END CYBER RISK

Cybersecurity should reduce cyber risk

87%

of security leaders believe their organizations is falling short in addressing cyber risk.

Source: IDG Security Priorities Study 2020

Cybersecurity has an **effectiveness** problem.

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Some Observations

Why aren't security leaders feeling confident?

LIKELIHOOD OF AN INCIDENT

IMPACT OF AN INCIDENT

59%
Organizations breached in a year

40 day
Increase to patch 'critical' vulnerabilities

$8.6M
Average cost of a data breach in the US

206 days
Mean Time To Detect

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Switch your thinking from a tools mindset to an operational mindset

Optimize

Optimize your existing tech stack and send to the cloud

Embrace Security Operations

Focus on a complete security operations framework with broad coverage across attack types and attack surfaces

Build Resilience

Add expert guidance, 24x7 protection, and implement tactical and strategic actions across the security operations framework

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Security Operations Outcomes that Matter to You

IDENTIFY

You need an accurate picture of your threat posture and exposures across all attack surfaces

PROTECT

You need confidence that you have things secured & configured properly

DETECT

You need the ability to spot threats early; both commodity and APTs

RESPOND

You need to respond to threats and intrusions quickly and efficiently

RECOVER

You need experience and capabilities to ensure you can get back to business - fast & implement improvements

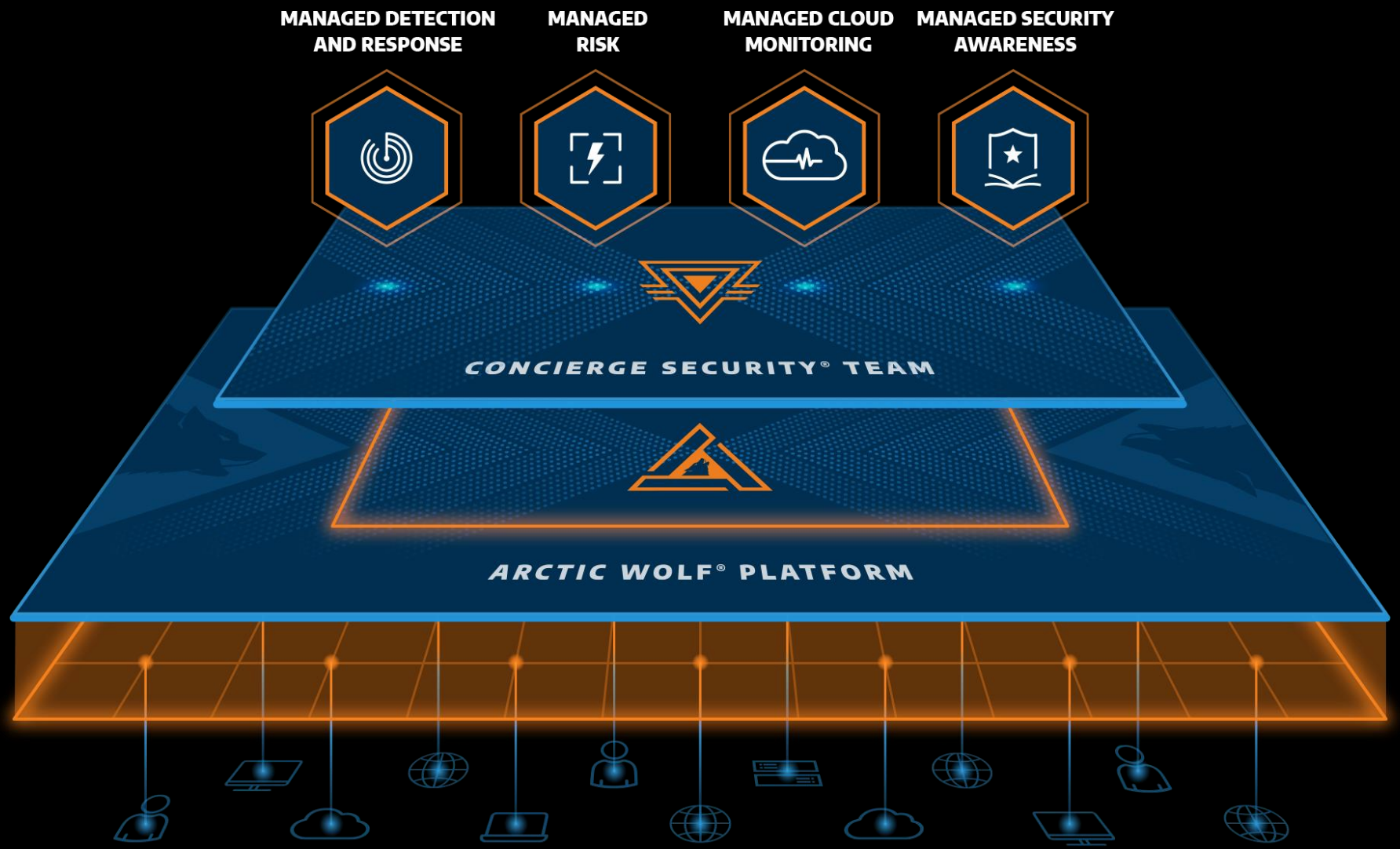
Security Operations Framework

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

ARCTIC WOLF
SECURITY OPERATIONS PLATFORM

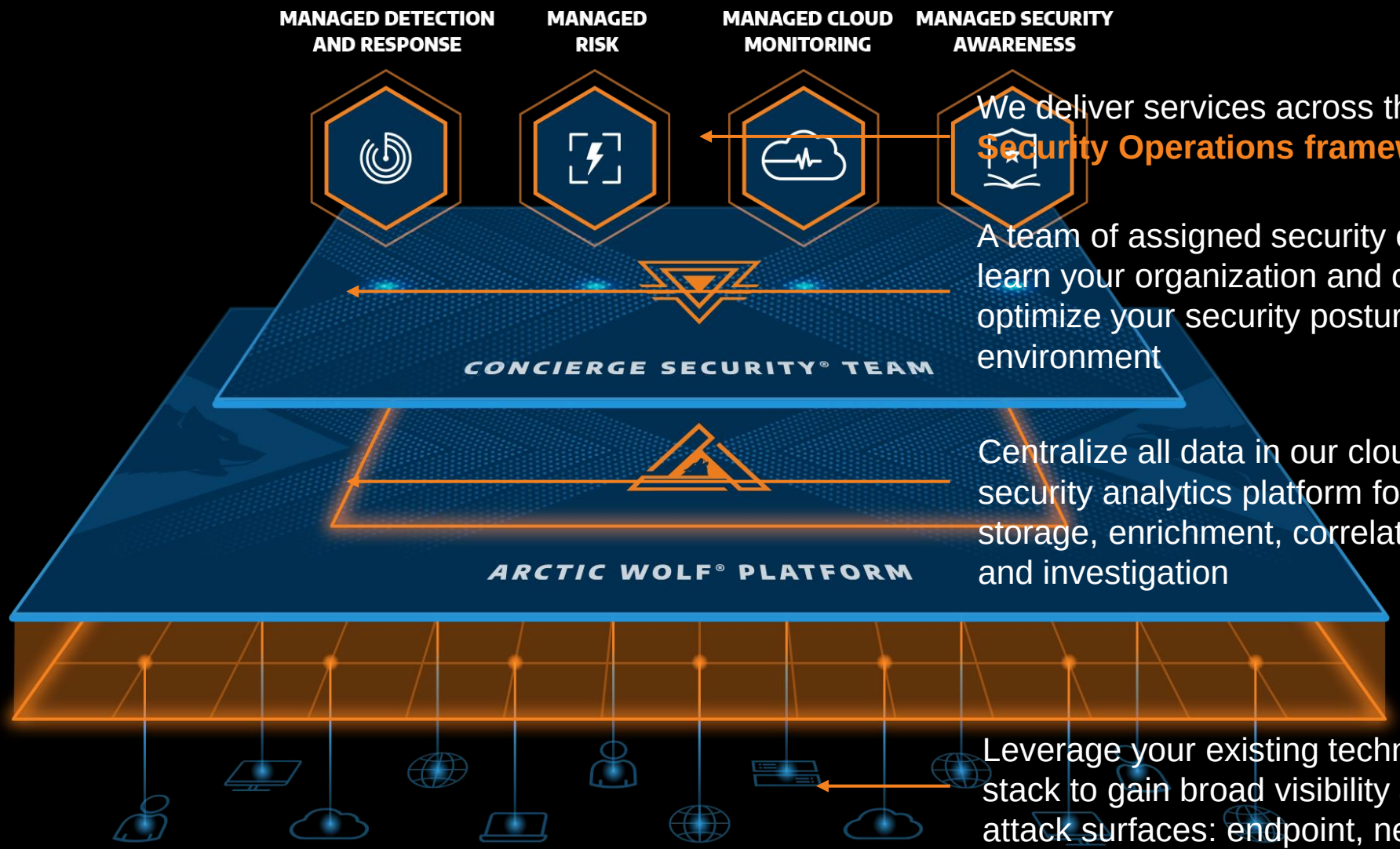
©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Arctic Wolf Platform



©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Arctic Wolf Platform



We deliver services across the entire **Security Operations framework**

A team of assigned security experts who learn your organization and continually optimize your security posture for your environment

Centralize all data in our cloud-native security analytics platform for 24/7 storage, enrichment, correlation, analysis and investigation

Leverage your existing technology stack to gain broad visibility across attack surfaces: endpoint, network, cloud, identity & human

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Why Arctic Wolf?

Our innovative Security Operations platform and concierge delivery model enable you to end Cyber Risk

Time to Value

- Leverage existing investments
- Add resources & expertise to your team
- Reduce noise & drive efficiency

Guidance

- Concierge Security Team
- Framework tailored to your environment
- World-class expertise on-demand

Protection

- Against commodity & advanced threats
- Attack surfaces
- All-the-time (24x7)

Resilience

- Proactive risk mgt
- Continuous posture assessment
- Sustained compliance

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

ARCTIC WOLF

THE LEADER IN **SECURITY OPERATIONS**

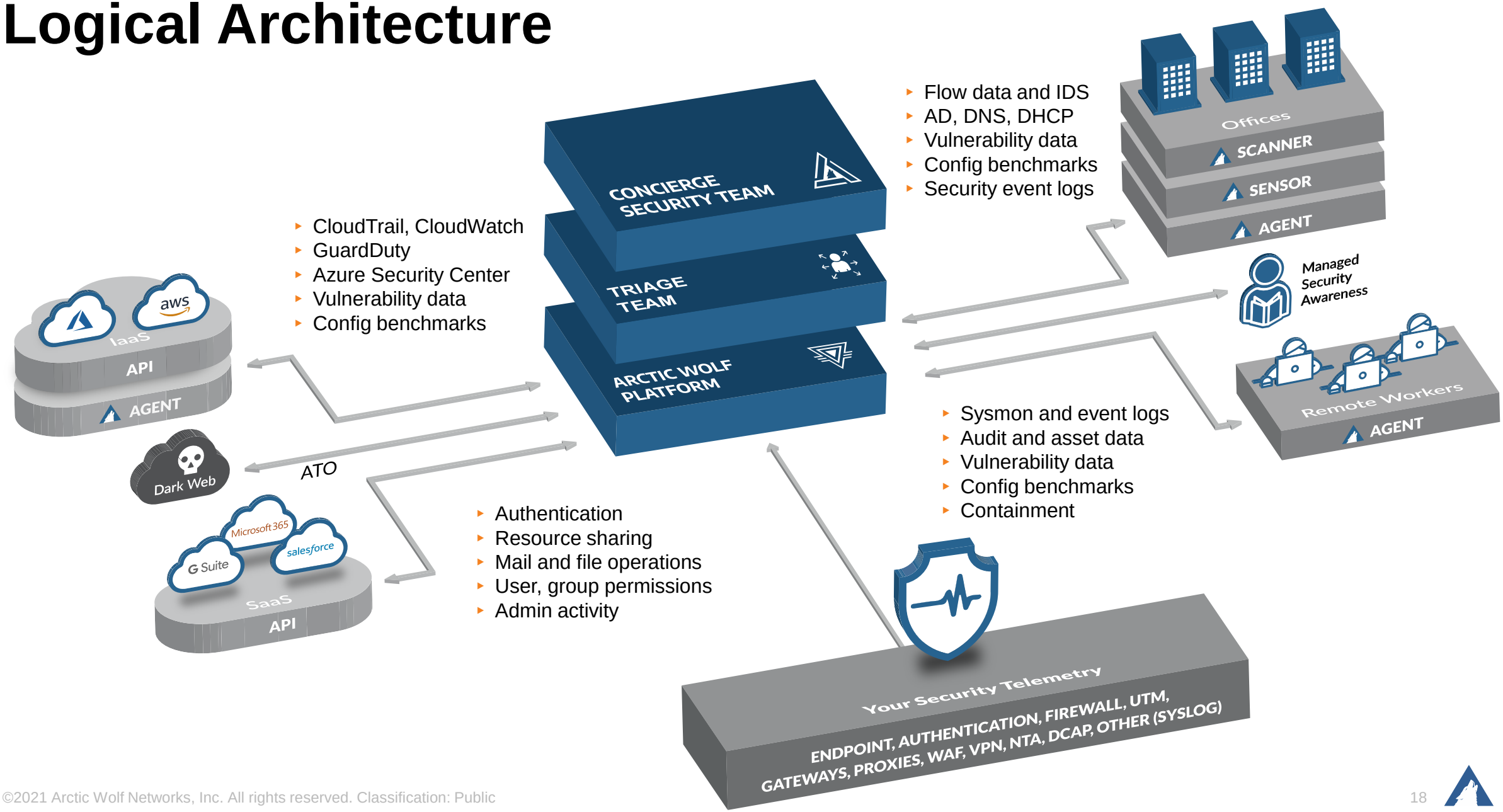
Thank You

ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

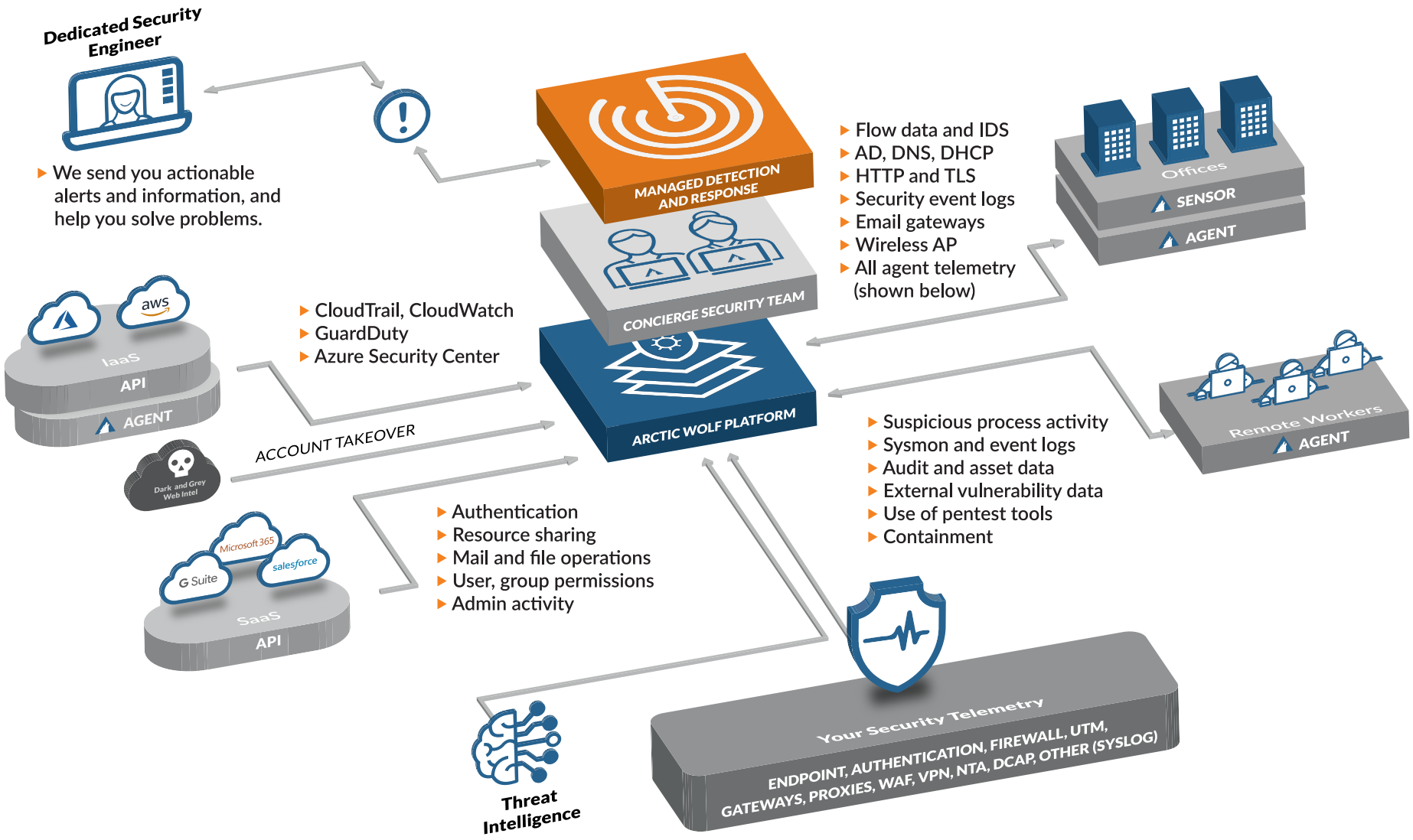
Appendix

Logical Architecture



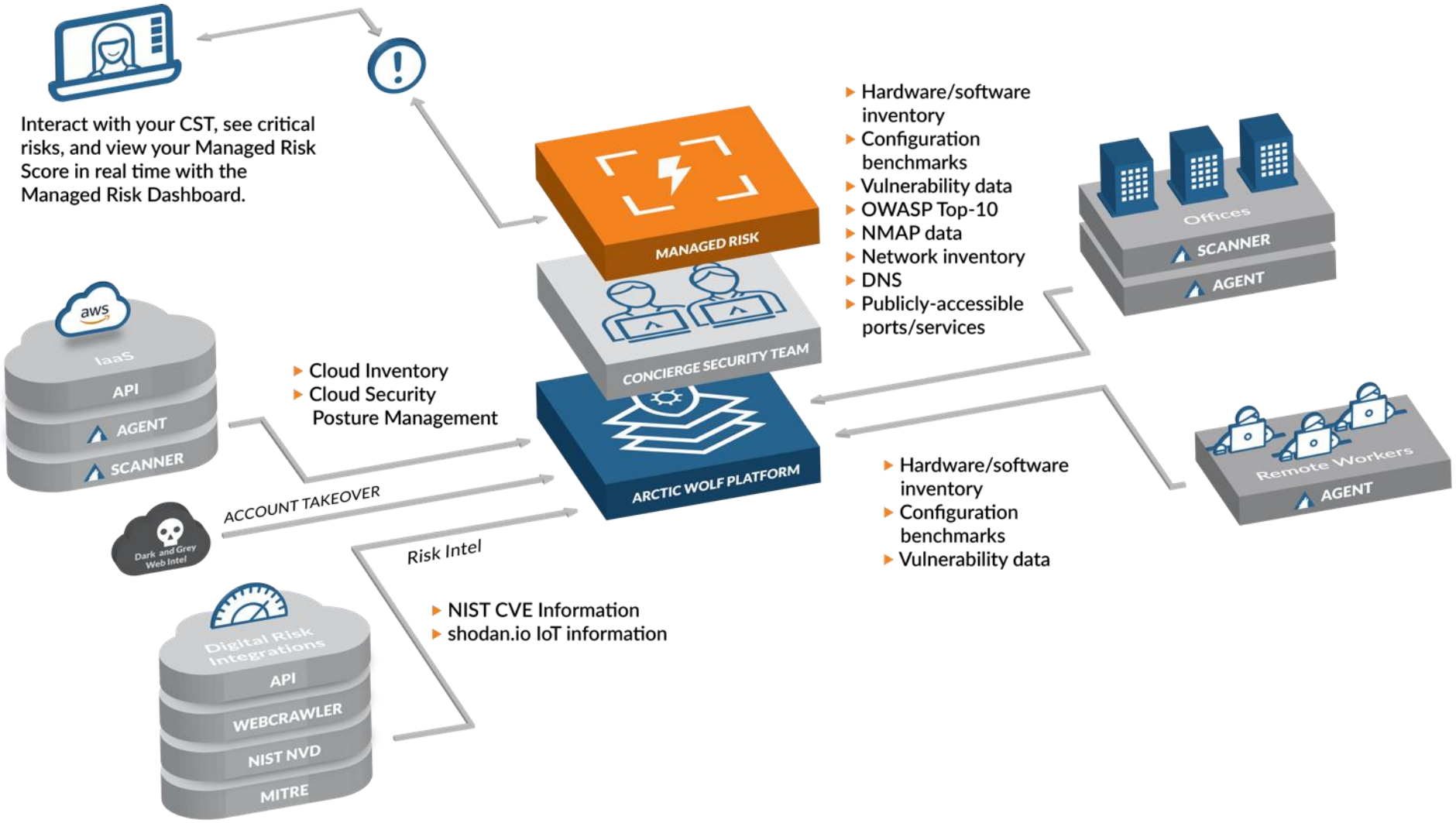
©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Managed Detection and Response Architecture



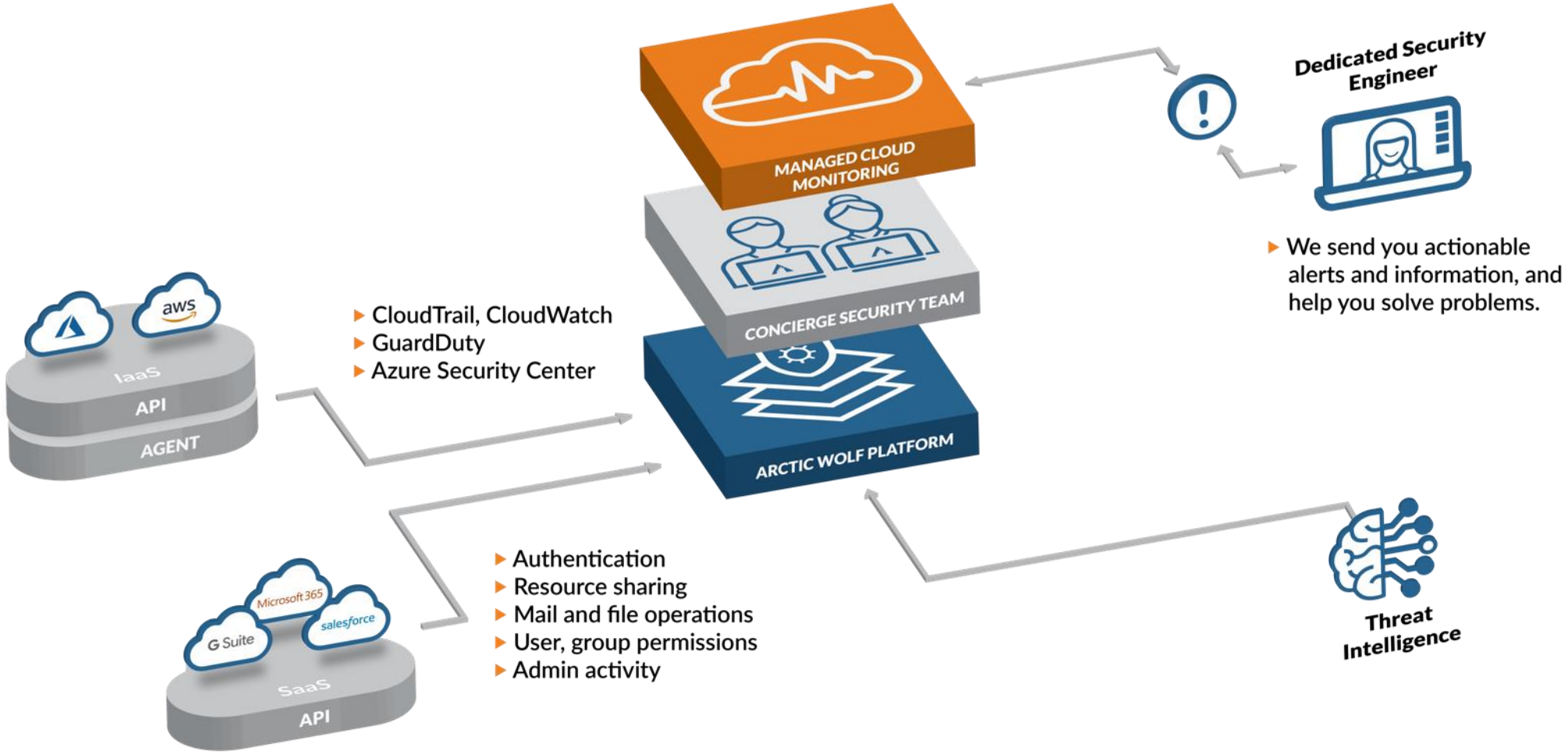
©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Managed Risk Architecture



©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Managed Cloud Monitoring Architecture



©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

AW Security Operation Teams

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Concierge Security Team (CST)

Your named Concierge Security Team will work with you to build and execute a Security Journey that meets your organization's goals and objectives while identifying opportunities to strengthen your security posture over time.

EXPERTISE

Deliver execution and operational excellence with skills required to detect advanced threats and manage risks in a way that's customized to your environment.

Security Operations Experts

Hundreds of years of combined experience with cybersecurity accreditations like CISSP, HCISPP, CCSP, CISM, CRISC, GCIH

Threat Hunting

Hunting for suspicious activity across your environment

Informed Incident Insights

Filter out the noise to reveal what happened, and what to do about it

STRATEGY

Strategic security guidance drives continuous improvement that's tailored to the specific needs of your organization.

Security Posture Reviews

Evaluate the root cause of threats and get prioritized recommendations to improve posture

Named Advisors

Trusted security operations experts paired with you to deliver tailored triage and strategic guidance

Security Journey Guidance

Quarterly reviews to help you design, implement, and achieve your security vision

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Arctic Wolf Triage Team

The Triage Team works 24x7x365 to investigate alerts generated by the Arctic Wolf Platform. This team provides tactical support and guidance to customers and the Concierge Security Team during security events.

COVERAGE

Work around the clock to triage critical events and deliver actionable insights when you need them the most.

24x7 Continuous Monitoring

Your environment is monitored around the clock for threats and risks

Rapid Response

Investigate and escalate critical events within thirty minutes

Real-Time Remediation

Rapidly contain incidents and get detailed guidance on remediation

On- Demand Access

To security analysts via telephone or email 24/7

INVESTIGATION

Deliver execution and operational excellence with skills required to detect advanced threats and manage risks in a way that's customized to your environment.

Security Operations Experts

Top-talent with hundreds of years of combined experience working for Military, Government and Public and Private sector organizations.

Informed Incident Insights

- Filter out the noise to reveal what happened, and what to do about it
- Detect threats across network, endpoint, & cloud.
- Expert analysis of IOCs across entire attack surface using a purpose-built cloud platform
- Discover vulnerabilities and misconfigurations

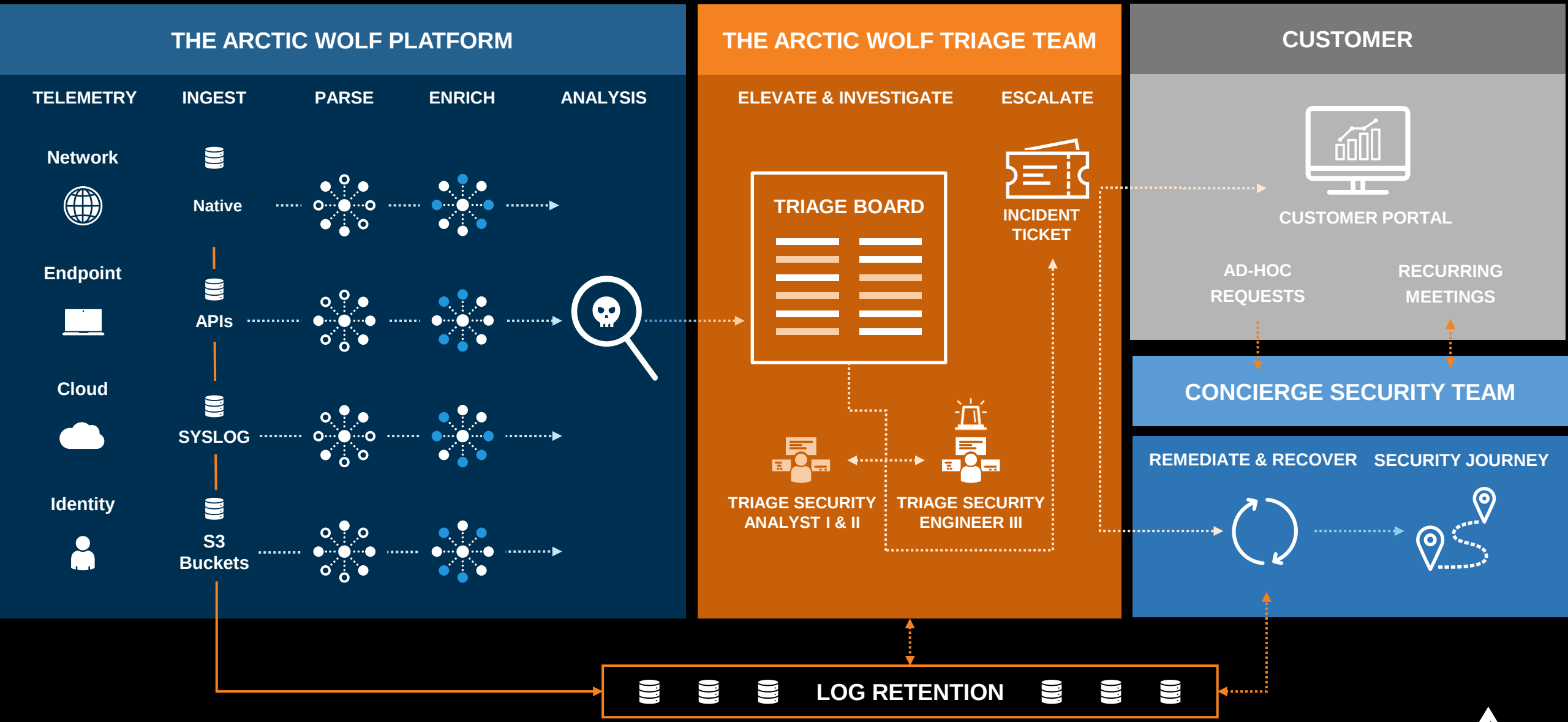
©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

AW Security Operations Workflow

THE ARCTIC WOLF PLATFORM					THE ARCTIC WOLF TRIAGE TEAM		Customer	CONCIERGE SECURITY TEAM	
TELEMETRY	INGEST	PARSE	ENRICH	ANALYSIS	ELEVATE & INVESTIGATE	ESCALATE	CUSTOMER PORTAL	REMEDIATE & RECOVER	SECURITY JOURNEY

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

AW Security Operations Workflow



©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Concierge Engagement Model

CUSTOMER

ARCTIC WOLF

Activation

CUSTOMER

- Attend call and provide environment details, points of contacts, etc.

ARCTIC WOLF

- Host kickoff call
- Provision customer environment
- Begin Deployment

Deployment

CUSTOMER

- Deploy agent
- Receive and install sensors and scanners
- Configure log sources to send to Arctic Wolf

ARCTIC WOLF

- Start EVA, ATO and Cloud monitoring
- Install virtual Scanners
- Verify install & config
- Document next steps
- Host validation call
- Handoff to CST
- 24x7 coverage begins

Customization

CUSTOMER

- Validate contacts, escalation path, tuning and customization requests

ARCTIC WOLF

- Host first review call
- Verify data ingestion
- Begin tuning and customization
- Likely to find first threat

Service Delivery

CUSTOMER

- Engage with tickets, execute remediation
- Call us with emergency
- Notify us of architecture changes

ARCTIC WOLF

- Alert triage
- Threat detection
- Threat hunting
- Vulnerability assessment
- Config benchmarking
- Cloud monitoring
- Prioritize and send tickets to customer

Ad-Hoc

CUSTOMER

- Request custom report
- Email us questions
- Request audit support
- Request logs or access to log search

ARCTIC WOLF

- Facilitate resolution to requests

Scheduled

CUSTOMER

- Attend meeting
- Give feedback
- Implement recommendations

ARCTIC WOLF

- Recurring reviews and interactions to guide strategic enhancements

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Different Approaches to ‘Security Operations’

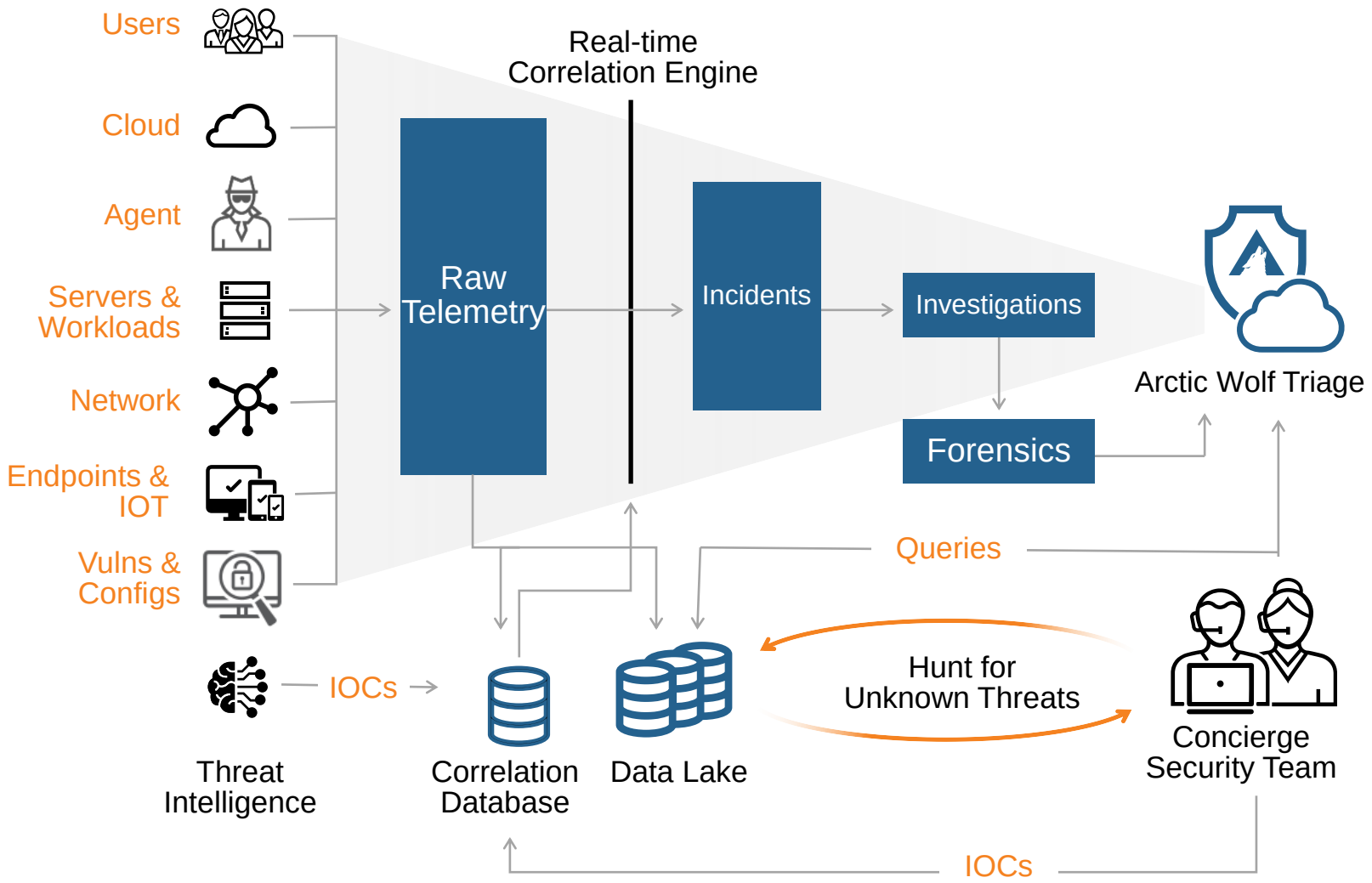
	Security Operations framework coverage	Tech Stack & Compatibility	Visibility across attack surfaces	Pricing	Service Delivery Engagement
SIEM					
MSSP					
EDR					
MDR					
XDR					
AW					
	Coverage across Sec Ops framework	Use existing tech and or AW tech	Endpoint, network, Cloud, Apps, Identity and People	Unlimited & unmetered data pricing	Invented Concierge Security Team

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Arctic Wolf Validation

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Arctic Wolf Security Operations



The Average Customer:
~497M Observations/Week
~70 Investigations/Week
~5 Tickets/Week

Identify

- Detect threats across network, endpoint, and cloud.
- Expert analysis of IOCs across entire attack surface using a purpose-built cloud platform
- Discover vulnerabilities and misconfigurations

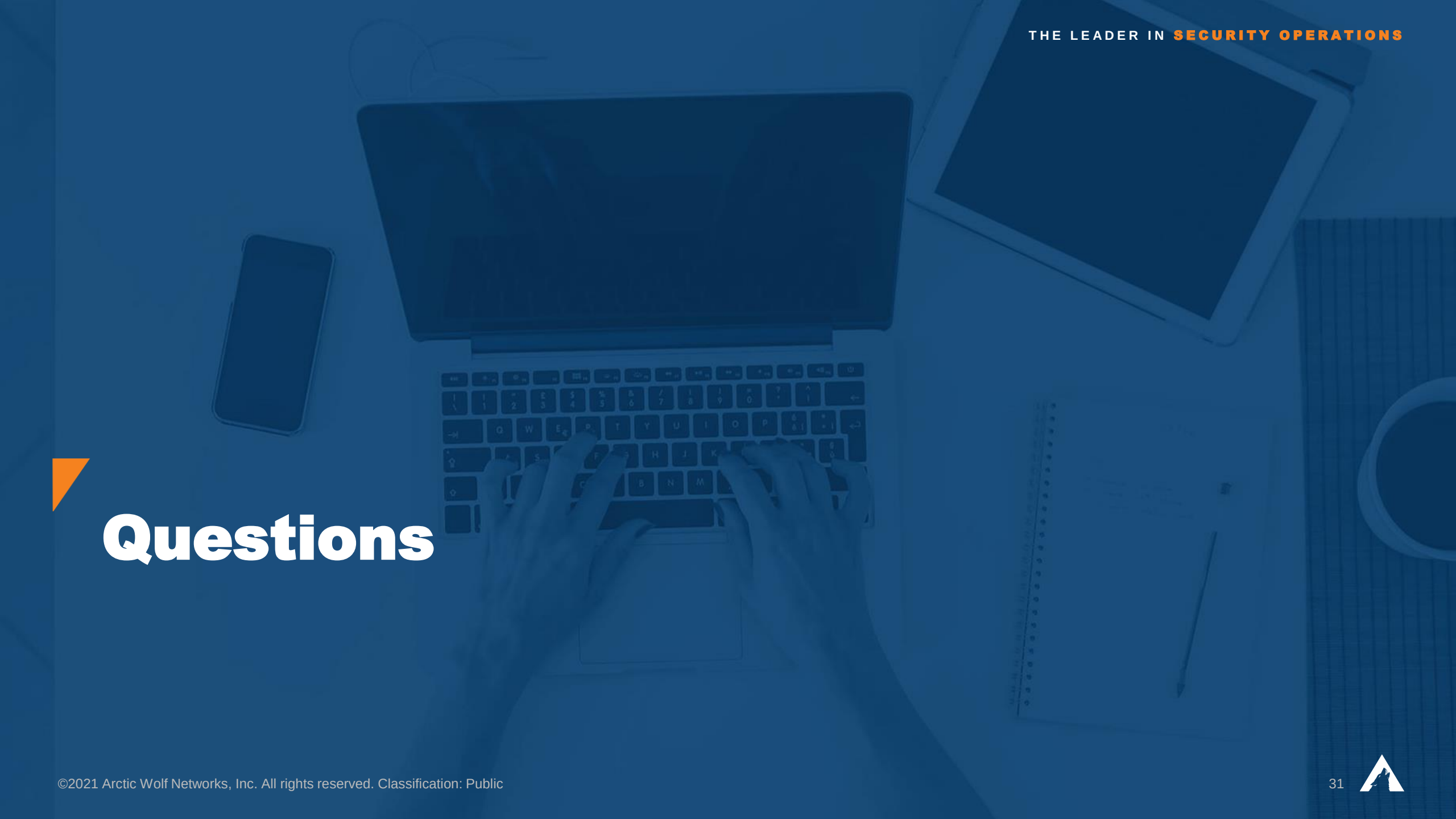
Act

- Guidance and prioritization for remediating threats, vulnerabilities, and risks.
- Detailed recovery and hardening recommendations with closed-loop follow-up

Improve

- Hunt for Advanced threats across endpoints, network and Cloud with deep analytics and human expertise
- Security Journey program to improve overall security posture

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public



Questions

©2021 Arctic Wolf Networks, Inc. All rights reserved. Classification: Public

Thank You