

Threat intel

IBM Cloud Pak® for Security

X-Force Global Threat Intelligence

Global visibility + advanced analytics = Global Threat Intelligence



QRadar NDR

- Behavioral analytics
- Next-gen forensics
- Automated network learning

The screenshot displays the QRadar NDR interface. At the top, it shows 'Network Traffic Analysis' with 'All traffic: 41/48' and 'Anomalous traffic: 50/17'. The main view is a world map with traffic flows, filtered by 'Region' to 'United States'. A 'Flow details' panel on the right provides the following information:

Overview	Flow details
High frequency port scanning	Protocol: TCP, Application: 1017
Source payload: 7 packets, 68K bytes	Destination payload: 19 packets, 35K bytes
First packet time: Feb 5, 2021, 8:20:48 AM	Last packet time: Feb 5, 2021, 8:52:23 AM
Source location: Europe	Destination location: External host
Source region: Europe	Destination region: China
Source IP: 192.168.105.236	Destination IP: 10.213.85.136
Source port: 326	Destination port: 375

Below the map is a timeline of 'Anomalous flows over time' with a 'NEW' sticker. At the bottom, a navigation bar includes 'EDR', 'NDR', 'SIEM', 'SOAR', and 'Threat intel', with 'NEW' stickers above 'EDR' and 'NDR'. The footer reads 'IBM Cloud Pak® for Security'.

QRadar SIEM

- Advanced analytics
- Advanced correlation
- Simplified visibility

The screenshot displays the IBM Security QRadar SIEM dashboard with the following components:

- Open offenses:** 15 offenses.
- Magnitude Summary:** Critical magnitude: 0, High magnitude: 11, Medium magnitude: 4, Low magnitude: 0.
- World source and destination:** A world map showing event flows between various geographic locations.
- Average event rate (EPS):** A line graph showing the event rate over time.
- Top log sources:** A bar chart showing the top log sources, including QRadarAdmin@Wilson, McAfee Network Security Platform, Juniper JunOS Platform @ 10.10.10.10, WindowsAuthServer @ 10.64.2.11, WindowsAuthServer @ 10.64.2.12, and LinuxServer @ 10.64.2.13.
- Log source count:** A line graph showing the count of log sources over time.
- Events per user:** A donut chart showing the distribution of events per user, including root, UCM, USA, admin, configservices, Real, and unknown.

On the left side of the dashboard, there are two blue banners with the word "NEW" written on them, positioned over the "G" and "X" labels. Below the dashboard, there is a navigation bar with five tabs: EDR, NDR, SIEM, SOAR, and Threat intel. The SIEM tab is currently selected and highlighted.

IBM Cloud Pak® for Security

QRadar SOAR

- Streamlined orchestration
- Streamline legal notifications
- Enterprise artifact analysis

The screenshot displays the SOAR (Security Orchestration, Automation, and Response) interface within IBM Cloud Pak for Security. The main workspace shows a workflow for a 'Phishing attack' incident. The workflow starts with 'Attach eml file' (#1), followed by 'Parse email attachment' (#2). This task branches into three parallel tasks: 'Extract URL(s) from email body' (#3), 'Extract header IP addresses from email' (#4), and 'Extract Subject, Sender, and Recipient from email' (#5). These tasks converge into a 'Collect all data before continuing' task (#6), which is marked with a red 'FPC' (Final Process Check) icon. The final task is 'Email parsing function' (#7). On the right, a 'Task details' panel shows the task is a 'Global task', 'Initial' phase, 'Mandatory', 'Enabled' status, and 'None' due date. A 'NEW' sticker is placed over the 'NEW' button in the interface.

IBM Cloud Pak[®] for Security

QRadar EDR

- Tamper resistant
- Autonomous threat detection
- Stops ransomware

The screenshot displays the QRadar EDR interface. At the top, it shows 'Alerts / Alert Details For Behavioral Anomaly - HRMANAGER'. Below this is a navigation bar with icons for 'TREE', 'SEARCH', and 'FILTER'. A 'CREATE REMEDIATION PLAN' button and a 'CLOSE ALERT' button are visible in the top right. The main area features a process tree diagram with nodes representing different processes and their relationships. A 'Mitre Events (24)' panel is open on the right, listing events with details such as Time, Tactic, Technique, and Events. The interface is overlaid on a dark background with a grid of security solution categories: EDR, NDR, SIEM, SOAR, and Threat intel. The 'EDR' category is highlighted with a white border and a 'NEW' sticker. The 'SIEM' category is also marked with a 'NEW' sticker. The overall theme is dark blue and purple.

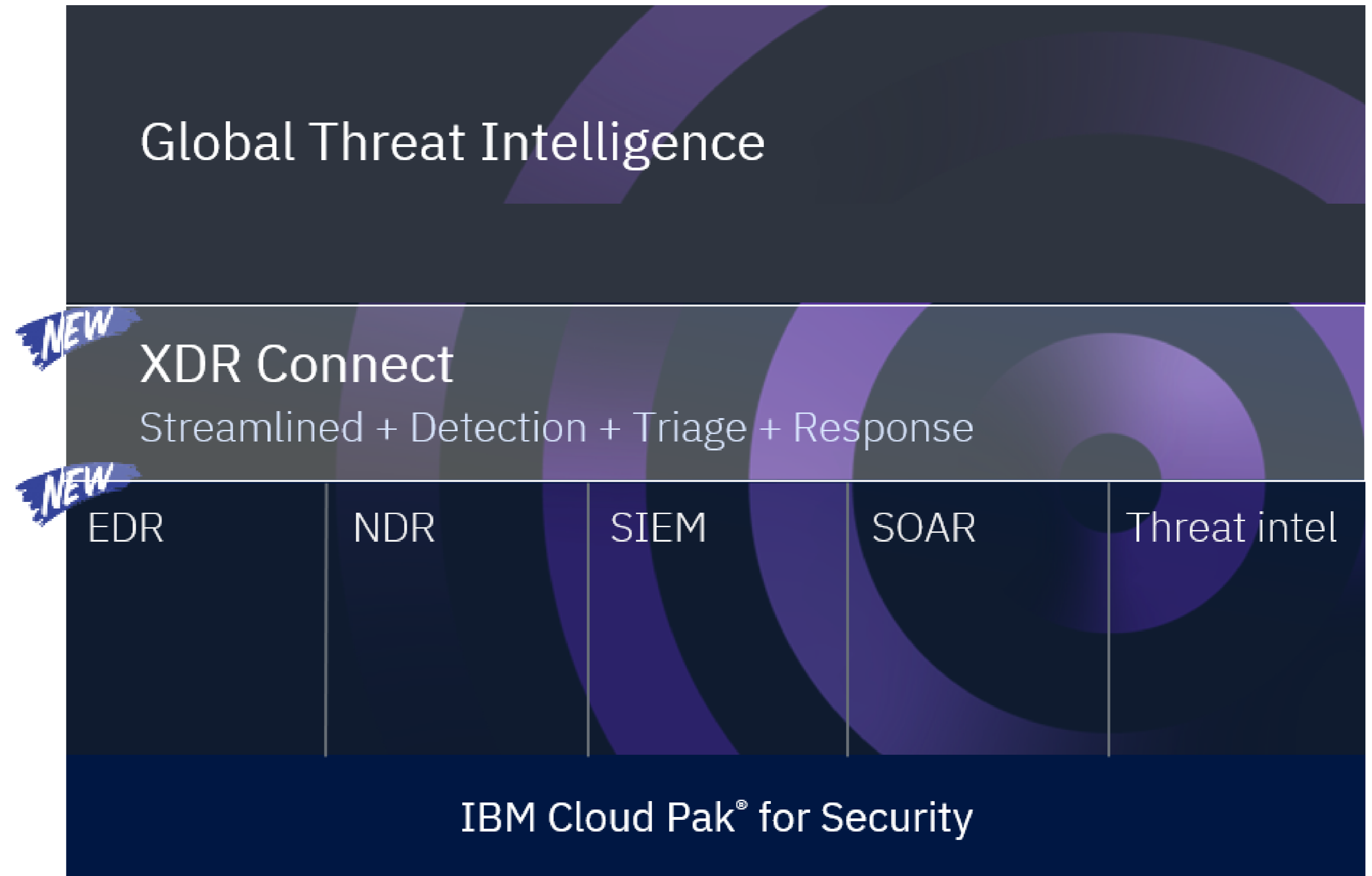
NEW
NEW

EDR NDR SIEM SOAR Threat intel

IBM Cloud Pak® for Security

QRadar XDR Connect

- Supports native or hybrid XDR
- Interconnects key components of a threat practice



Simplifying threat management (native or hybrid XDR)

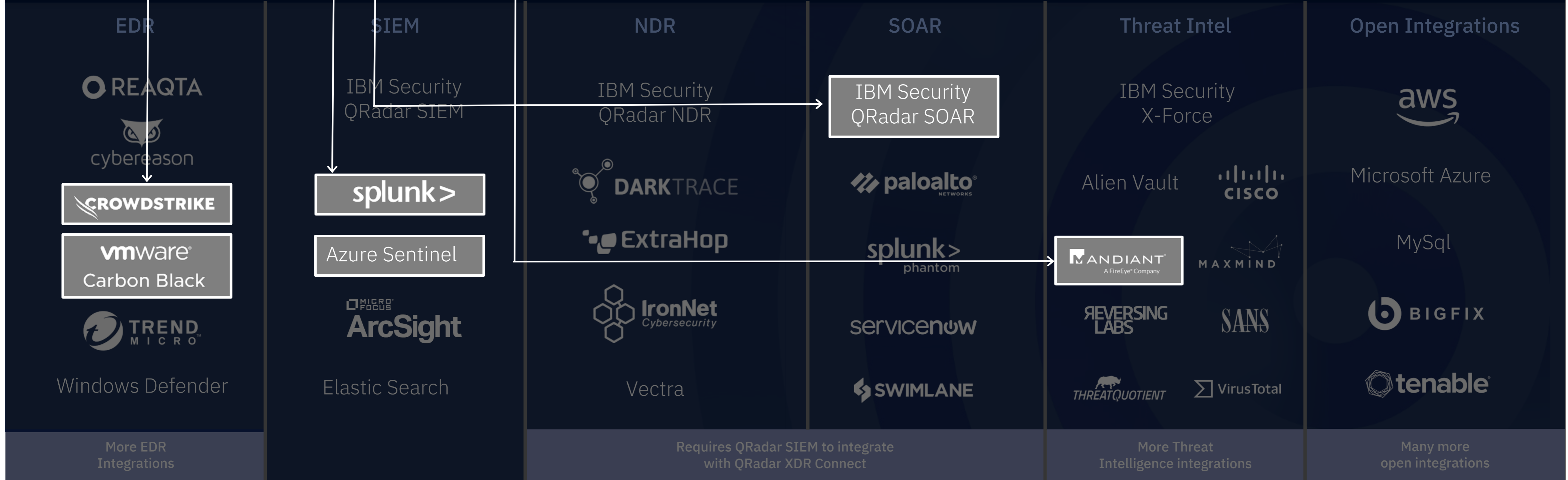
NEW

QRadar XDR

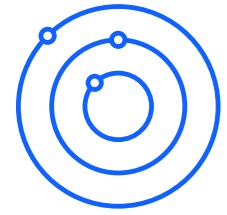
 QRadar XDR Connect

Connect your tools and automate your SOC using IBM and open third-party integrations

Open Source and Standards



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

