Security Implications in the Cloud

Patchara Srinimnuan (CISSP,CISA,CISM)
Technical Solution Specialist, IBM Security

IBM

Every business is racing to manage cybersecurity risk.

Geo and industry trends

31%
Asia-Pacific region top attacked geography

25%
Manufacturing top attacked industry

63% of organizations seek to improve their ability to detect and respond[1]

Poor visibility
2 out of 3 organizations' external attack surface has expanded in the last year[2]

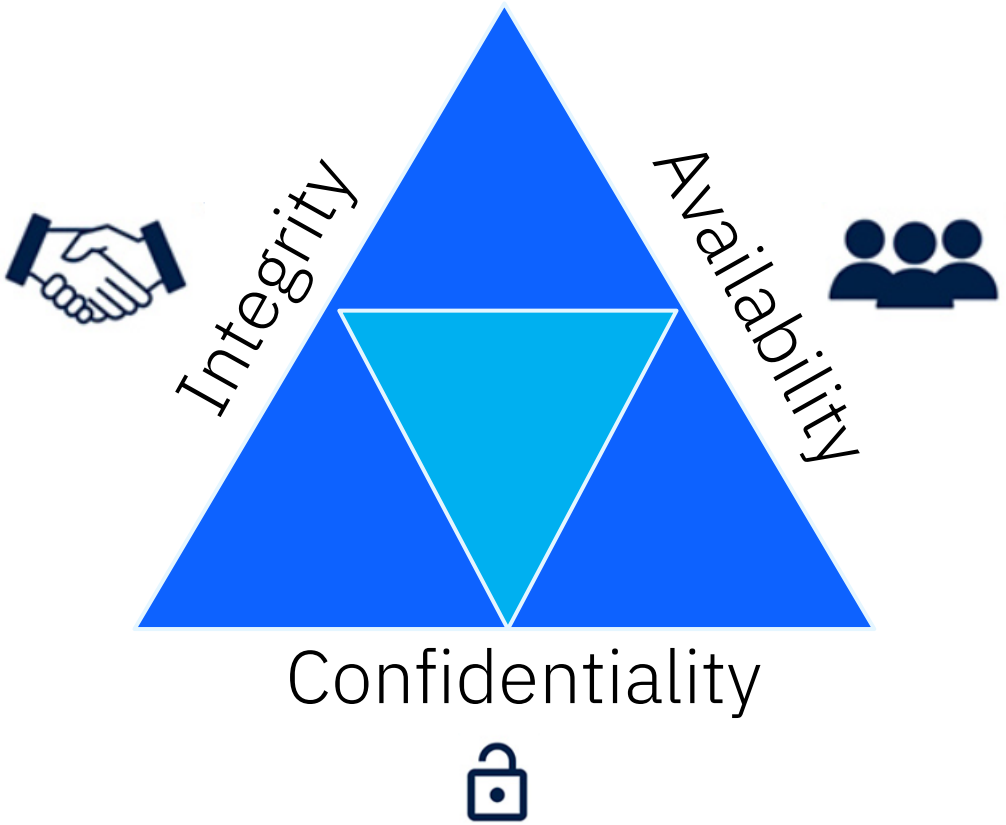
Disconnected tools
80% of organizations use at least 10 disparate solutions to manage security hygiene[2]

Outdated processes
29% of security operations processes are immature and need reengineering before they can be automated[3]

Security complexity
52% of security environments have become more difficult to manage over the last two years[3]

[1] ESG: *The XDR Payoff: Better Security Posture,* 2020; [2] *The State of Attack Surface Management 2022*, Randori; [4] ESG: *SOC Modernization and the Role of XDR, 2022*

Cybersecurity - CIA TRIAD

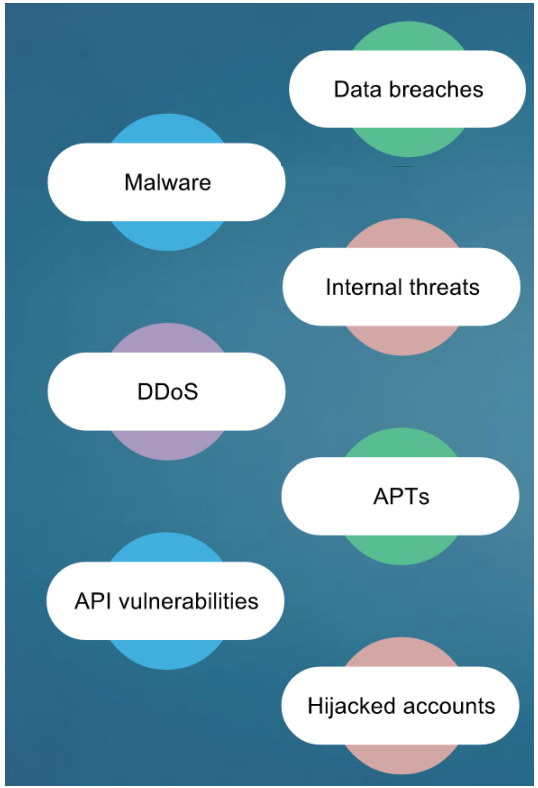


Common Threats for Cloud Security

Malicious scripts in the form of malware injections can potentially be uploaded by attackers to a cloud server that may host applications and services. This can cause any number of serious issues for any organization that may be operating on those servers.

Distributed denial of service (DDoS) is an attempt by attackers to flood an organization's systems with requests for data from multiple sources. This can result in the affected system being overwhelmed and therefore prevent access by customers and users to mission-critical data and applications.

Application programming interfaces (APIs) that have not been secured or configured correctly can leave an open door for intruders to attack from outside sources.



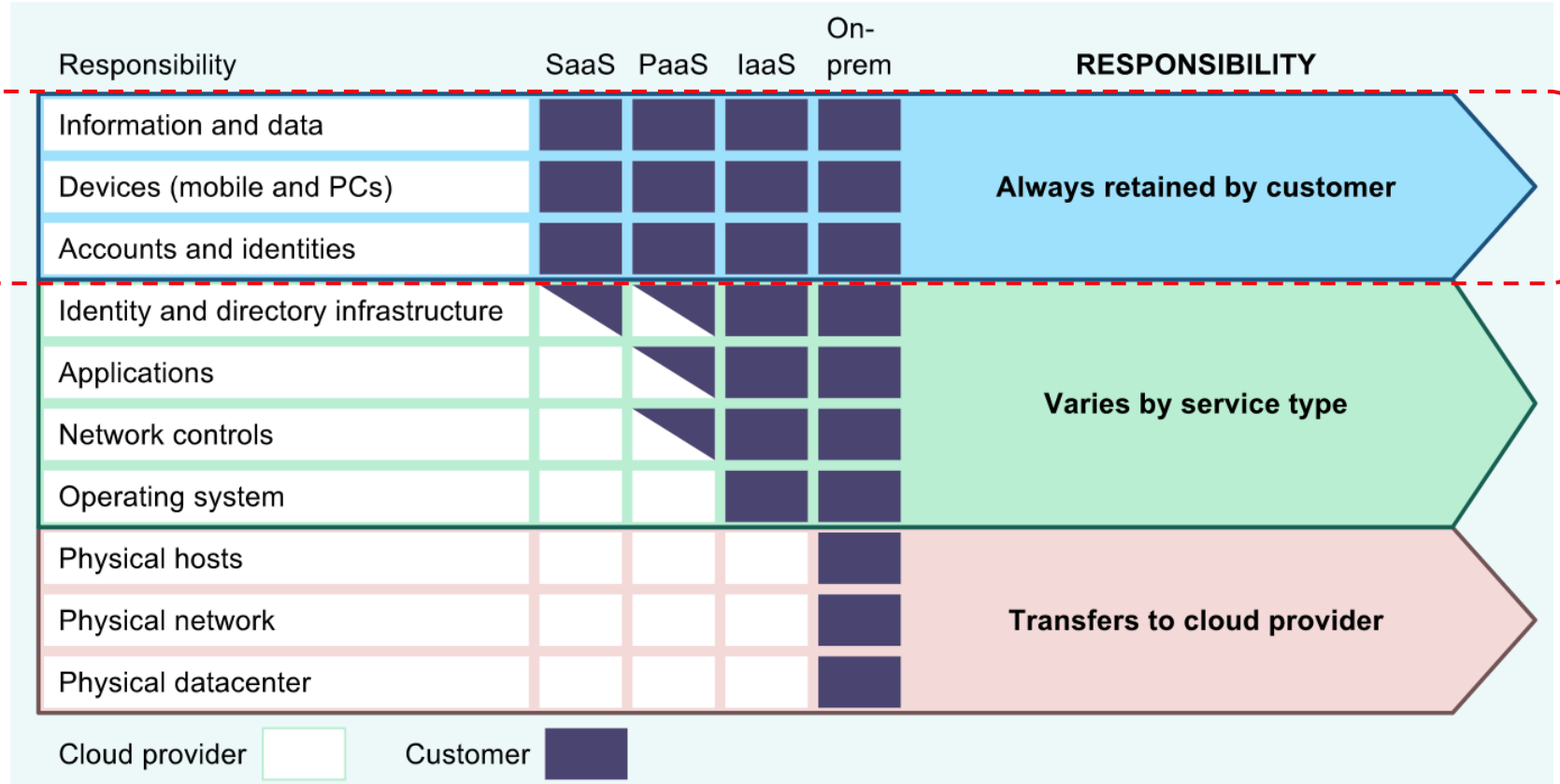
Data breaches are the result of unauthorized access to confidential or sensitive data, which can potentially be exposed, stolen, or used by an attacker. With more businesses operating in the cloud, cybercriminals can exploit new potential access points into an organization's IT infrastructure.

This form of attack may be from a current or former employee, business partner, or anyone with permitted access to an organization's systems or network with the intent of abusing their security privileges.

Advanced persistent threats (APTs) are where intruders have successfully infiltrated an organization's systems and remain undetected for an extended period of time. These types of attacks operate silently with the intent of spying on a business's activity.

Another common threat is login credentials being stolen or compromised by hackers using sophisticated tools and methods to obtain access to an organization's systems. This might also include the use of phishing techniques, an example of which might be whereby user data or credentials are obtained by getting the user to enter or confirm account details through a website masquerading as a trusted entity.

Cloud security responsibility



Identify your data in cloud

Data

- ✓ *At Rest*
- ✓ *In Motion*
- ✓ *In Use*

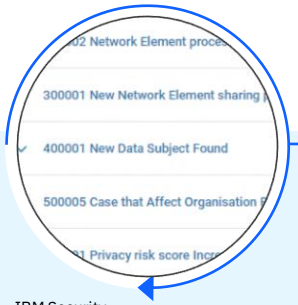
- *Database*
- *Database as a service*
- *File base*
- *PII*
- *Confidential data*

Protect data across the hybrid cloud

Data

Discover and classify data

Automate discovery and classification of on premises and cloud data and uncover critical vulnerabilities



Encrypt and protect data

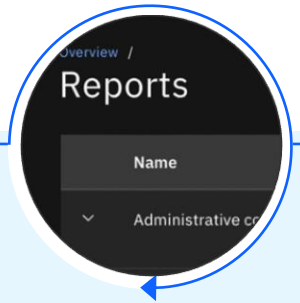
Safeguard privacy and confidentiality of data at rest, in motion, and in use with encryption and access controls

Monitor activity across clouds

Protect cloud-native data sources

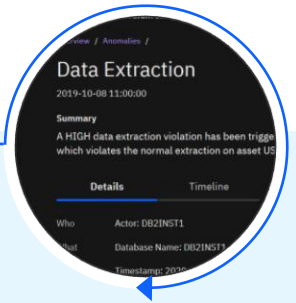
Help automate compliance

Generate reports and automate notification on long-term data activity within seconds, across the audit lifecycle

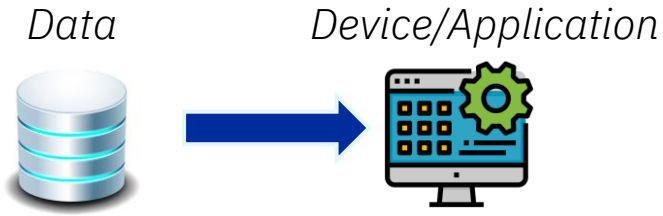


Detect threats and respond

Identify and respond to compliance and data security risks, across environments and teams, from one place

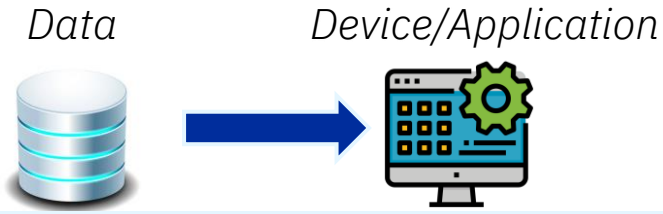


Concept for secure cloud workloads



- ✓ Secure Design
- ✓ Secure Build
- ✓ Secure Operation

Secure application from modern threats.



Workload Protection

continuous protect for cloud workloads across different types of modern environments

- Runtime scanning
- CWPP
- Cloud threat detection

Threat Detection & Response

Detect and respond to suspicious activity in real time

- Application Logs
- Cloud Logs
- Threat Intel

Secure Coding & Vulnerability Management

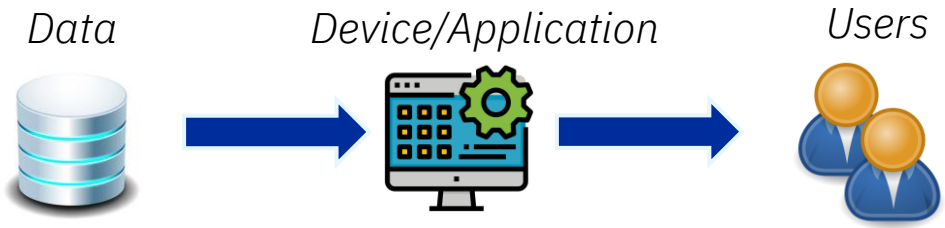
Secure coding and secure build to manage misconfigurations

- SAST/DAST/ Pentest
- Vulnerability Assessment
- Open-Source Scanning

Posture Management & Compliance

Enforce policy across environments with a shared policy model and remediation

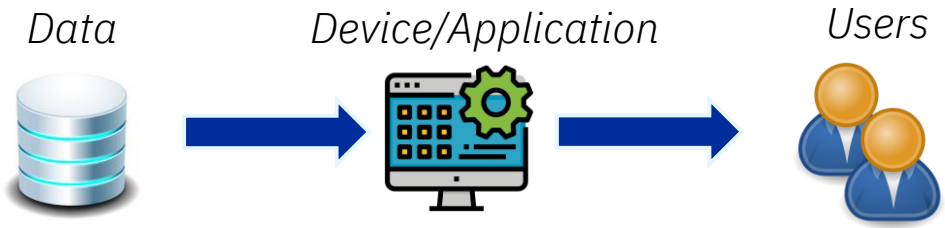
- Compliance Checklist
- Multi-cloud CSPM
- CIEM



Secure remote workers and consumers

- A growing number of siloed constituents (including employees, suppliers, partners, and customers) all using multiple devices from distributed and remote locations
- Brind your own device (BYOD) policies that were expanded to help employees manage the shift to remote work
- Need for granular permission setting on what workforce individuals can do with cloud resources

Secure user access and improve employee productivity



Workforce Identity

Drive cloud modernization, technical agility and user productivity

Continuous Access Control

- Single Sign-On and MFA
- Adaptive access
- Passwordless authentication
- Lifecycle management
- Privileged access
- Privacy and consent management

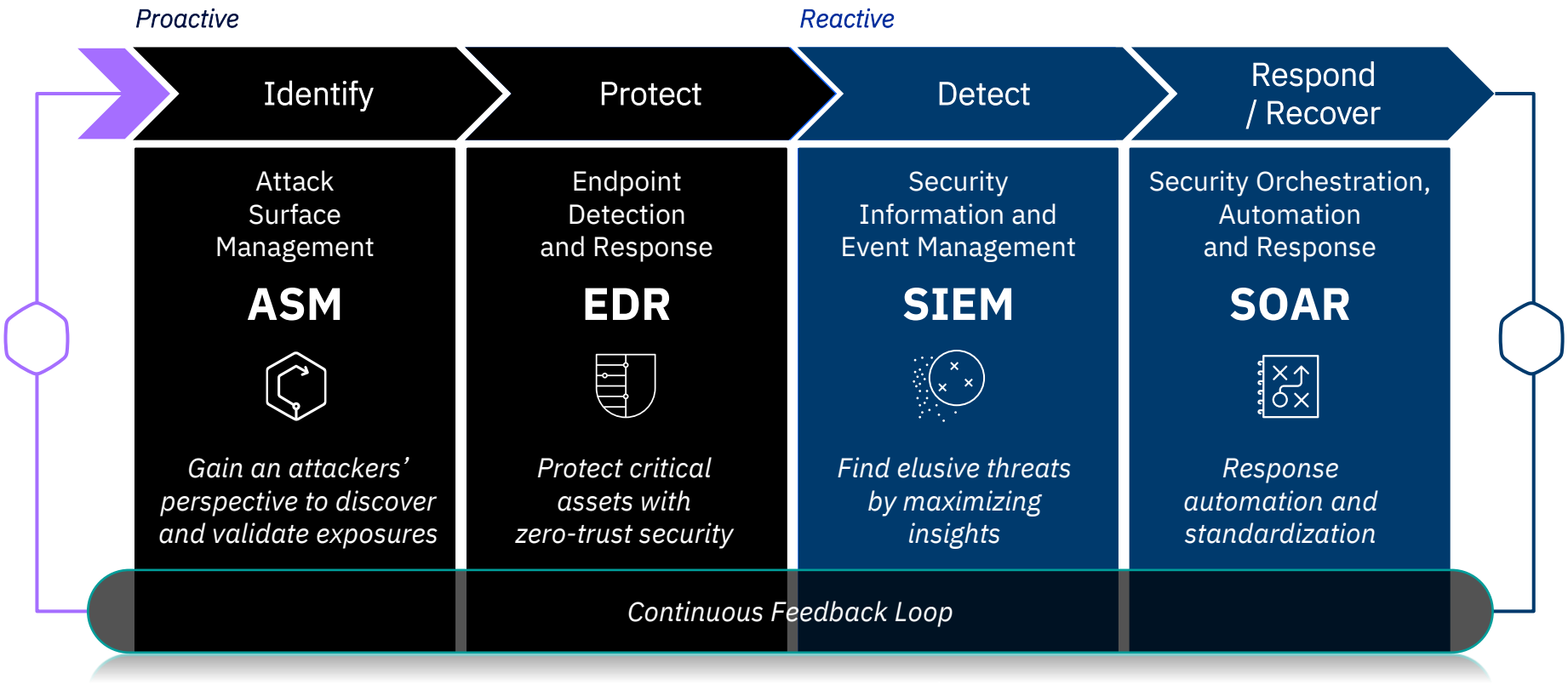
Consumer Identity

Deliver on-demand, personalized, and trusted experiences

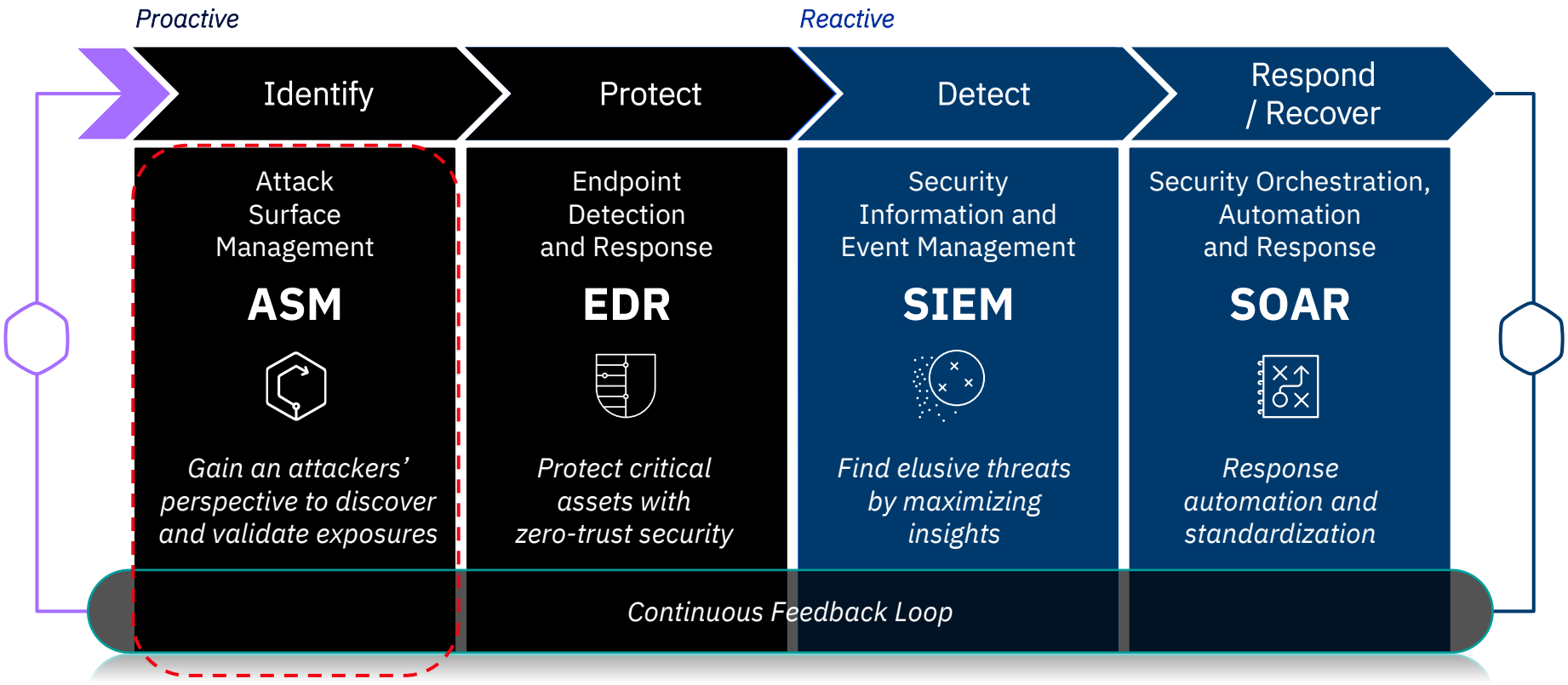
Cloud user directory

Manage users and groups through a scalable and elastic directory while also co-existing with existing directories as needed

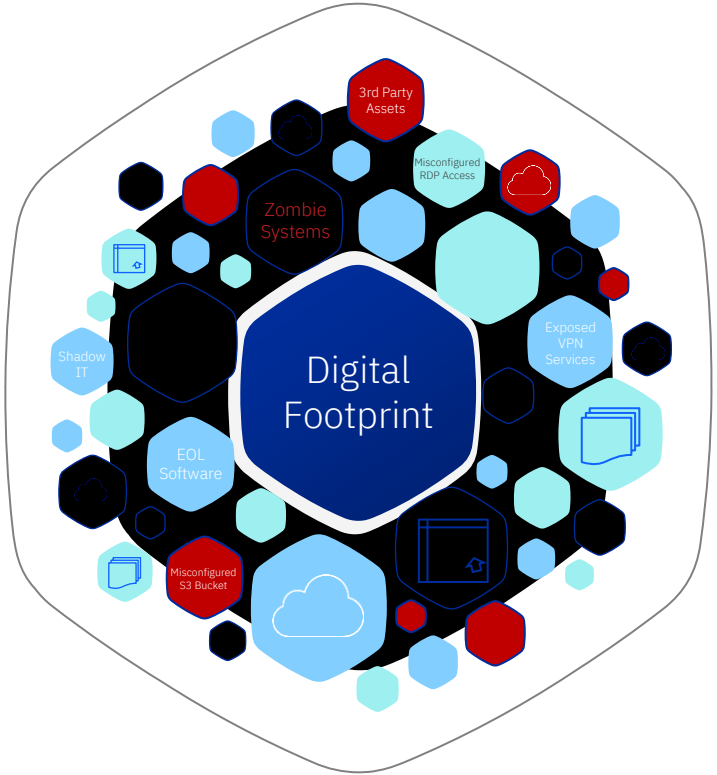
Proactive Threat-Driven Defense Strategy



Proactive Threat-Driven Defense Strategy



Enterprise Attack Surfaces continue to Expand

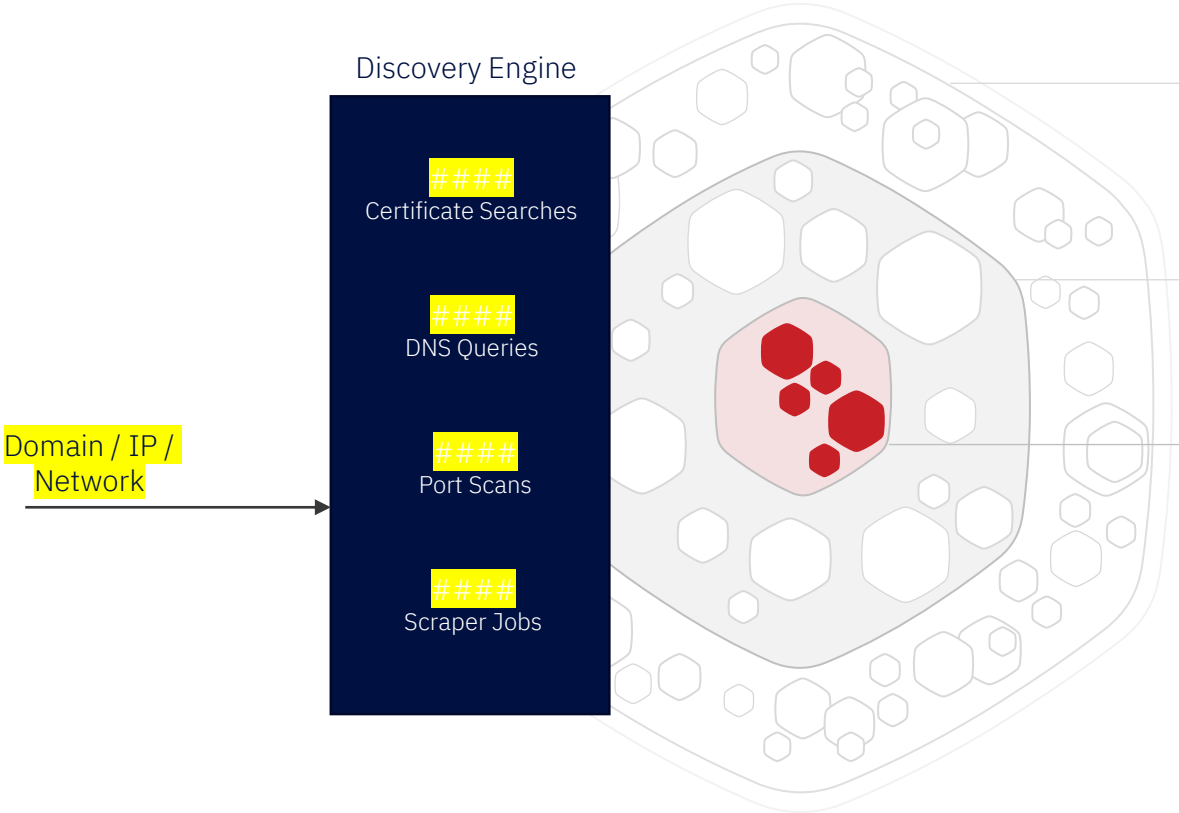


01 Merger & Acquisition

02 Migration to the Cloud

03 Support of Remote Workforce

Discovering your Attack Surface



ACTIVE ASSETS

Assets on your perimeter directly affiliated to the organization with indicators of current use.

TARGETS

Instances of potentially attackable software.

TOP TARGETS

Instances likely to be highly tempting to an adversary.

Core Pillars of Continuous Threat Exposure Management.

01

Attack Surface Management

“What does my organization look like from an attacker’s point of view, and how should it find and prioritize the issues attackers will see first?”

02

Vulnerability Management

“What software is present and what configuration has my organization set that will make it vulnerable to attack?”

03

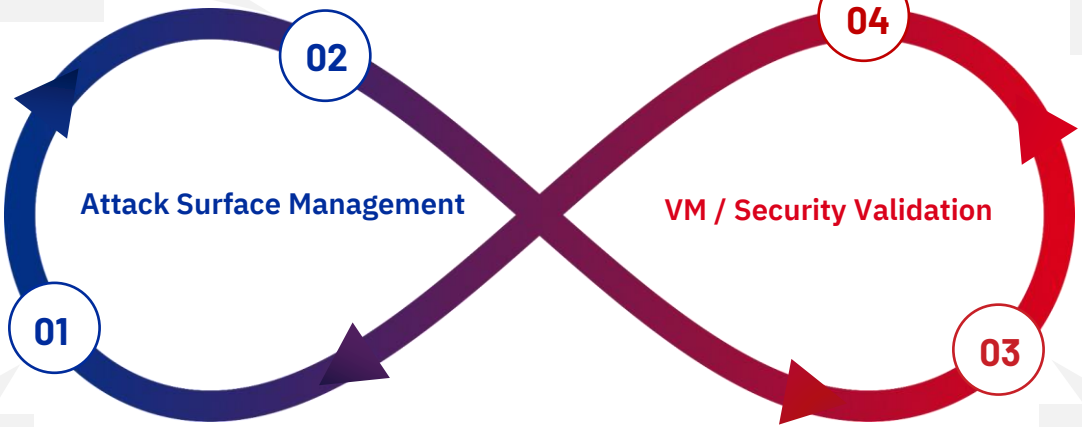
Security Posture Validation

“What would happen if an attacker carried out a campaign against my organization’s infrastructure, how would its defenses cope and how would processes perform?”

CTEM adoption decreases likelihood of a breach by

3x

Build Resilience with Unified Offensive Security



PRIORITIZE

"Understand what an Adversary would Target"

VALIDATE

"Test your Defenses like an Adversary"

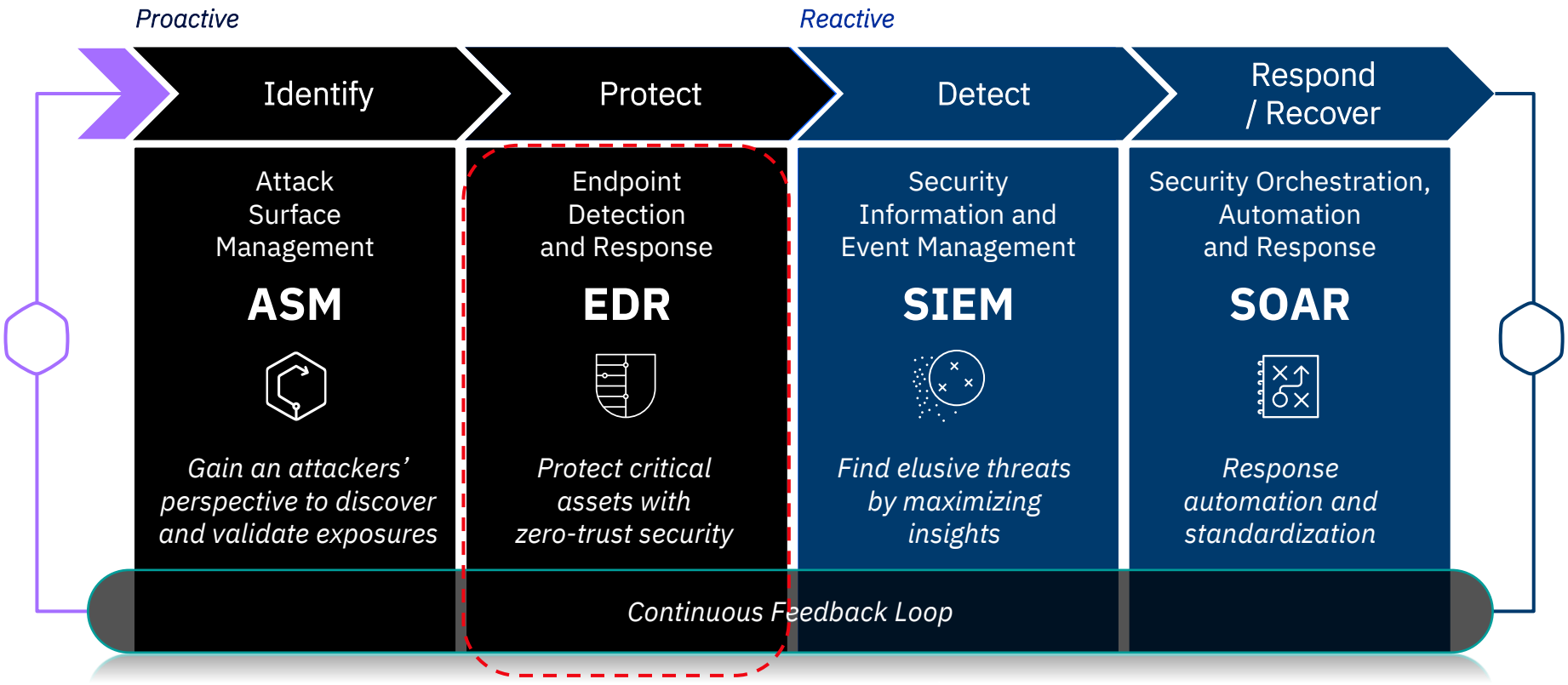
DISCOVER

"See your Attack Surface like an Adversary"

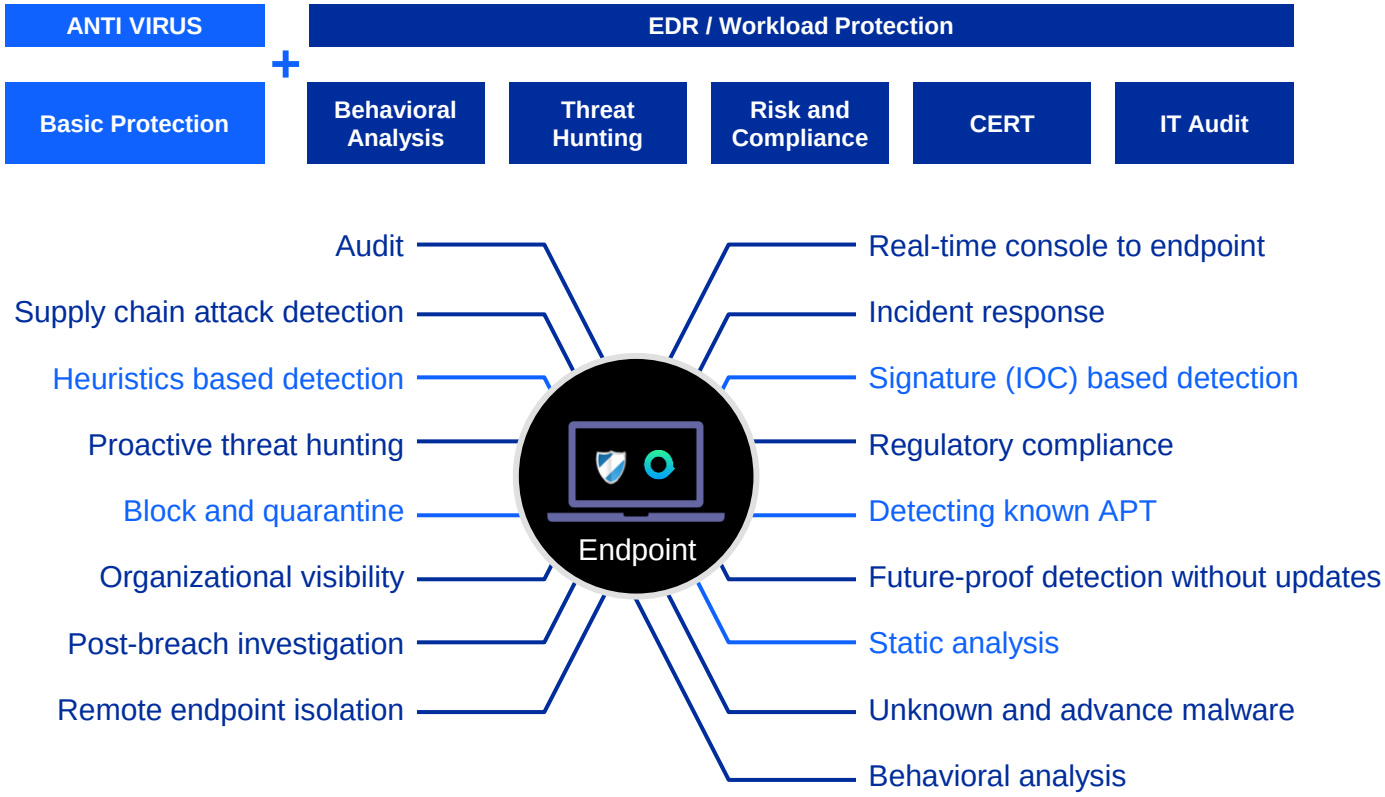
AUTHORIZE

"Scope your most relevant assets for attack emulation"

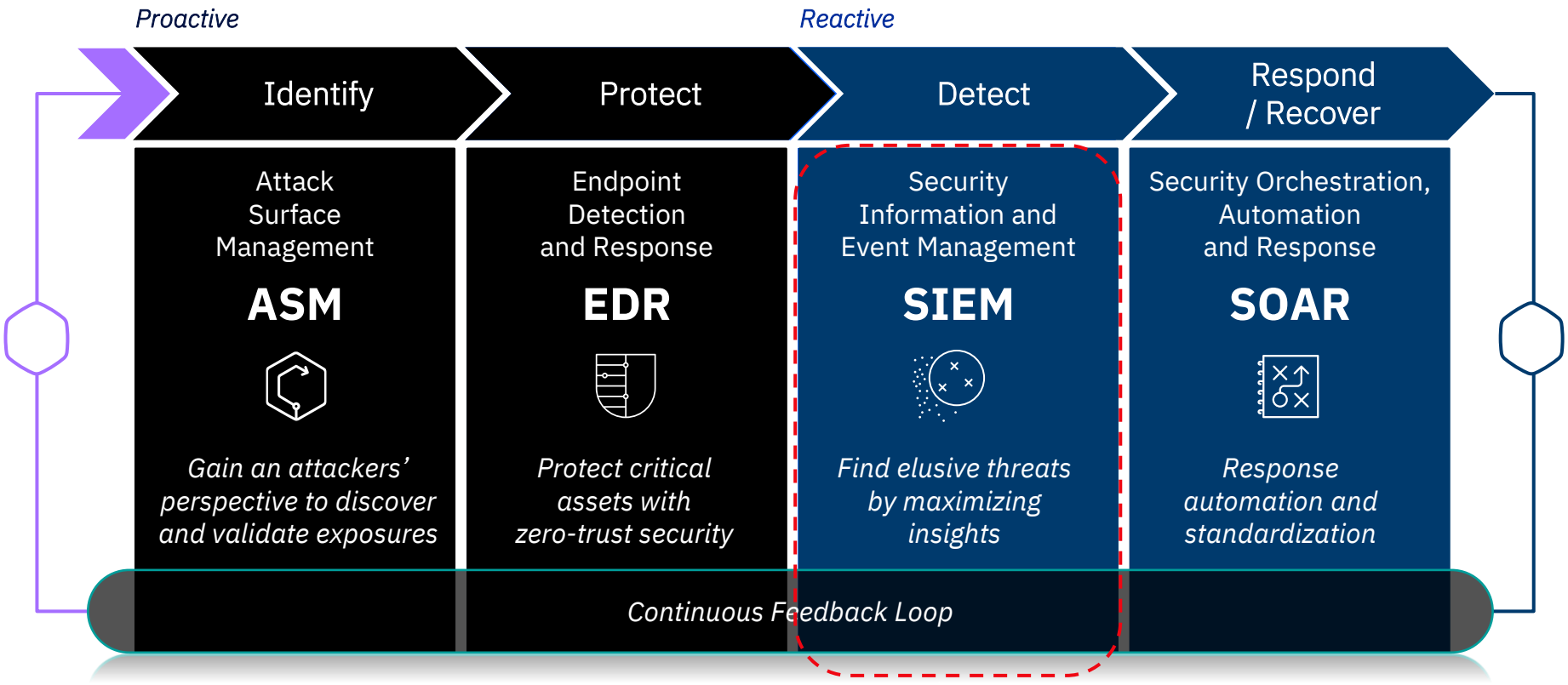
Proactive Threat-Driven Defense Strategy



Why Endpoint Detection & Response?



Proactive Threat-Driven Defense Strategy



Current Security Monitoring Challenges

Complete Visibility

- What happened in our organization?
- Network visibility
- Multiple cloud

Threat Detection

- How to prioritize threat?
- Correlation rules are enough?
- News and Feeds

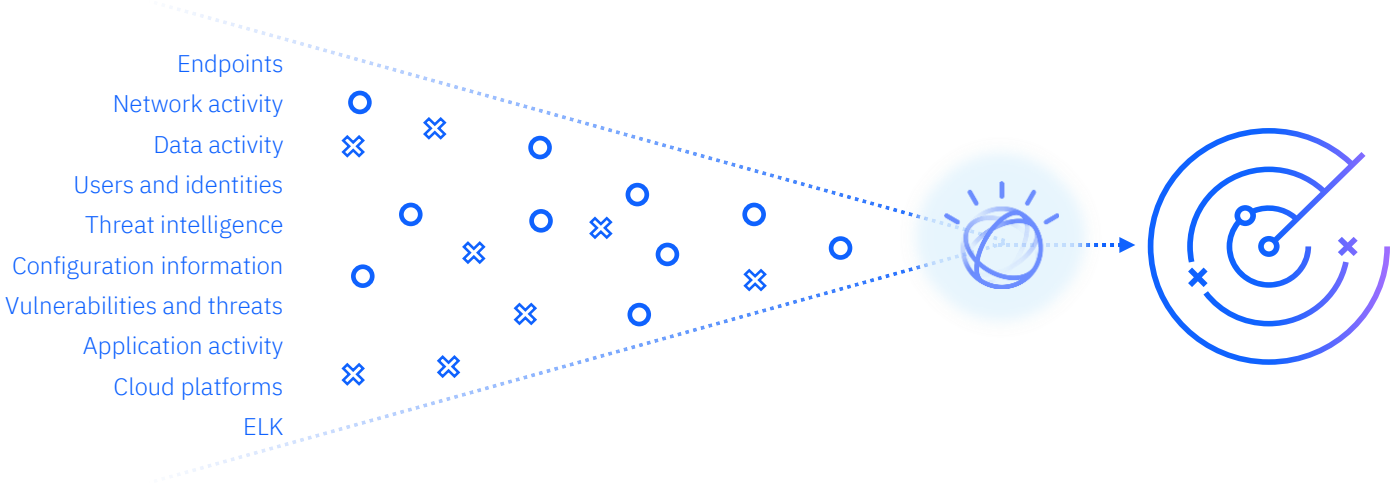
Investigations

- Actionable Information
- Dashboard and report
- Automated Investigation

Integrated Response

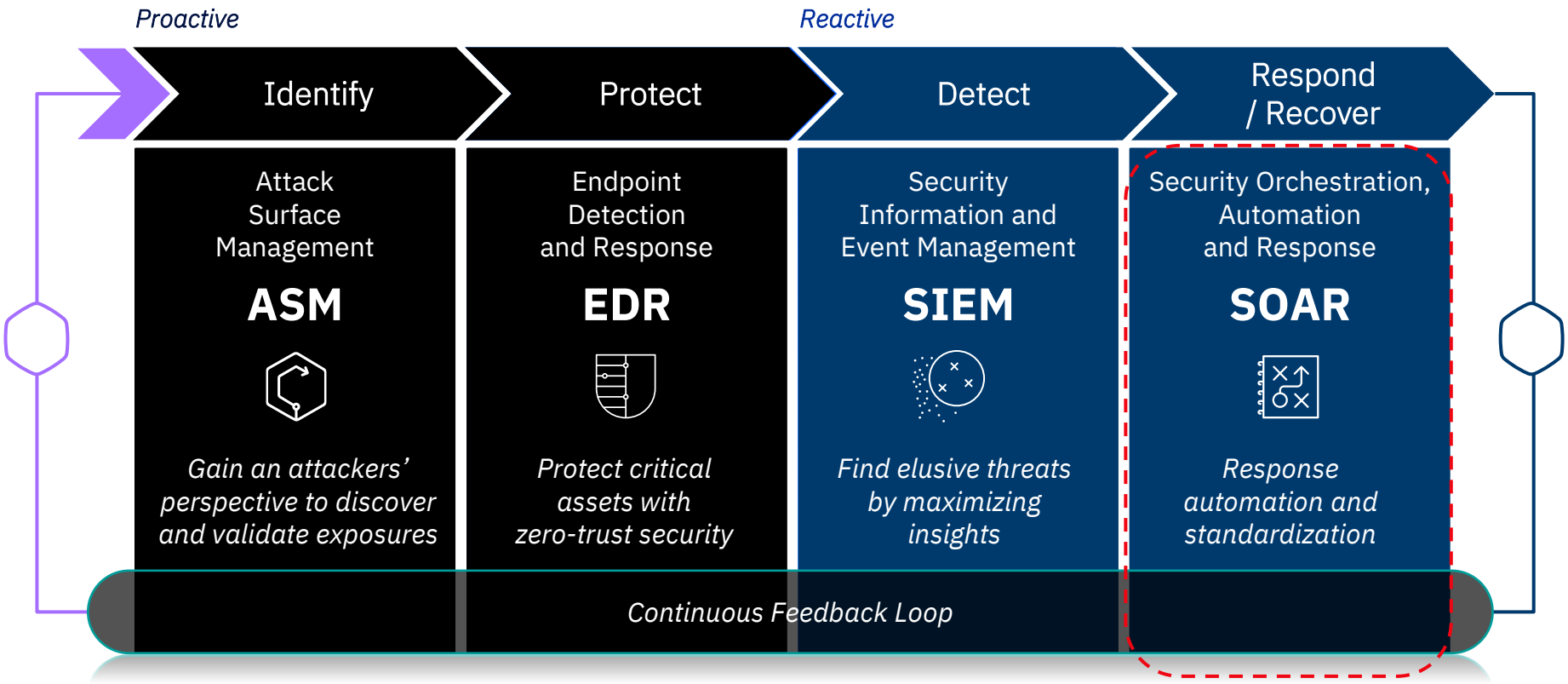
- Security Control Integration
- Ecosystem

Intelligent analytics for actionable insights into the most critical threats

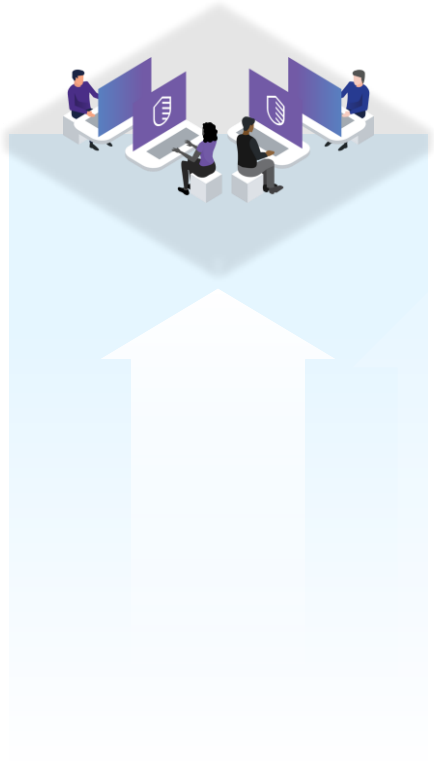


Insider Threats | External Threats | Cloud Risks | Critical Data | Vulnerabilities

Proactive Threat-Driven Defense Strategy



Organizations need to modernize threat detection and response



Eliminate silos

Gain visibility across data sources — from the cloud to the core

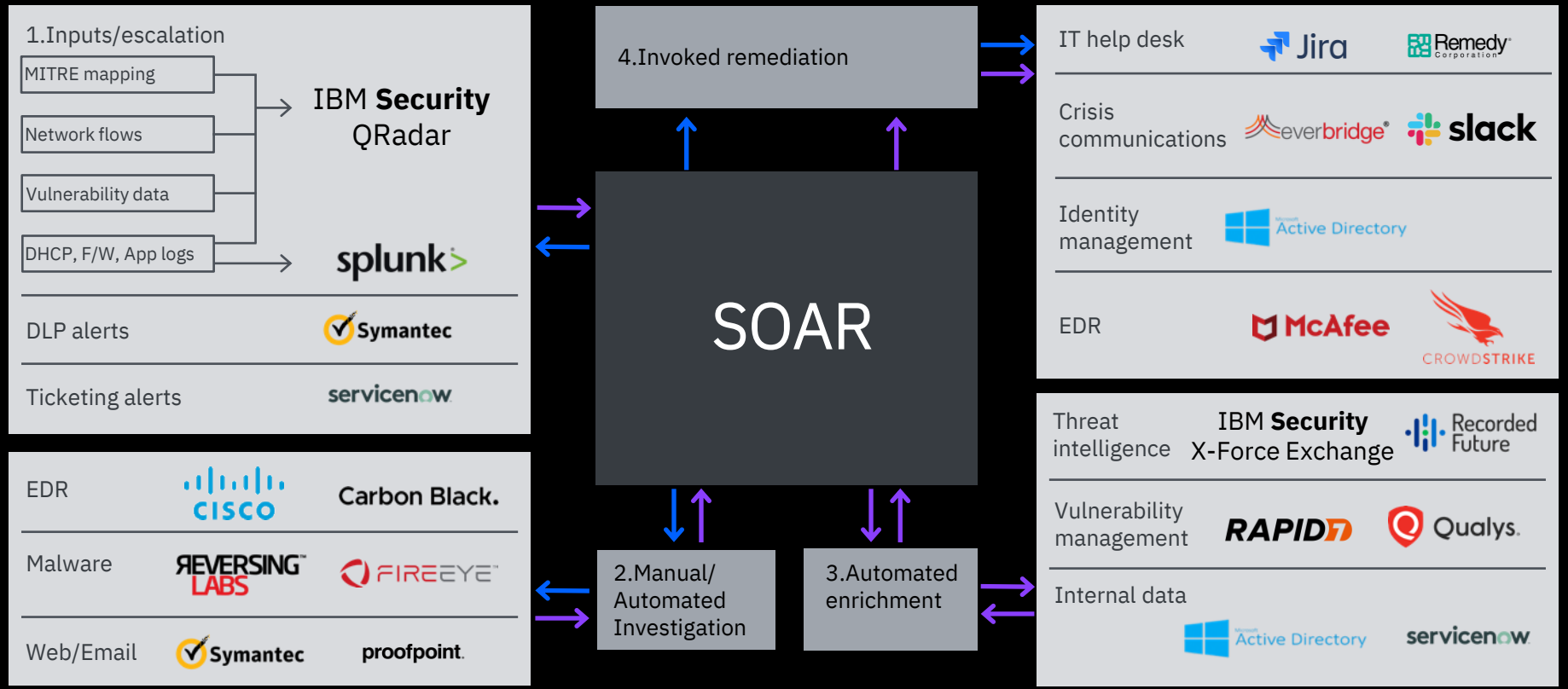
Unify workflows

Work without pivoting between tools

Automate work

Let machines do the heavy lifting — whether mundane tasks or complex analysis

Central hub for resolving security incidents



Moving critical applications to the cloud widens the attack surface

Security should span across all layers of your environment, with data as the center of the universe.

Cyber security and cyber resilience

Organizations need the means to respond and recover from an attack

Cyber security	Cyber resilience

Ideally, an organization should be both cyber secure and cyber resilient

Cyber security is about prevention; it's about trying to keep the bad actors out of your environment

Cyber resilience is about an organization's ability to continue operations despite a cyber-incident

Thank You