

Disrupting the kill chain

Philipp Hunold
Lead Cybersecurity Specialist
Western Europe



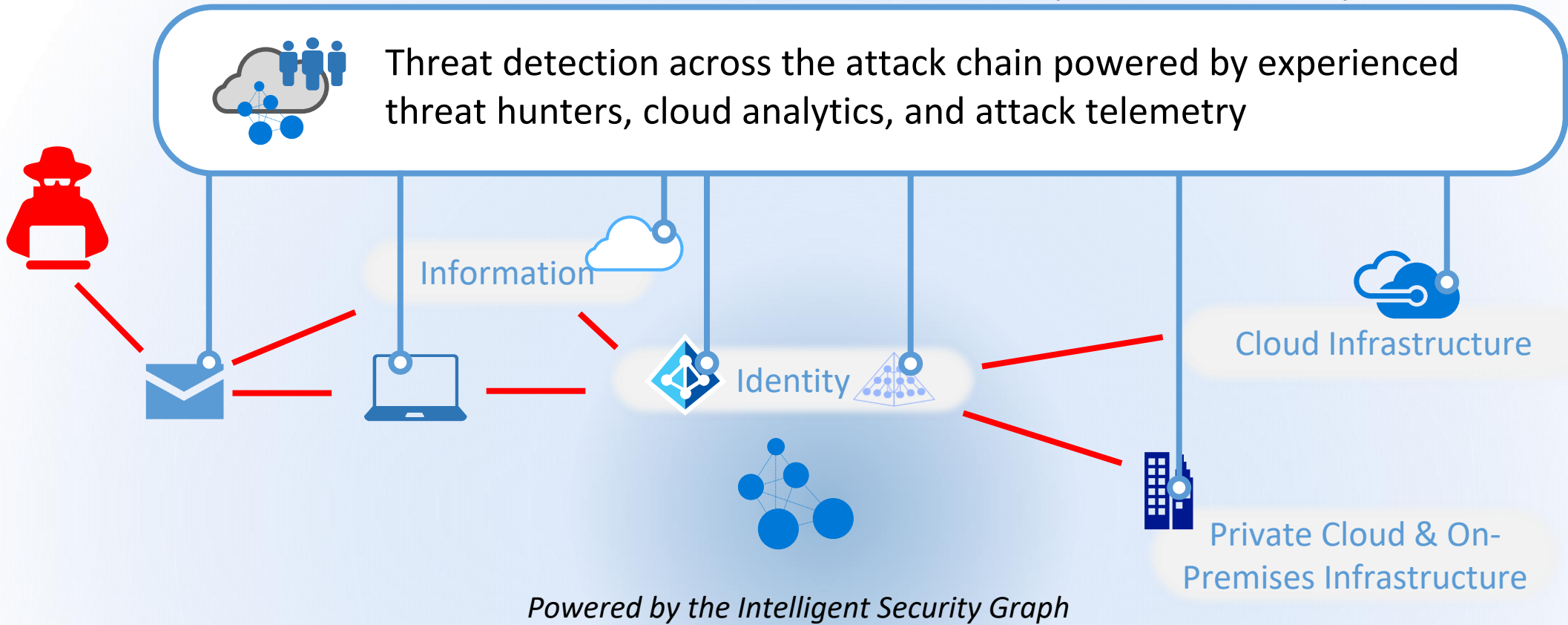
Microsoft
Security Summit

Vision Days / 28 Mars / Akalla



Detection Along the Kill Chain

Microsoft Threat Detection - *Everywhere they want to be*

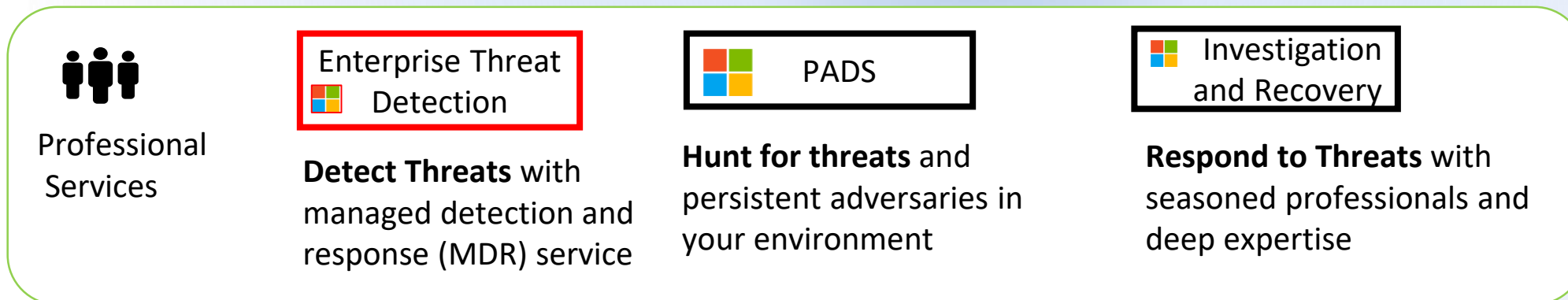
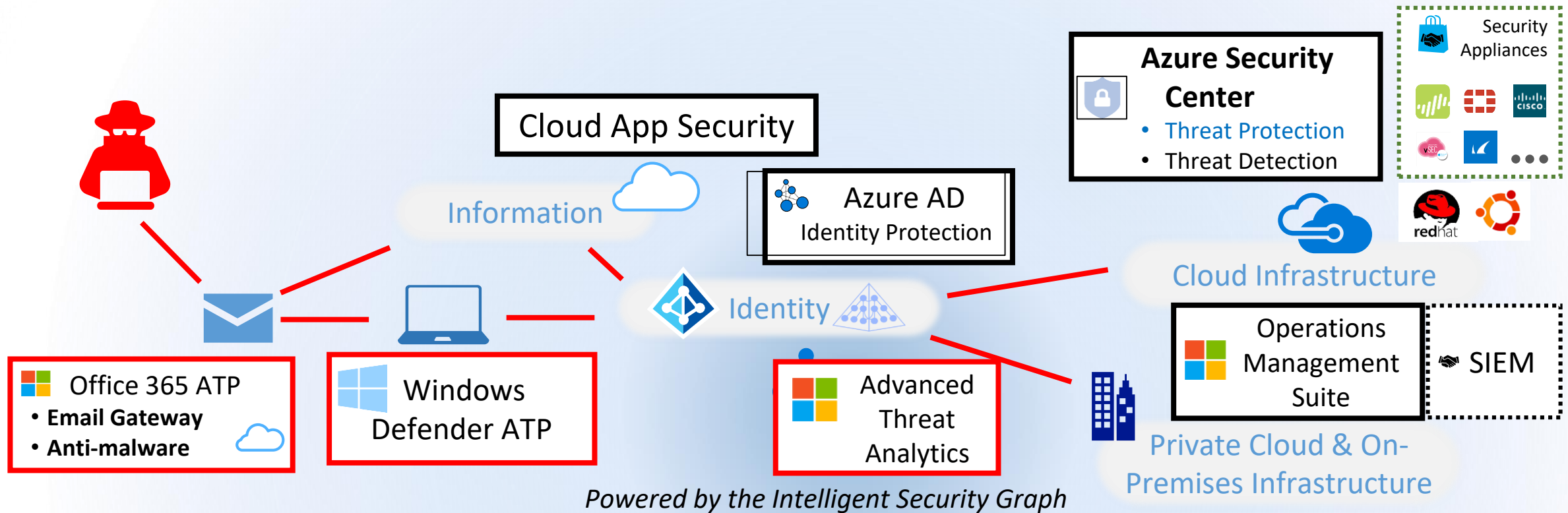


Expertise on demand through Professional services to assist with deployment, ongoing threat detection, incident response and recovery, and proactive hunting for advanced attackers



Easy to integrate with existing SIEM capabilities, security vendors already in Azure marketplace of security, and includes partnerships with industry

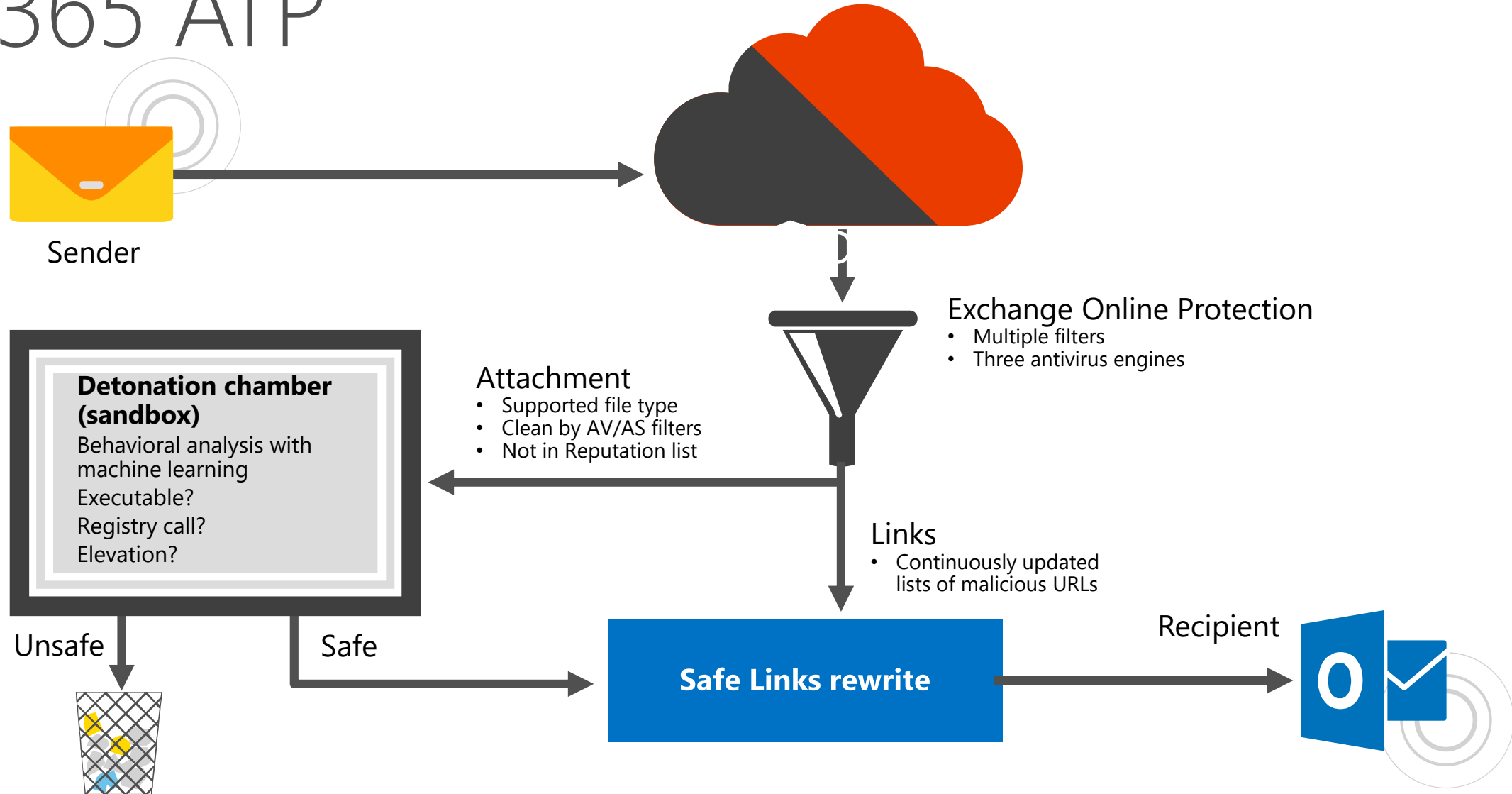
Microsoft Threat Detection - *Everywhere they want to be*



Delivery

Protect your frontdoor

O365 ATP



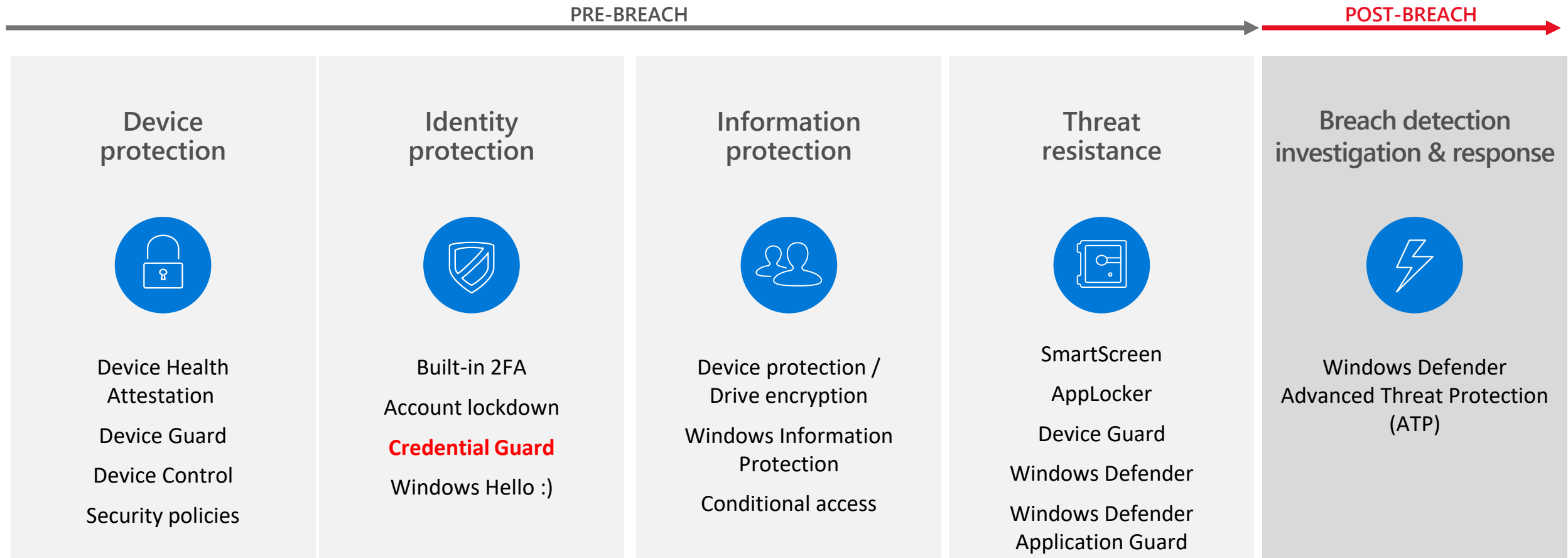
Exploitation

Installation

Command & Control

Protect your endpoints

ADDING A POST-BREACH MINDSET



Windows Defender Advanced Threat Protection

Detect advanced attacks and remediate breaches



Built in to Windows 10

No additional deployment & infrastructure.
Continuously up-to-date, lower costs.



Behavior-based, cloud-powered breach detection

Actionable, correlated alerts for known and unknown adversaries.
Real-time and historical data.



Rich timeline for investigation

Easily understand scope of breach. Data pivoting
across endpoints. Deep file and URL analysis.



Unique threat intelligence knowledge base

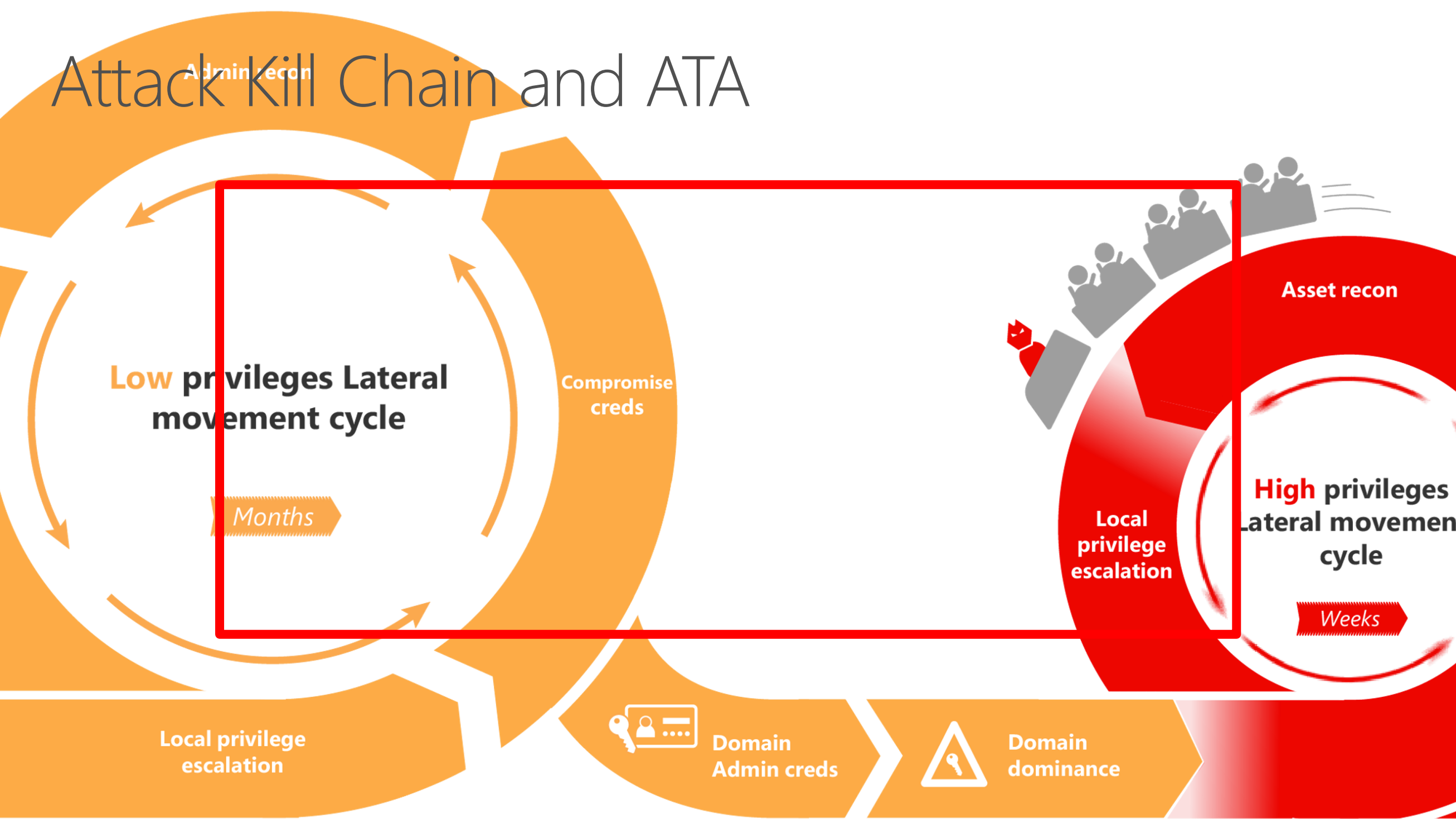
Unparalleled threat optics provide detailed actor profiles
1st and 3rd party threat intelligence data.



Privilege Escalation
Lateral Movement
Domain Dominance

Protect your Identities

Attack Kill Chain and ATA



Advanced Threat Analytics (ATA)

- Account enumeration
- Net Session enumeration
- DNS enumeration
- Abnormal resource access



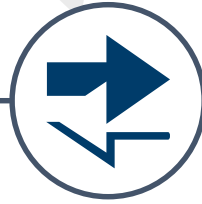
Reconnaissance

Compromised
Credential



- Abnormal working hours
- Brute force using NTLM, Kerberos or LDAP
- Sensitive accounts exposed in plain text authentication
- Service accounts exposed in plain text authentication
- Honey Token account suspicious activities
- Unusual protocol implementation
- Malicious Data Protection Private Information (DPAPI) Request

- Pass-the-Ticket
- Pass-the-Hash
- Overpass-the-Hash
- Abnormal authentication requests
- Abnormal resource access



Lateral
Movement

Privilege
Escalation



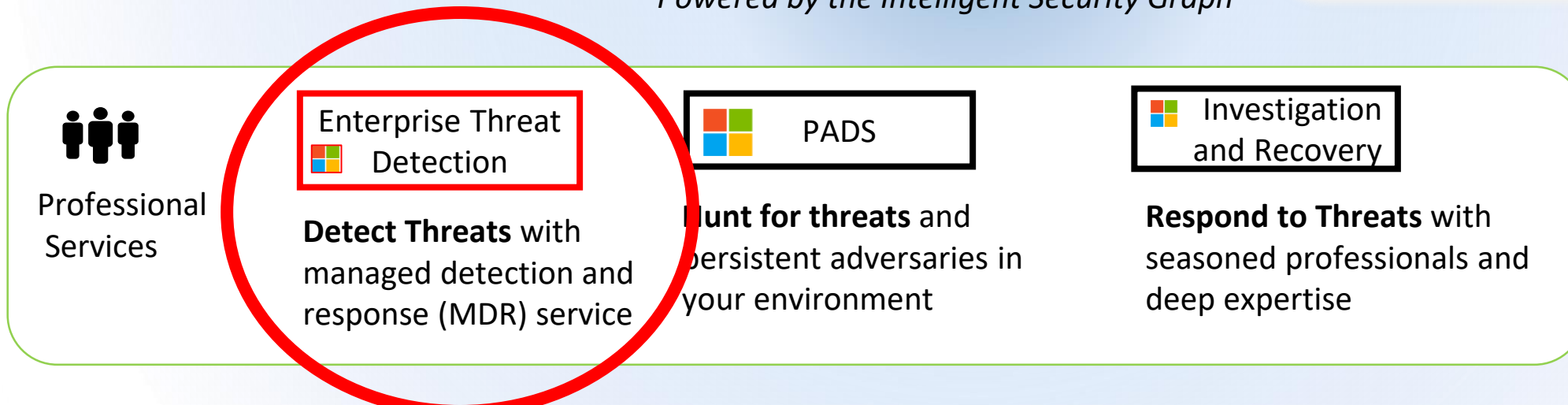
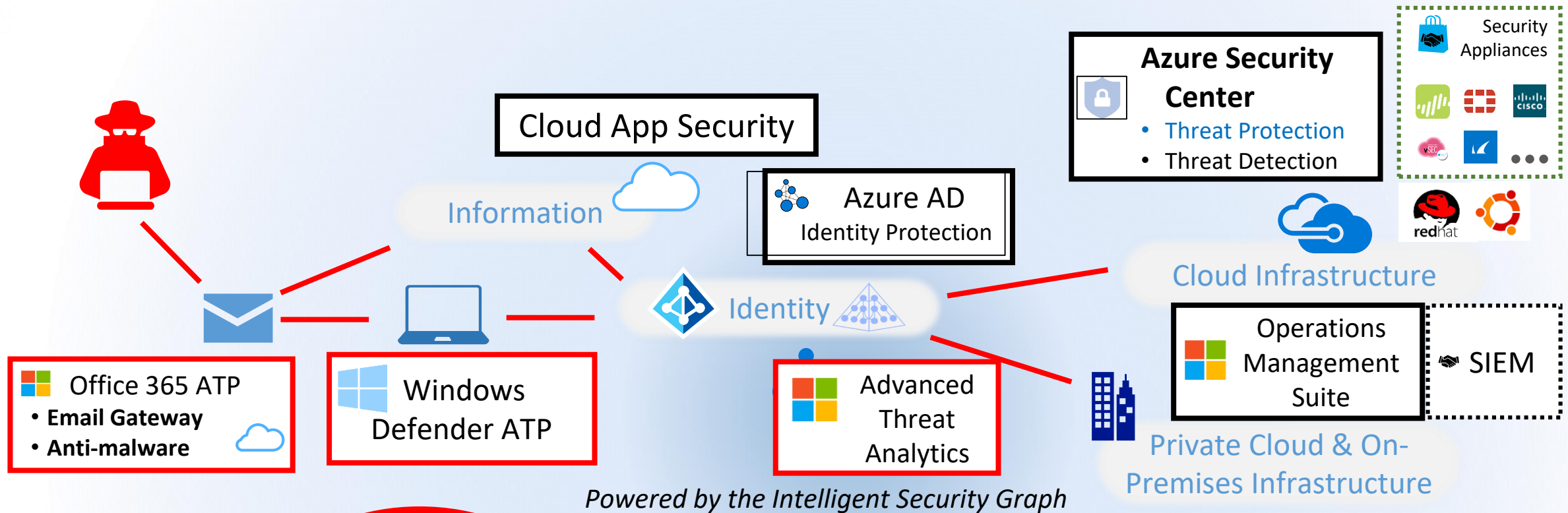
- MS14-068 exploit (Forged PAC)
- MS11-013 exploit (Silver PAC)

- Skeleton key malware
- Golden ticket
- Remote execution
- Malicious replication requests



Domain
Dominance

Microsoft Threat Detection - *Everywhere they want to be*

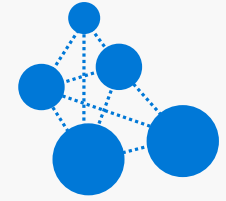


Enterprise Threat Detection

"Cybersecurity Analyst for hire"

Enterprise Threat Detection (ETD)

A managed threat detection service



Advanced Threat Detection with Unique Microsoft Capabilities

Industry Leading Telemetry

Advanced Technology

Deep Cybersecurity Experience

Provides Deep Expertise on demand

Microsoft Platform Expertise

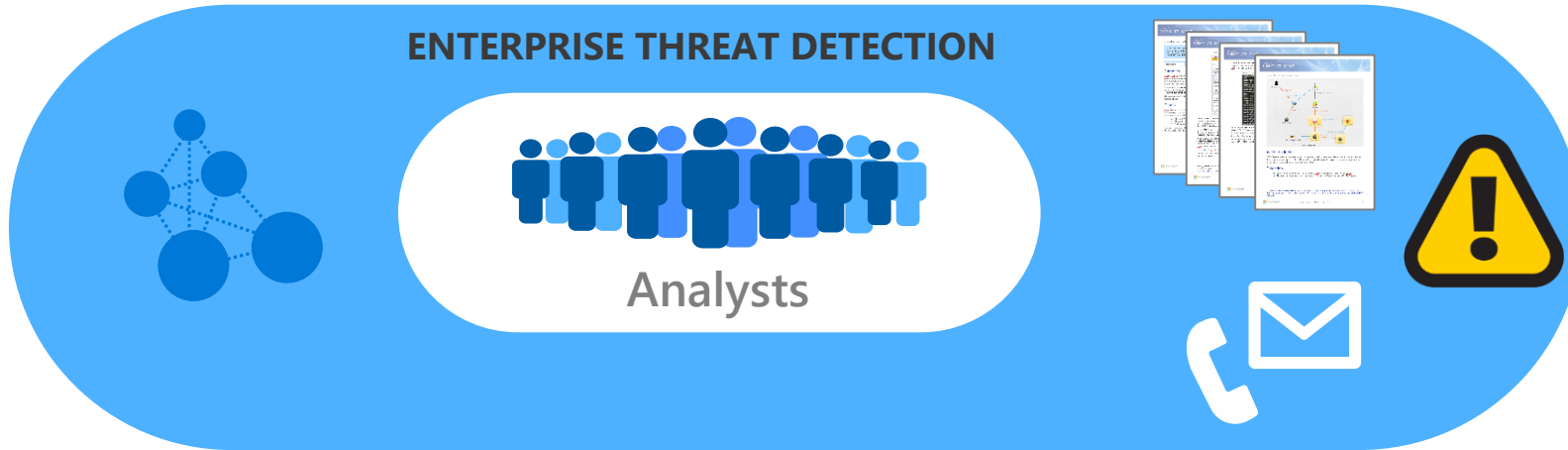
Threat Detection

Combines Machine + Human Analysis for Power and Accuracy

Offered as an annual subscription

Enterprise Threat Detection

Managed Threat Detection Service



- **Alerts** on urgent detections
- **Reports** on additional detections and findings
- **Phone** and **Email** consulting with expert analysts

- Analysis and investigation support using
 - Data and Analytics from Microsoft's Intelligent Security Graph
 - Data from your deployment of Microsoft detection technologies
 - Windows Operating System
 - Windows Defender Advanced Threat Protection (ATP)
 - Advanced Threat Analytics (ATA)
 - Deep expertise on Microsoft platform, threat detection tools, and cyber attacks

Integrating Data

