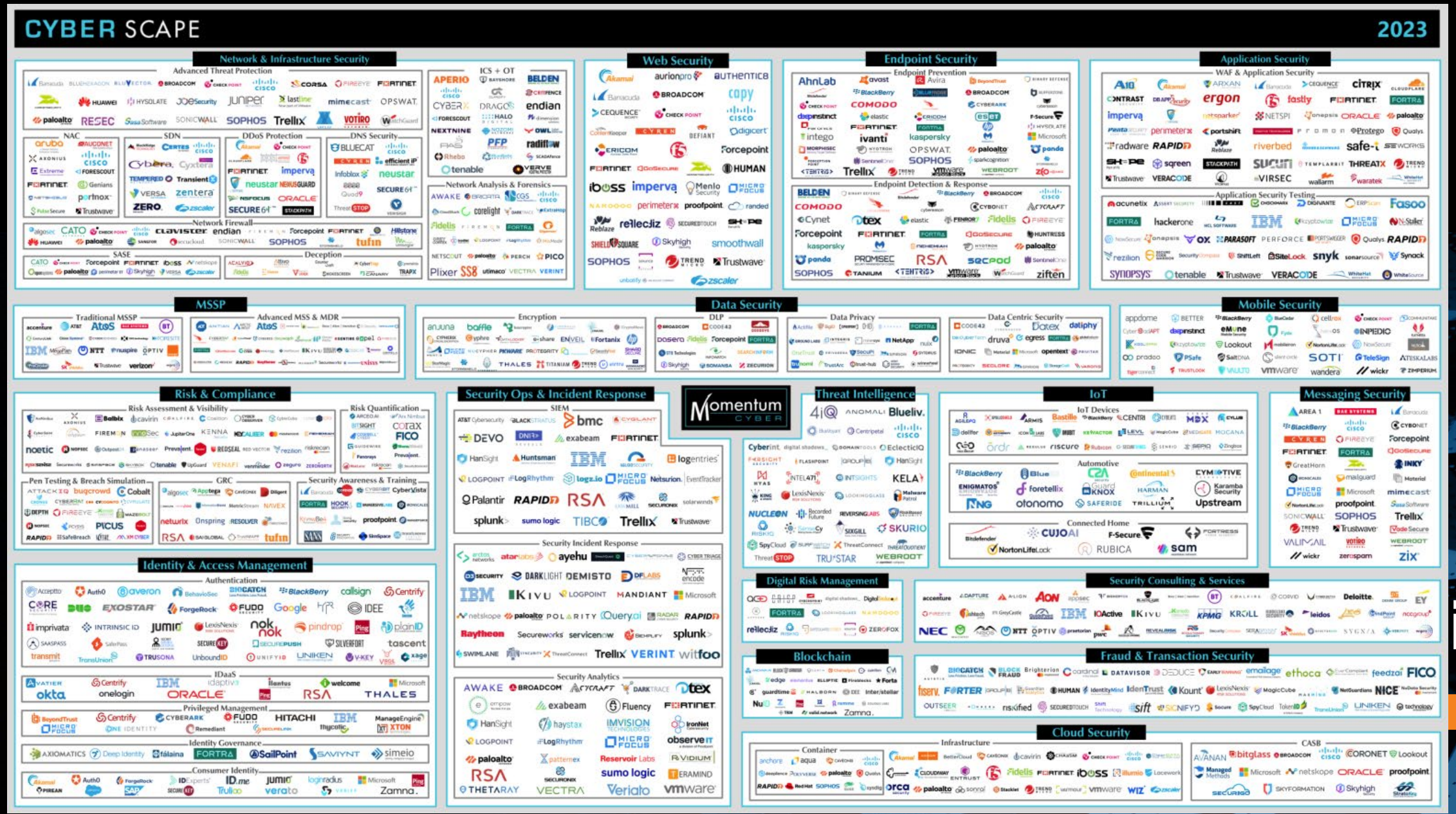
ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

Arctic Wolf

END CYBER RISK

Christian Wagner
Senior Sales Engineer Enterprise
Christian.Wagner@arcticwolf.com



Ending Cyber Risk

Security Operations

Angestrebtes Sicherheitslevel

Arctic Wolf Security Operations

Lücke

Die meisten Firmen sind hier

BASIS

Passwörter / AD

Patch Management

Backups

PERIMETER

Firewalls

SPAM / Web Filters

WAF / Proxy

ERWEITERTE VERTEIDIGUNG

Endpoint (NGAV, EDR)

DLP / SSL Inspection

Anti-DDoS / IPS / CASB

WIDERSTANDS-FÄHIGKEIT

Proaktiv

Konform (ISO etc)

Versicherbar

ARCTIC WOLF

Arctic Wolf Security Operations

We Make Security Work

6,000+
Kunden

24x7
In deutsch

700+
Security Engineers

5
Datacenter weltweit

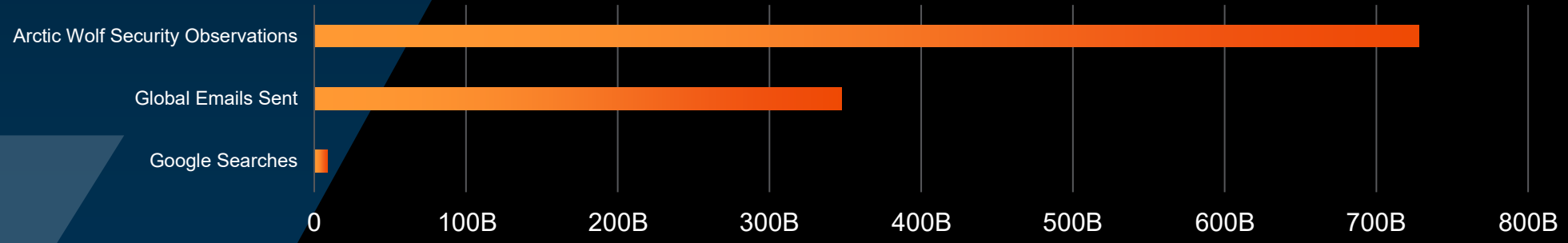
5.1+
Milliarden Logzeilen pro Tag

3.5M+
aktive Agenten and 25,000+ Sensoren

12M+
Schwachstellen werden pro Woche identifiziert

600+
Incident Response Fälle pro Jahr

Global Volumes Per Day



Arctic Wolf Security Operations

We Make Security Work

6,000+
Kunden

24x7
In deutsch

700+
Security Engineers

5
Datacenter weltweit

5.1+
Milliarden Logzeilen pro Tag

3.5M+
aktive Agenten and 25,000+ Sensoren

12M+
Schwachstellen werden pro Woche identifiziert

600+
Incident Response Fälle pro Jahr

RED HERRING 100 WINNER N. AMERICA

Gartner COOL VENDOR

CHANNEL PARTNERS SECURITY AWARDS 2018 WINNER

500 Technology Fast 500 2019 NORTH AMERICA Deloitte.

SC 2018 awards Winner

GENERAL DATA PROTECTION REGULATION GDPR READY

DSGVO konform

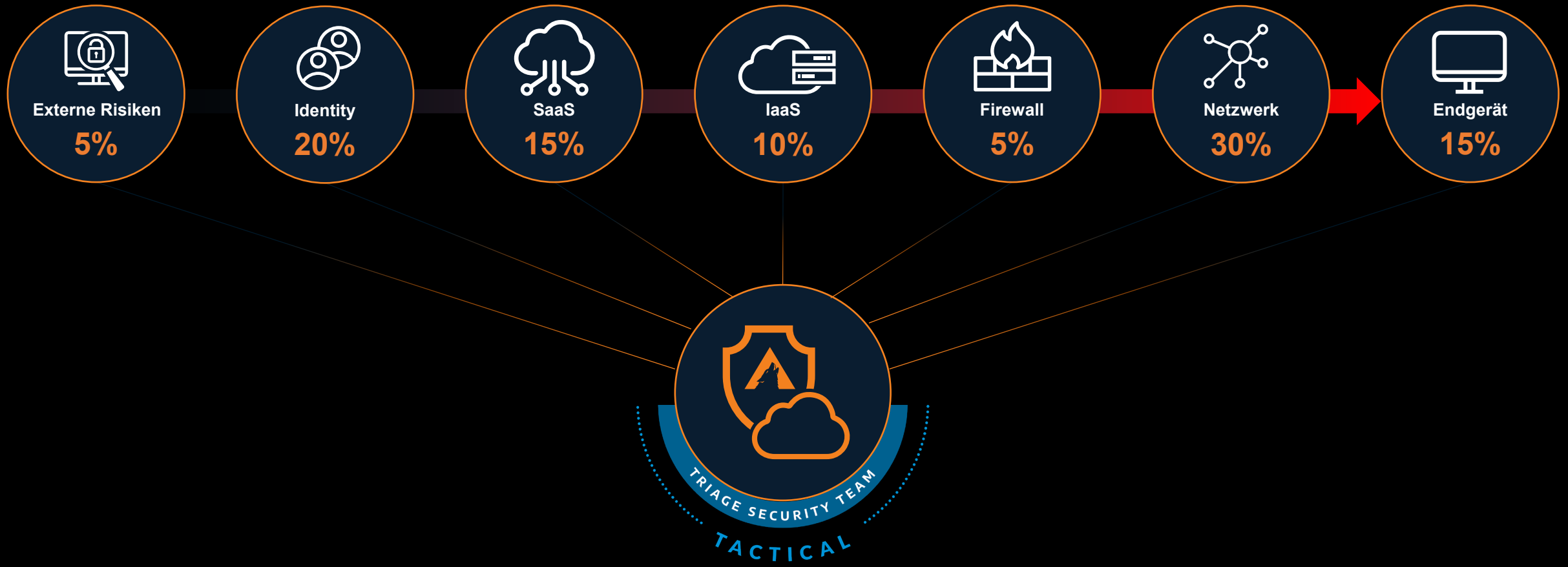
Privacy Shield Compliant

SOC 2 TYPE 2 AICPA SOC

ARCTIC WOLF

Security Operations Cloud

Cyberattacke via Cloud & Identity



ARCTIC WOLF LABS

KI und Data Science

Threat Intelligence und Security Research

Detection & Response Engineering

Security Posture Engineering

Arctic Wolf Security Operation Teams

Das Triage Security Team überwacht ihre Umgebung 24x7 um Angriffe zu indentifizieren und Sie bei der Behebung unterstützen

Das Concierge Security® Team entwickelt eine auf Sie angepasst Security Journey, um ihren Schutz kontinuierlich zu verbessern.

AW Security Operations Workflow

Das Arctic Wolf Triage Team		Kunden	CONCIERGE SECURITY TEAM	
eben & suchen	Eskalieren	Kunden Portal	Beheben & Wiederherstellen	Security Journey

Arctic Wolf Security Journey

Onboarding Team & Kunde

CST und Kunde

Phase 1

Onboarding
Ca. 30 Tage

Erbracht durch das **Onboarding Team**

- Projekt Kick Off & Technical Kick Off
- Vorstellung des Portals
- Sensoren werden verschickt
- Konfiguration der Log-Quellen, ausrollen des Agenten

Phase 2

Die ersten 90 Tage
Go Live

Das **Concierge Security Team** startet die Zusammenarbeit mit dem Kunden

Meetings alle vier Wochen

Triage Team übernimmt 24/7 Monitoring

- Unlimitierte „Guided Incident Response“

Phase 3

Dauerzustand

Kontinuierlicher Zugriff auf das Concierge Security Team

Security Journey – Regelmässige Termine

#1 #2 #3 #...

Security Assessment der Kundenumgebung

Kennenlernen, Businessprozesse verstehen

Überprüfung von
- Log-Quellen
- Firewalls
- Active Directory
- Endgeräte

Finetuning der Plattform

Monatlich Externe **Vulnerability Assessments und Account TakeOver Analyse**

Security Bulletins & Threat Hunting bei Mega Events

SPiDRs *(Security Posture in Depth Reviews)*

Angepasst für jeden Kunden
- Bewertung – Lücken/Risken
- Konfigurations-Checks – Services (z.B. AD)
- Best Practice – Empfehlungen

Reporting

SLO (critical incident):
- Outbound Response 30min
- Inbound Response 5min

Solutions Agreement and Terms:
https://arcticwolf.com/terms/

Arctic Wolf Security Operations

Arctic Wolf Platform

Die Arctic Wolf-Plattform sammelt alle Telemetriedaten in der Cloud zur Speicherung, Anreicherung und Analyse. Sie deckt die Bereiche Endpunkt, Netzwerk, Cloud, Anwendungen, Identität und menschliche Angriffsflächen ab.

Arctic Wolf Triage Team

Ein 24x7-Team von Sicherheitsexperten, die von der Arctic Wolf-Plattform generierte Alarme untersuchen. Dieses Team bietet taktische Unterstützung und Anleitung für Sie während Sicherheitsereignissen.

Arctic Wolf CST

Das Concierge Security Team erarbeitet mit Ihnen zusammen ein Sicherheitskonzept, dass den Zielen des Unternehmens entspricht und gleichzeitig Möglichkeiten aufzeigt, die Sicherheitslage im Laufe der Zeit zu verbessern.

Arctic Wolf vs. Standard MDR

Arctic Wolf ist mehr als Managed Detection & Response

- 24x7x365 aus Deutschland von deutschen Experten
- Alle Logs werden DSGVO-konform gespeichert
- Breiteste Visibilität – **Herstellerunabhänige** Auswertung aller relevanten Logs
  AD, DNS, DHCP, Firewall, Endgeräte, IDS für Internet-Traffic und Cloud-Komponenten (IaaS, SaaS)
  DarkWeb Scanning & External Vulnerability Assessments
- **Concierge Security Team** : Zugriff auf zwei Security-Consultants, die Ihnen strategisch zur Seite stehen und den Service auf Ihre Bedürfnisse anpassen
- Schwarmintelligenz von >6000 Kunden
- Industrieführenden SLA von <30 Minuten für Identifikation, Analyse und detaillierte Lösungsbeschreibung
- **Flatrate** - Einfaches, verständliches und planbares Preismodel

Ransomware Attack – Local Government

Arctic Wolf Platform | Arctic Wolf Triage Team | Customer | CST

05:23

Source: Active Directory

[USER1] user account begins logging into multiple systems

05:26

Source: Arctic Wolf Sensor

- HTTP header information containing outbound communication with xx.xxx.230.236 detected, possible C2
- Suspected PowerShell Empire activity detected on [SERVER1]

05:28

Investigation Triggered

- C2 traffic is correlated with PowerShell Empire activity on [SERVER1]
- The incident is escalated to Triage Team Level 3 forensics dashboard with Urgent status

05:29

Investigation Starts

- Triage team begins investigation and finds activity within Active Directory logs of [USER1] user logging into many systems in a short amount of time.
- Confirms network and PS Empire alerts are a true positive and assess scope of attack

05:48

Incident Ticketed

Investigation concludes and Triage Team contacts customer with a CSV detailing the C2 traffic as well as logins which preceded these connections. Gives recommendation to:

- Contain the device / disconnect from network
- Change passwords for the [USER1] accounts / Service accounts
- Run AV scan on endpoints

06:13

Remediation

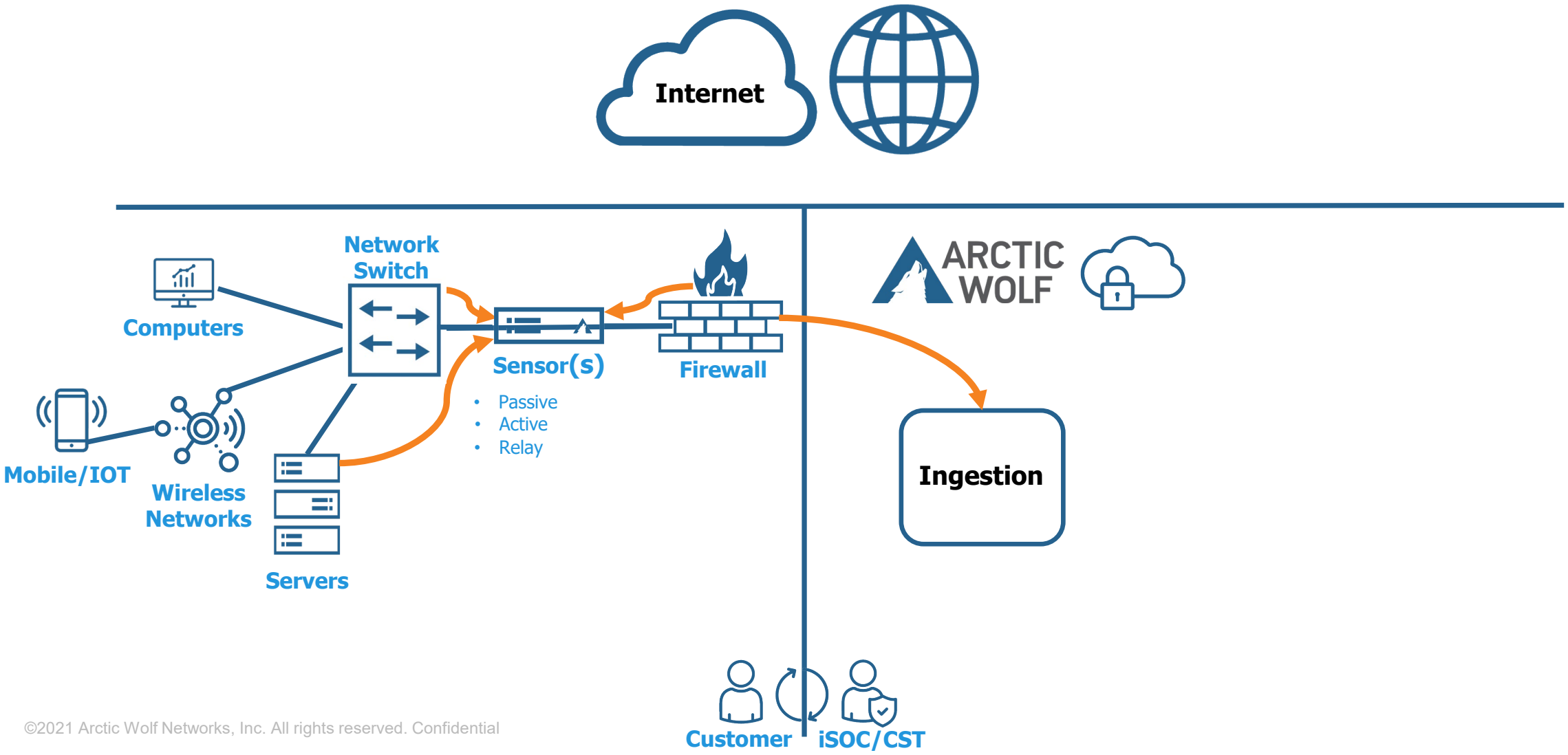
Customer responds that the device has been contained and passwords reset

Security Journey

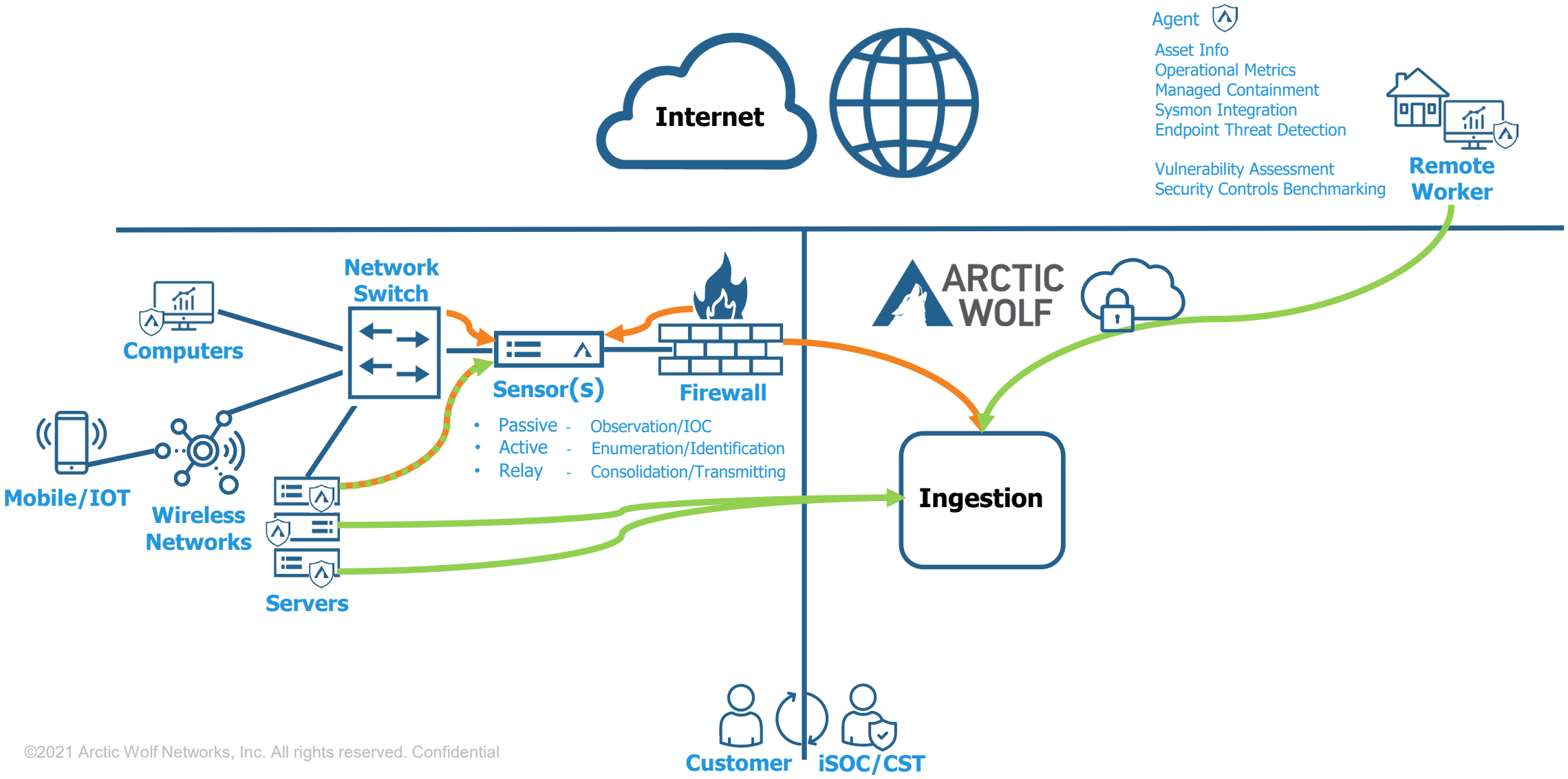
CST works with customer to identify areas of improvement for their security posture:

- Implement principle of least privilege for remote tools
- Geofence firewalls
- Enable MFA
- Setup GPO to block use of PowerShell
- Install Arctic Wolf Agent with Sysmon on all machines

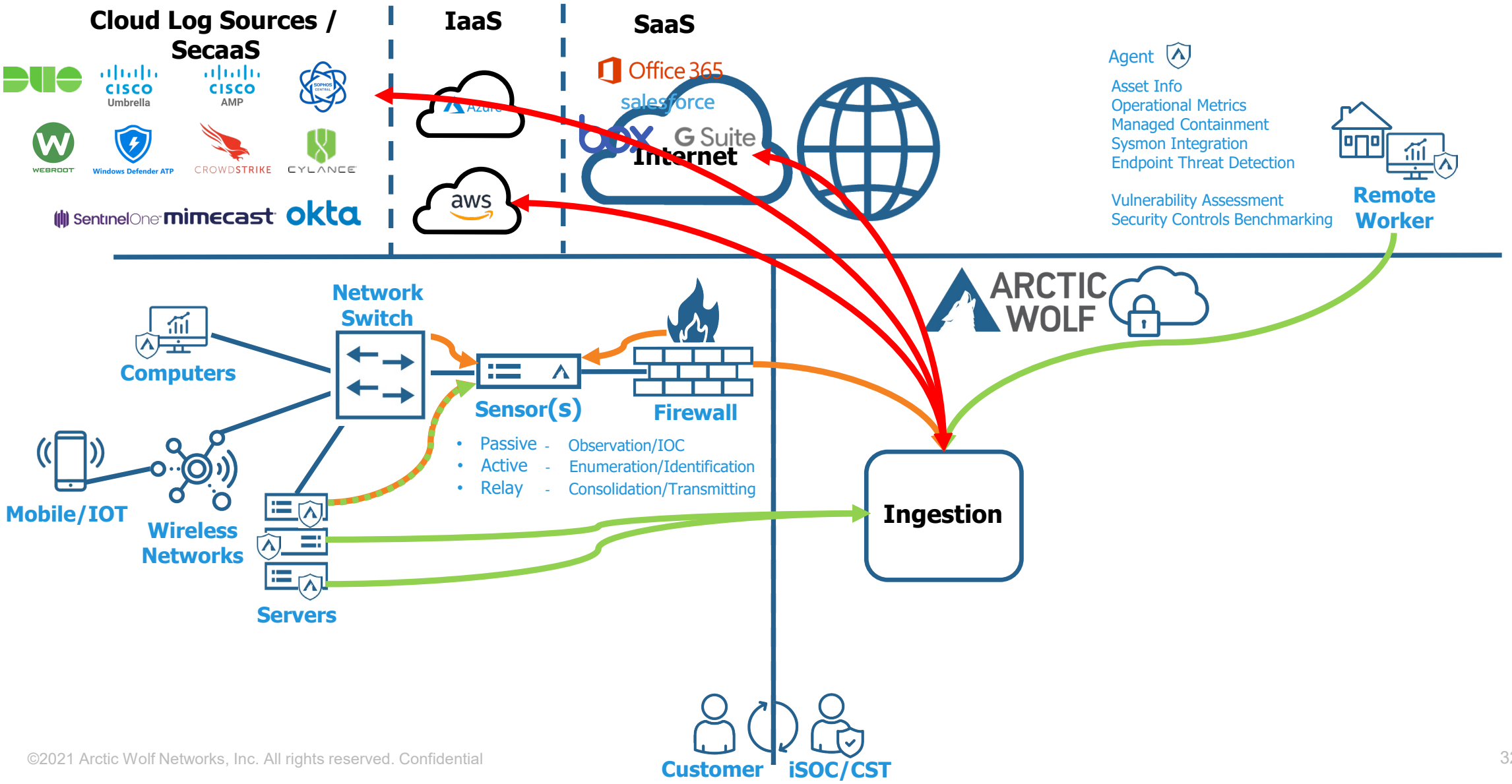
What Do Sensors Do?



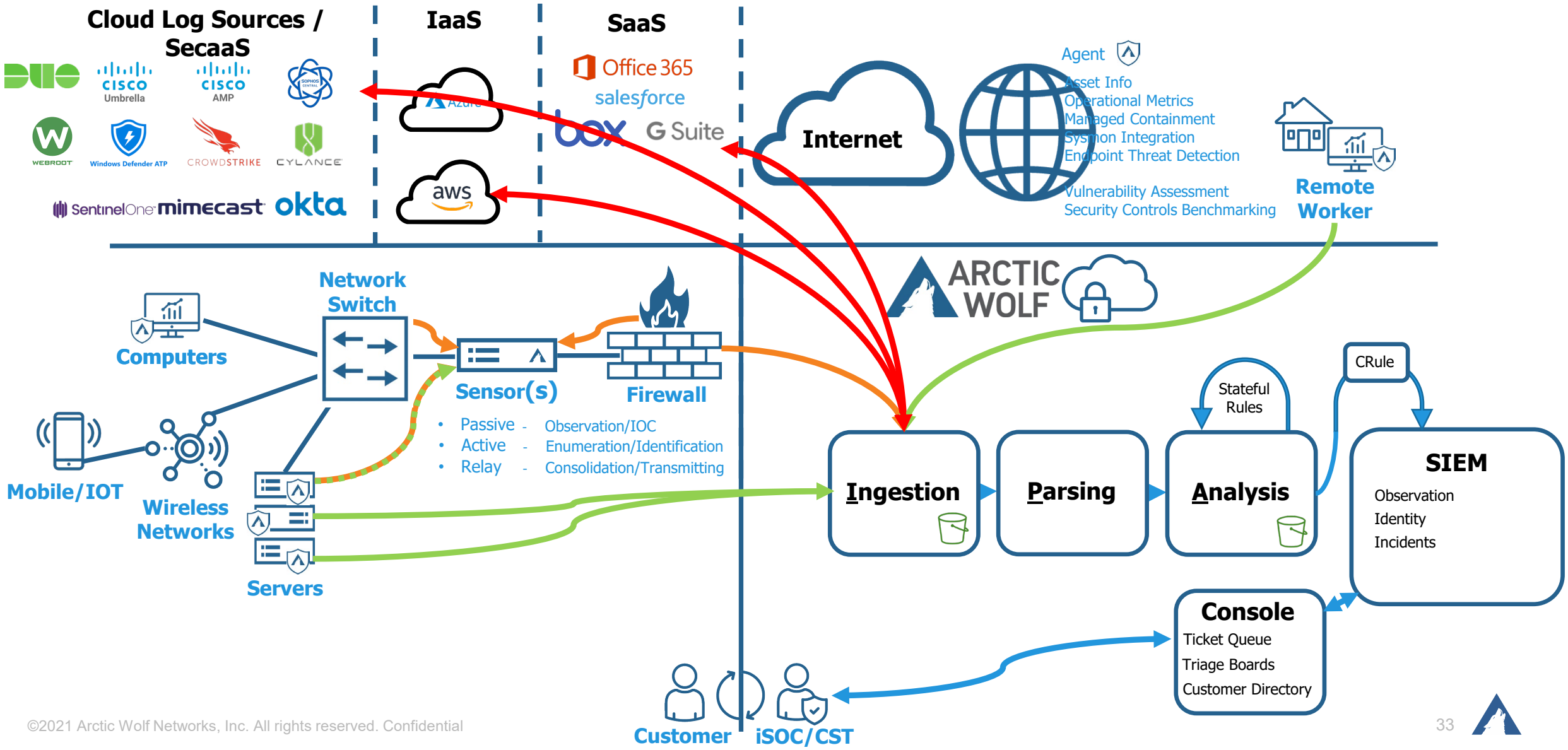
What Do Agents Do?



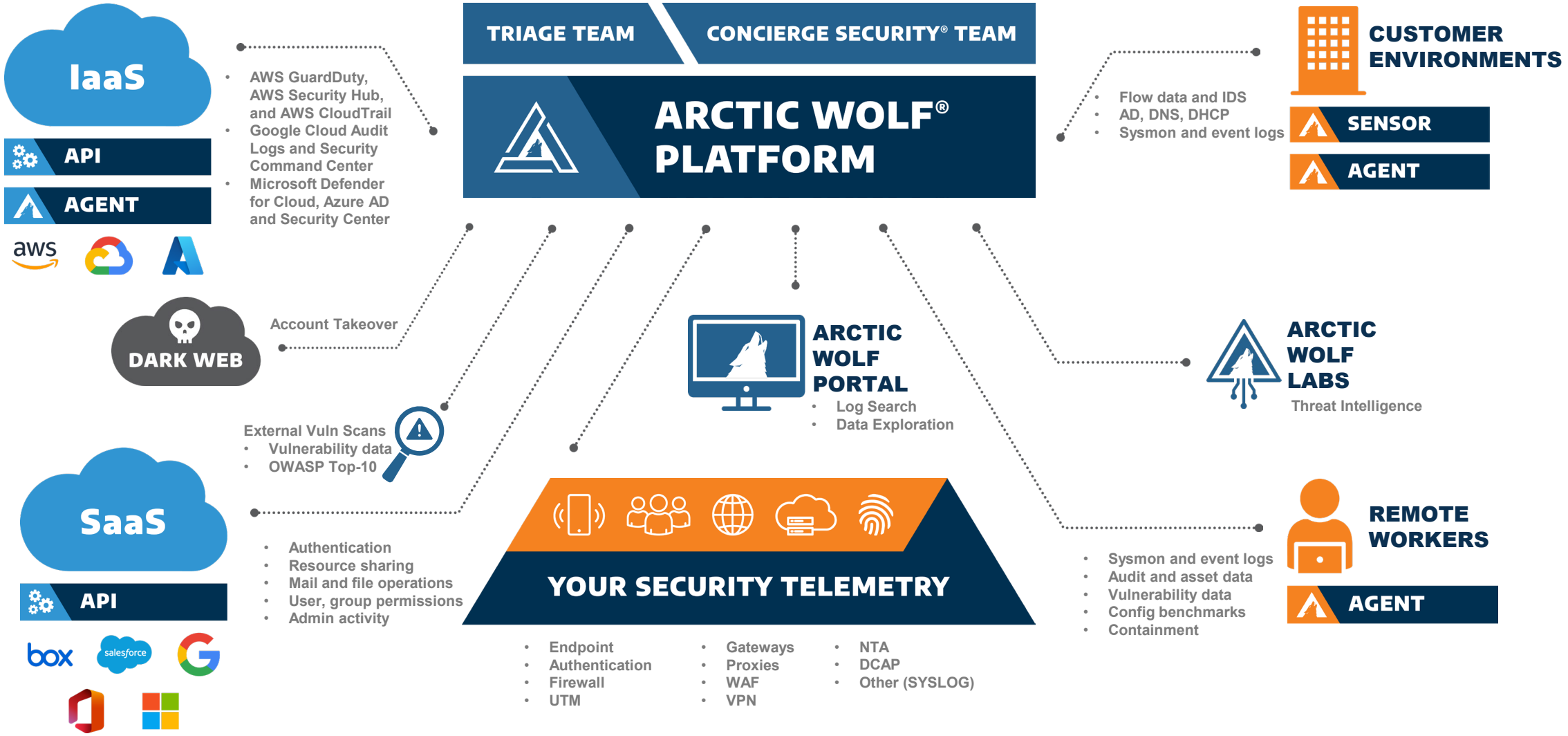
What Does Cloud Threat Detection Do?



How Does The Analysis Pipeline Work?



Managed Detection and Response Architecture

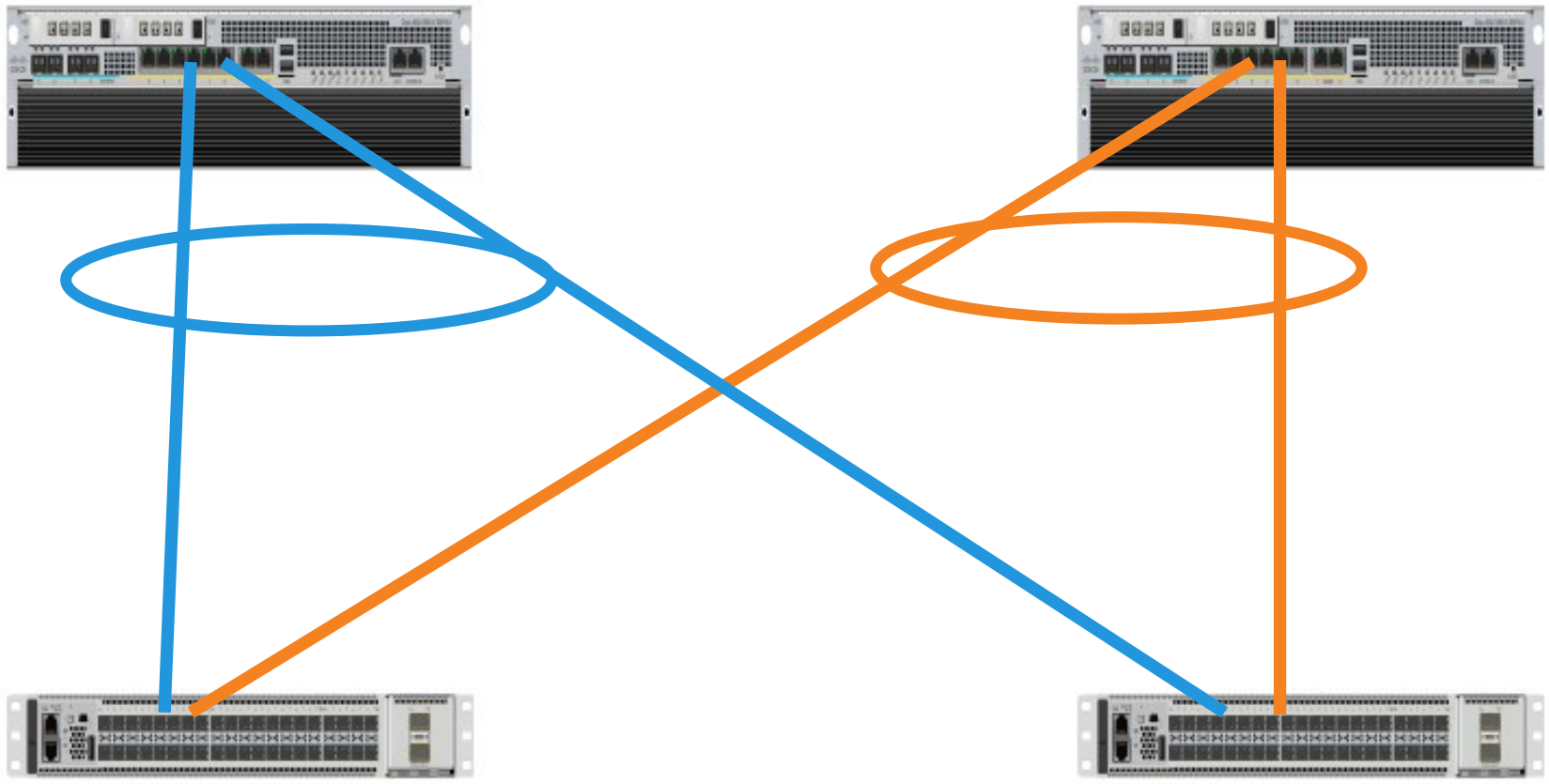


Client HA Architecture

High Availability Firewalls

Port Channels/Aggregated links for resiliency - Not increased throughput potential

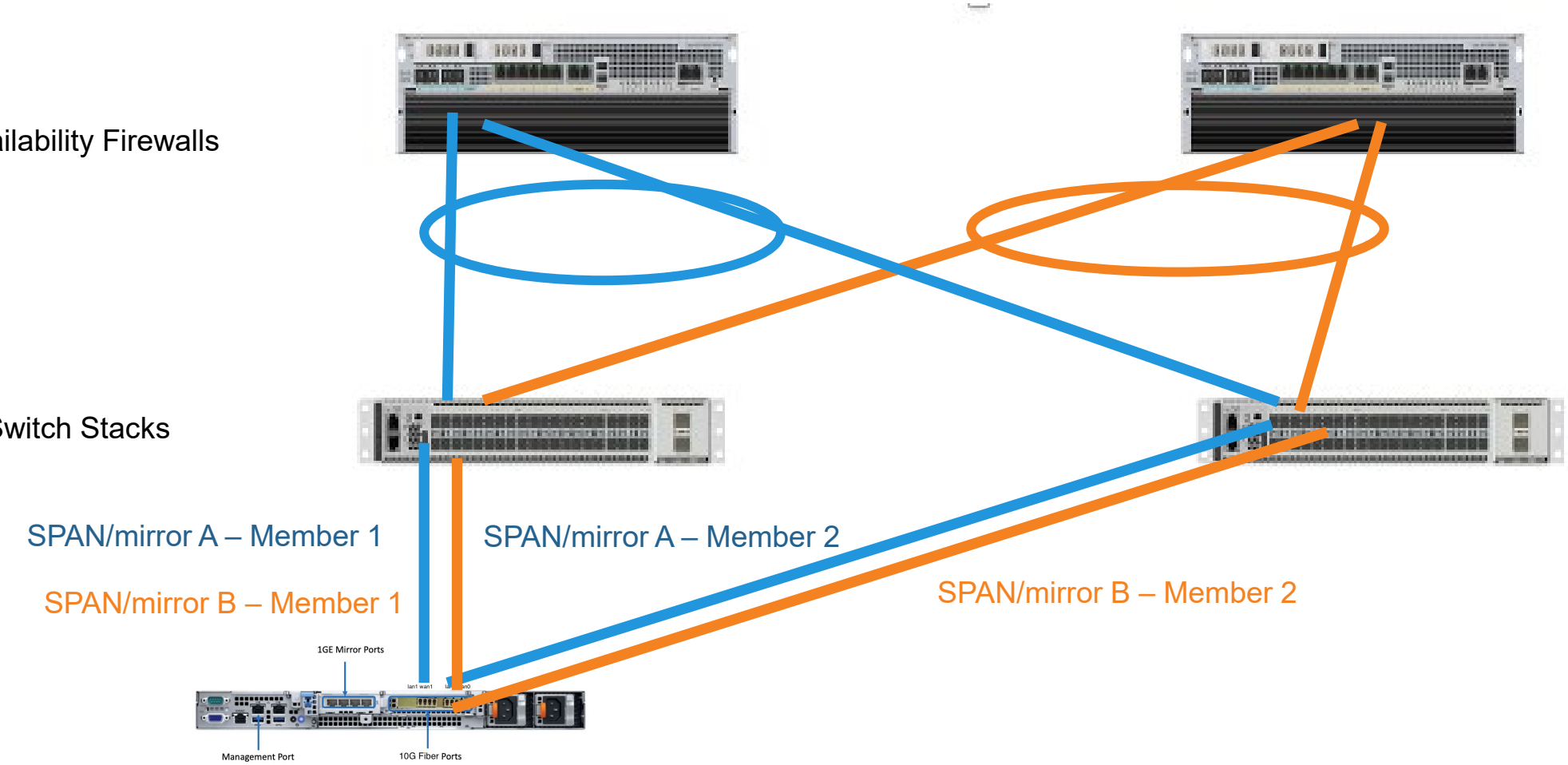
Redundant Switch Stacks



Client HA Architecture – Single Sensor

High Availability Firewalls

Redundant Switch Stacks



Client HA Architecture – Dual Sensors