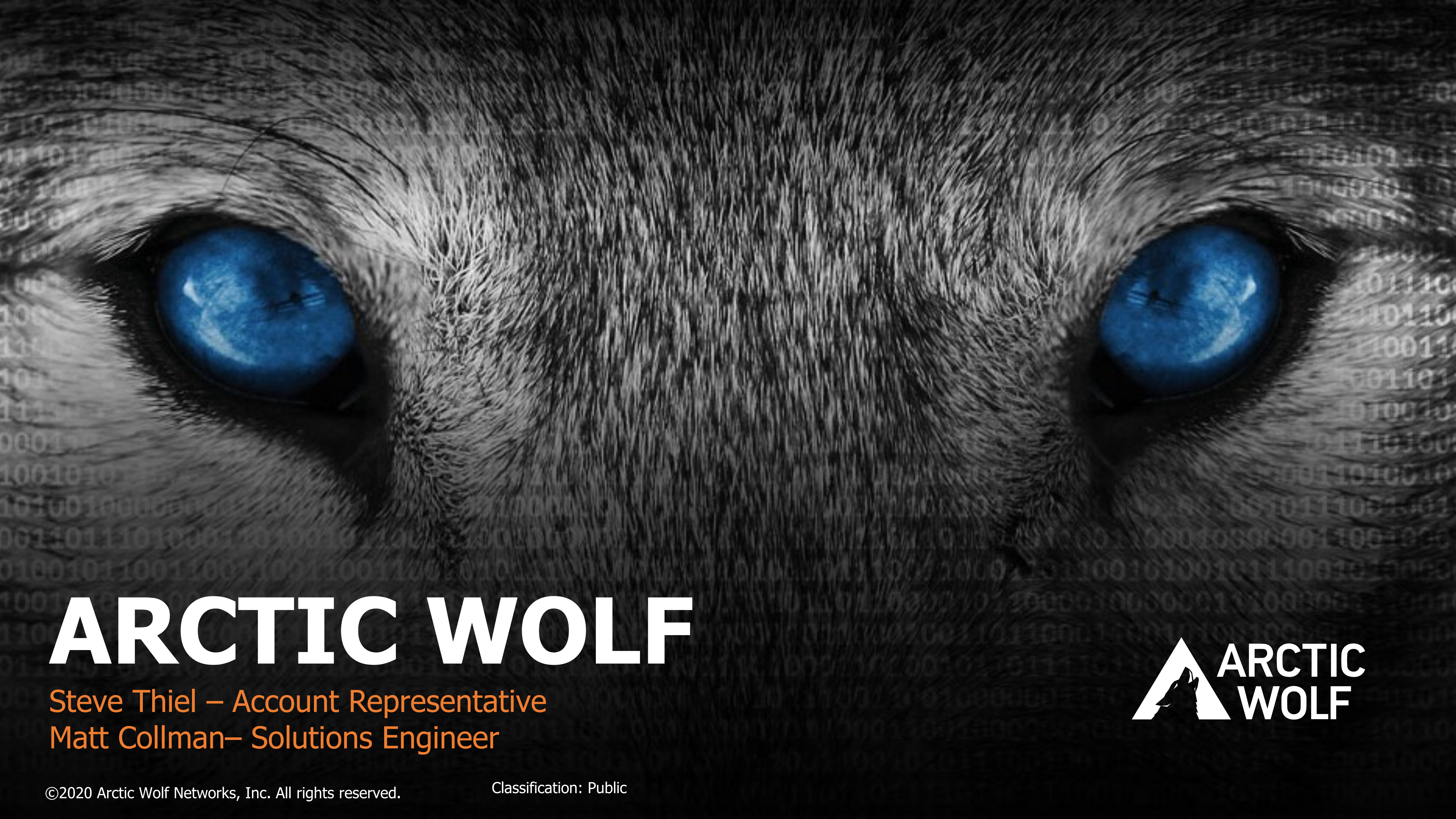


ARCTIC WOLF

Steve Thiel – Account Representative
Matt Collman– Solutions Engineer

Classification: Public

The Average Cost of a Data Breach in the United States… $8.19m

(Source: IBM)

Financial Service Firms are…

300x as likely as other companies to experience a cyber attack (Boston Consulting Group)

Experiencing a 520% increase in Ransomware and Phishing (for comparison: 64% blended across other industries)

CYBERSECURITY HAS AN EFFECTIVENESS PROBLEM.

Lessons Learned

2013

Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores

2017

Equifax Announces Cybersecurity Incident Involving Consumer Information

2019

Hacker Gain Access to 100 Million Capital One Credit Card Applications and Accounts

A security product detected the threat, but nobody responded to the alert.

Flaw was known by vulnerability management tools, but the patch was never installed.

Misconfiguration in cloud service went unnoticed despite availability of monitoring products.

THEY'RE NOT PRODUCT FAILURES.

THEY'RE OPERATIONAL FAILURES.

The Operational Approach

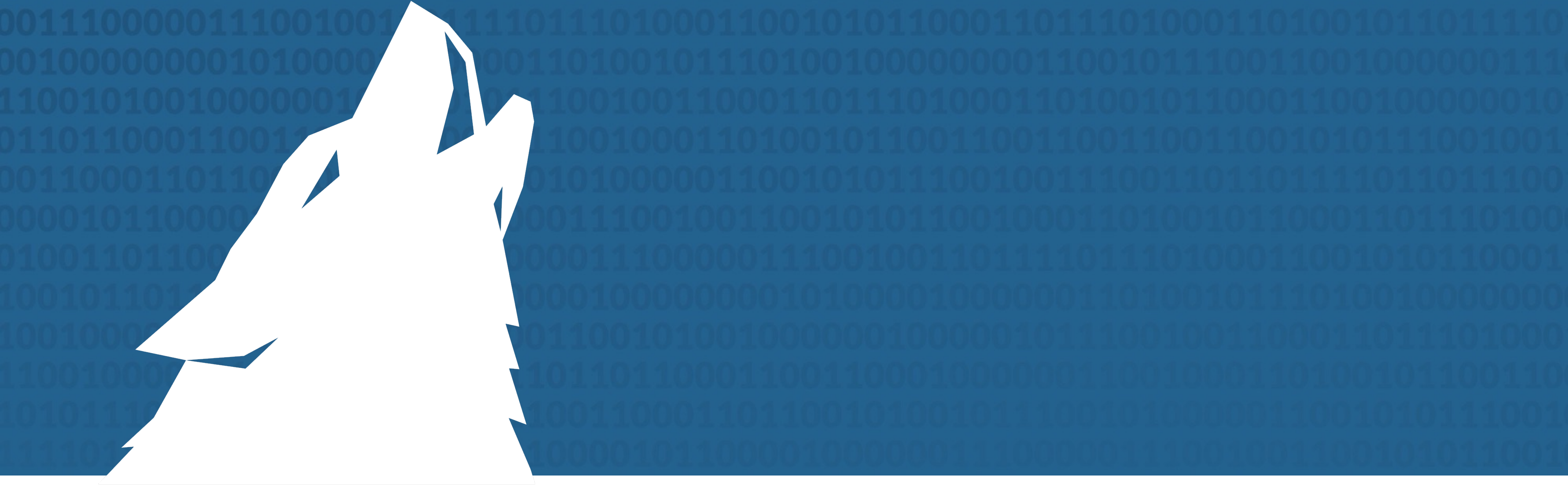
Broad Visibility

24x7 Coverage

Access to Expertise

Strategic Guidance

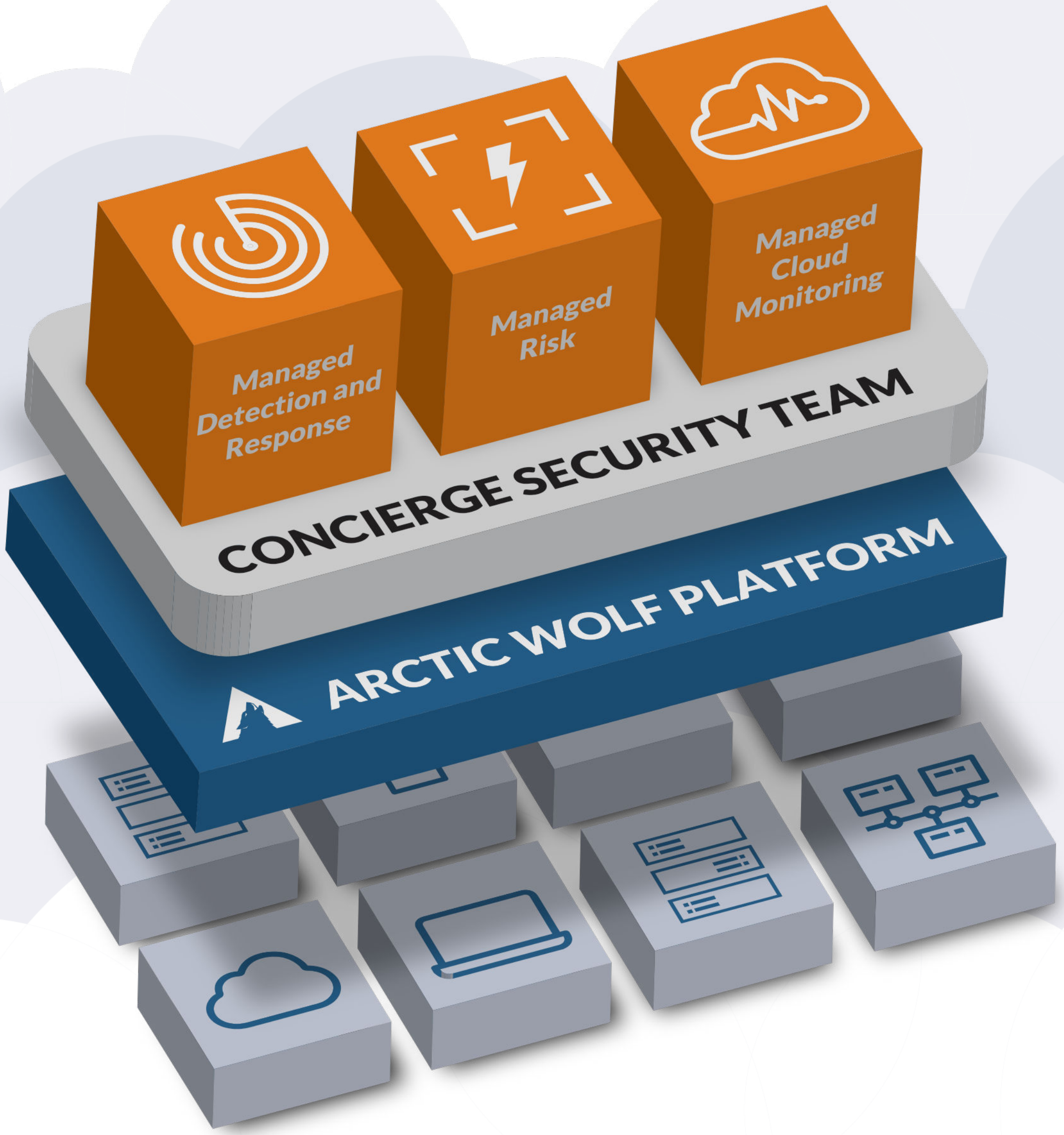
Continuous Improvement



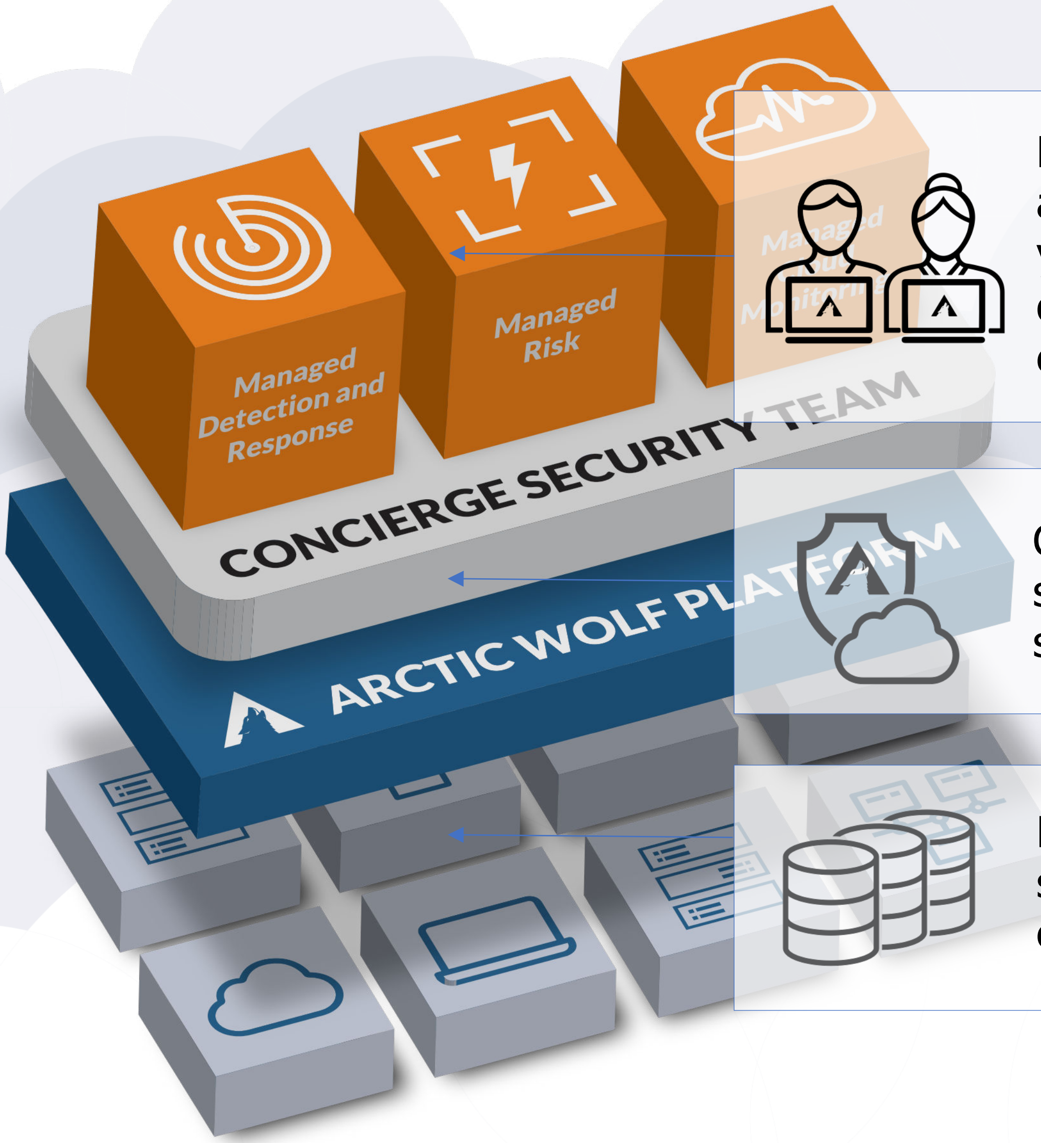
ARCTIC WOLF

SECURITY OPERATIONS

Arctic Wolf Platform



Arctic Wolf Platform



Monitor the data 24x7 by a team of assigned security experts who learn your organization and continually optimize our solutions for maximum effectiveness in your environment

Centralize all data in our cloud-native security analytics platform for storage, enrichment, and analysis

Leverage your existing technology stack to gain broad visibility across endpoint, network, and cloud

Concierge Security Team (CST)

✓ Named Security Experts

- Available to you 8am-5pm in your time-zone
- Emergency 5 Minute Response

✓ Understand Your Network and Business Risks

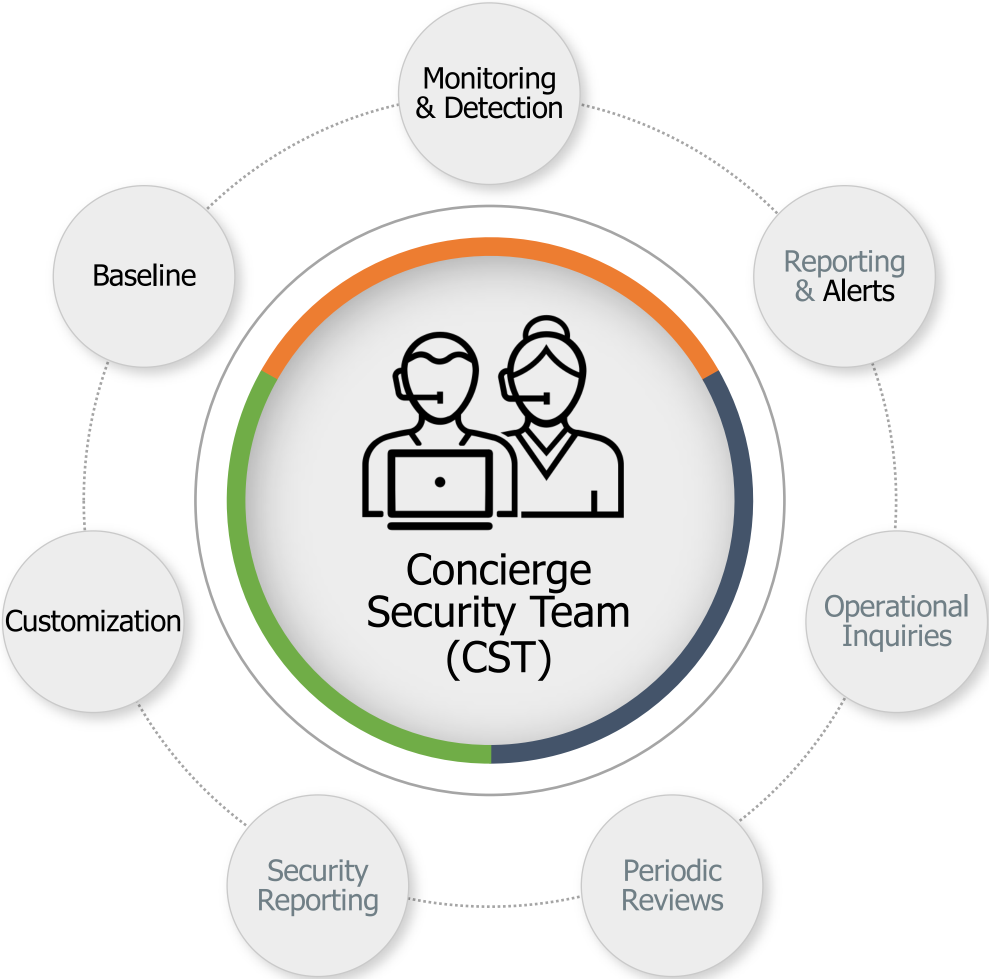
- Acts as trusted advisor for your IT team
- Builds a customized service for you

✓ Remote Forensics and Incident Response

- Proactively hunts for threats
- Recommends remediation actions

✓ Strategic Security Insights & Advice

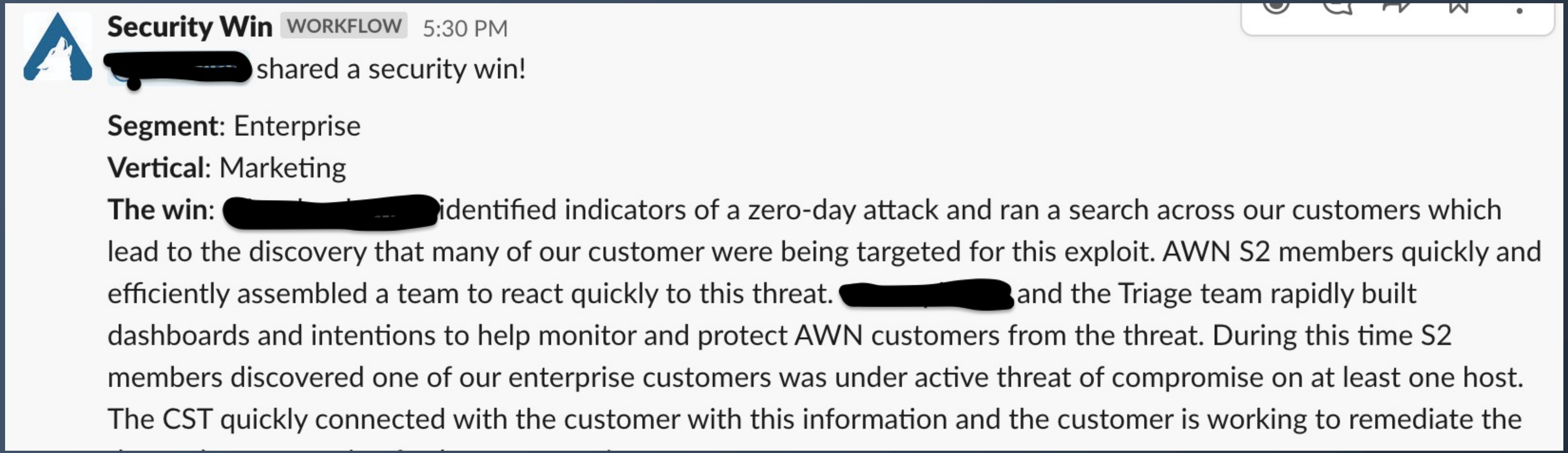
- Conducts quarterly strategic meetings to identify gaps in the overall security posture



Personal | Predictable | Protection

Recent Win Stories from our SOC

Zero Day attack caught



Security Win WORKFLOW 5:30 PM

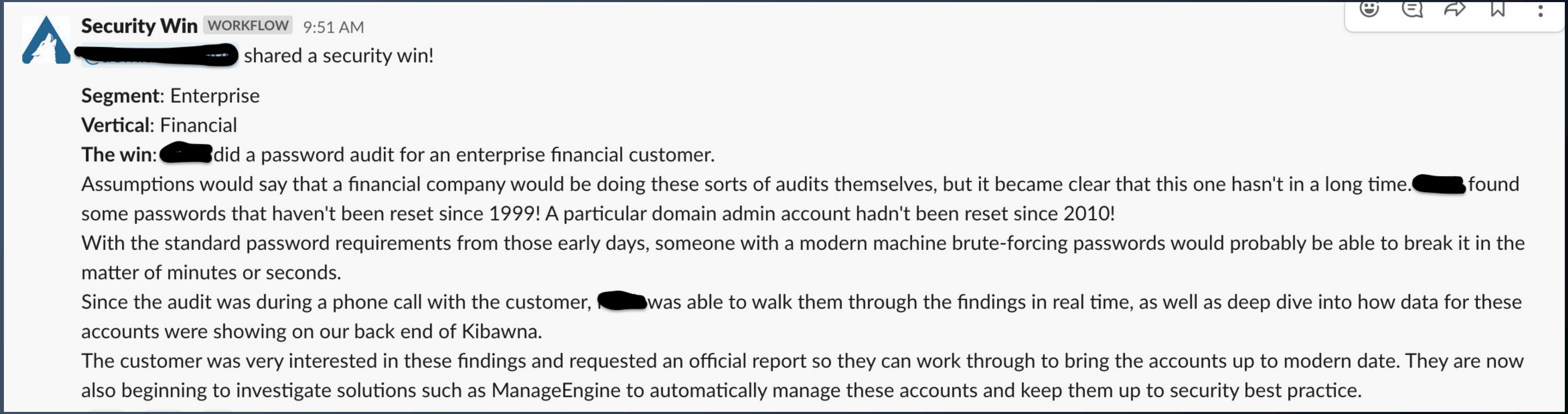
[redacted] shared a security win!

Segment: Enterprise

Vertical: Marketing

The win: [redacted] identified indicators of a zero-day attack and ran a search across our customers which lead to the discovery that many of our customer were being targeted for this exploit. AWN S2 members quickly and efficiently assembled a team to react quickly to this threat. [redacted] and the Triage team rapidly built dashboards and intentions to help monitor and protect AWN customers from the threat. During this time S2 members discovered one of our enterprise customers was under active threat of compromise on at least one host. The CST quickly connected with the customer with this information and the customer is working to remediate the

The value of the CST goes beyond simply detecting & responding to security alerts for our clients



Security Win WORKFLOW 9:51 AM

[redacted] shared a security win!

Segment: Enterprise

Vertical: Financial

The win: [redacted] did a password audit for an enterprise financial customer.

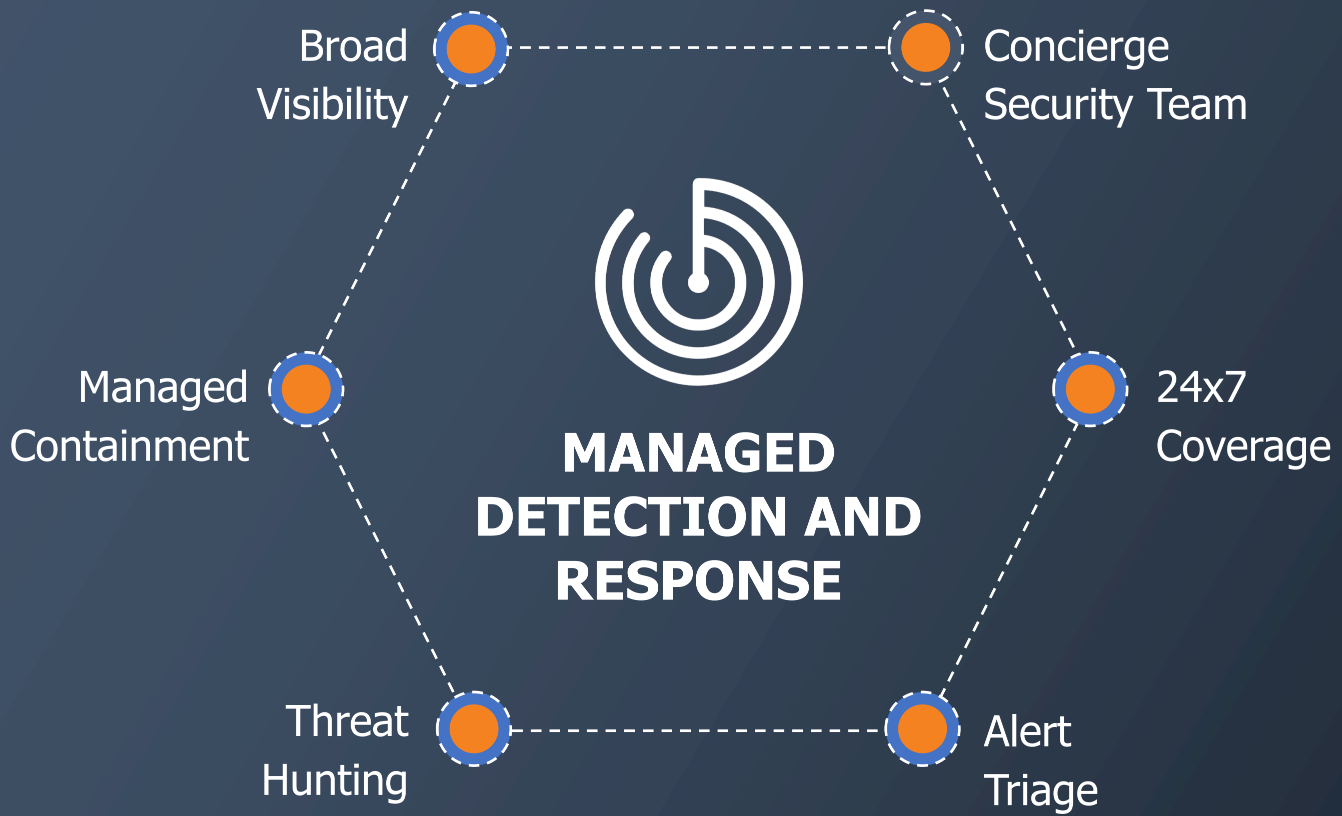
Assumptions would say that a financial company would be doing these sorts of audits themselves, but it became clear that this one hasn't in a long time. [redacted] found some passwords that haven't been reset since 1999! A particular domain admin account hadn't been reset since 2010!

With the standard password requirements from those early days, someone with a modern machine brute-forcing passwords would probably be able to break it in the matter of minutes or seconds.

Since the audit was during a phone call with the customer, [redacted] was able to walk them through the findings in real time, as well as deep dive into how data for these accounts were showing on our back end of Kibawna.

The customer was very interested in these findings and requested an official report so they can work through to bring the accounts up to modern date. They are now also beginning to investigate solutions such as ManageEngine to automatically manage these accounts and keep them up to security best practice.

Arctic Wolf Solutions



MANAGED DETECTION AND RESPONSE

Detect

Leverage your existing tech stack to identify advanced network, endpoint, and cloud threats

Respond

24x7 coverage and guided response stops threats before they can do harm

Recover

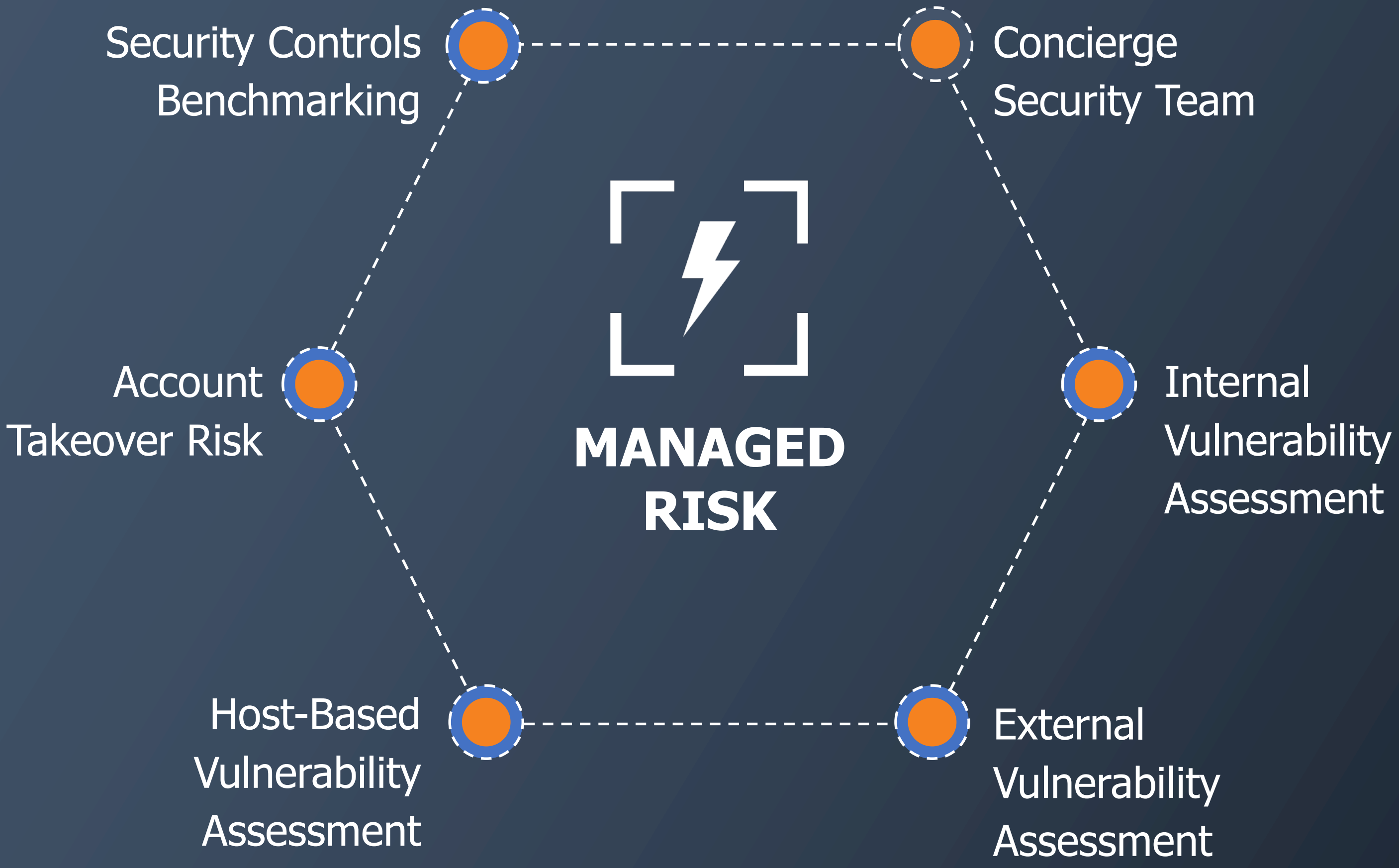
Find root cause, validate remediation, and collaborate to continuously improve your overall security posture

70%

Of new customer environments have latent threats

Classification: Public

Arctic Wolf Solutions


Security Controls Benchmarking
Concierge Security Team
Account Takeover Risk
MANAGED RISK
Internal Vulnerability Assessment
Host-Based Vulnerability Assessment
External Vulnerability Assessment

Discover

Identify and categorize risky software, assets, and accounts

Benchmark

Understand your current digital risk posture and identify gaps relative to best practices

Harden

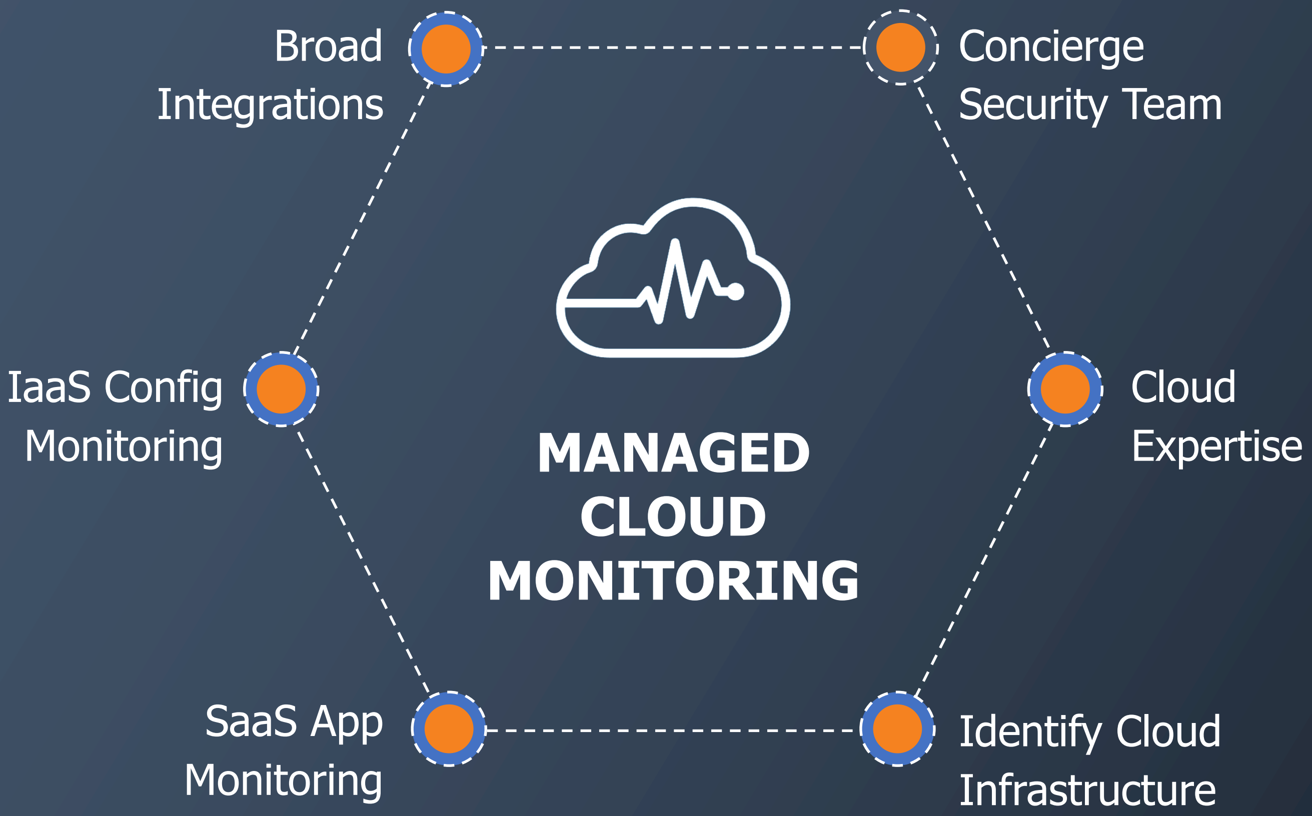
Know when you're exposed and prioritize security posture improvements

80%

Of threats can be prevented by meeting the top 5 CIS controls

Classification: Public

Arctic Wolf Solutions



Identify

Identify exposed cloud platforms and accounts to understand risks, such as unsecured S3 buckets and unauthorized cloud deployments

Monitor

Monitor IaaS services for configuration risks, and SaaS apps for key threats and indicators of compromise

Simplify

Streamline cloud security with cloud experts plus concierge deployment and management

47%

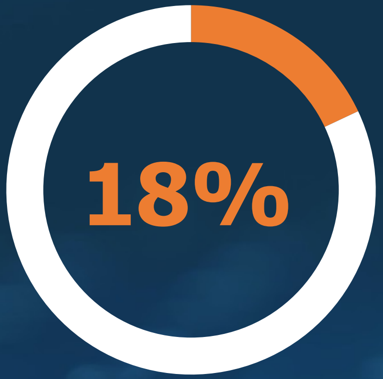
Of the incidents we detect include a cloud component

Better Protection Against All Attack Types

Dwell Time

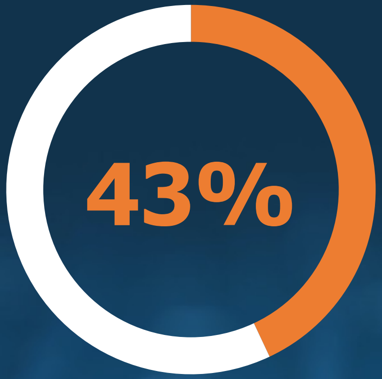
Industry average time to identify an intrusion is 206 days. Arctic Wolf does it in 30 minutes or less.

Phishing



Of customers have phishing activity that is missed by email security but caught by Arctic Wolf

Advanced Threats



Of customers have advanced threat activity being missed by security tools but caught by Arctic Wolf

Account Takeover

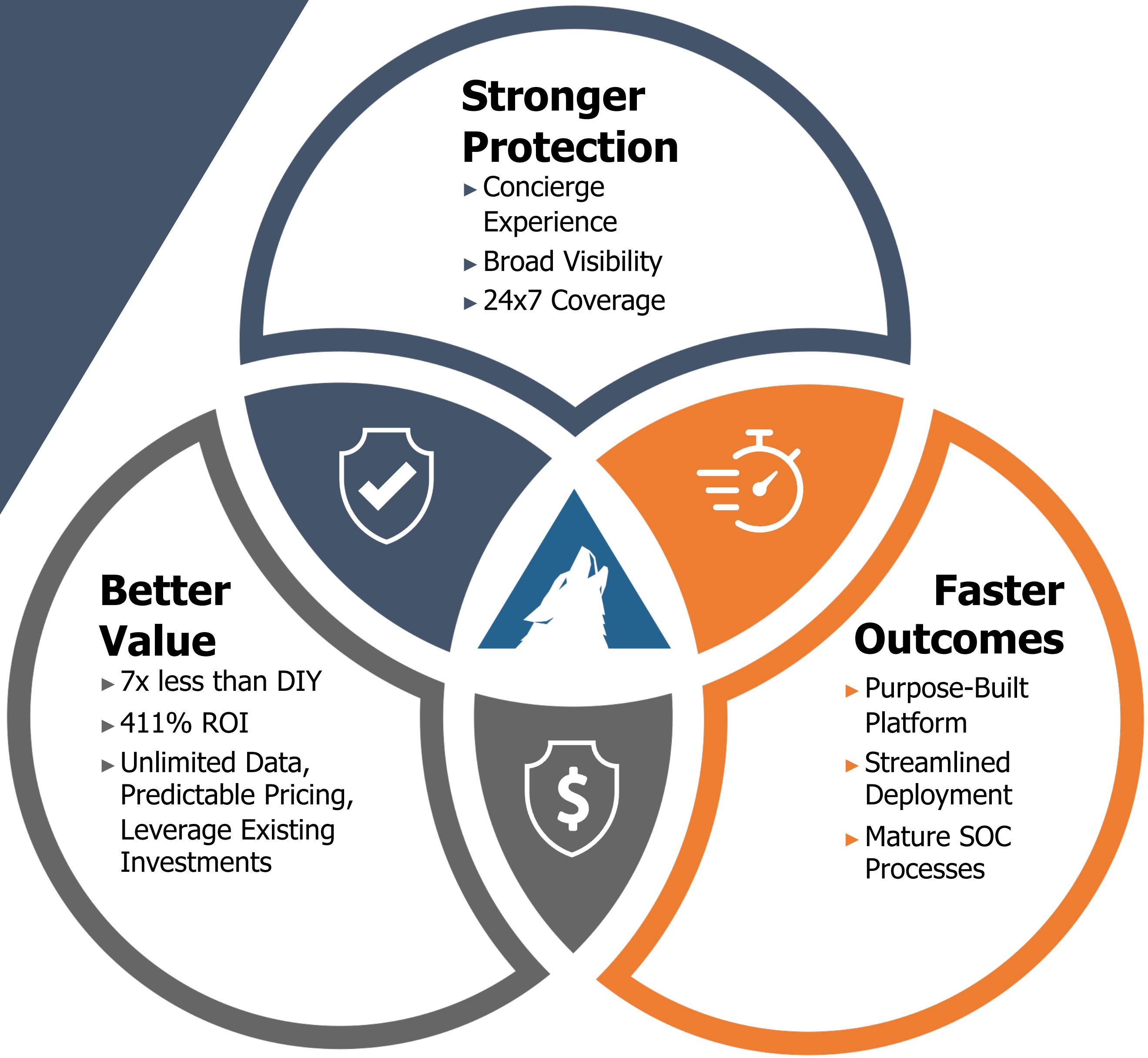
Of customers have some PII exposure and 5.5% have plaintext passwords exposed online

Unpatched Vulnerabilities

Reduction in time to patch critical vulnerabilities after activating Arctic Wolf

WHY ARCTIC WOLF?

Our innovative platform and concierge delivery model enable us to provide better protection in a way that is uniquely fast and cost effective.



Stronger Protection

- Concierge Experience
- Broad Visibility
- 24x7 Coverage

Better Value

- 7x less than DIY
- 411% ROI
- Unlimited Data, Predictable Pricing, Leverage Existing Investments

Faster Outcomes

- Purpose-Built Platform
- Streamlined Deployment
- Mature SOC Processes

ARCTIC WOLF

PERSONAL | PREDICTABLE | PROTECTION

THANK YOU

arcticwolf.com

Classification: Public

Architecture

Matt Collman – Sales Engineer

ARCTIC WOLF

Classification: Public

Arctic Wolf Validation

Gartner
COOL VENDOR

500™
Technology Fast 500
2019 NORTH AMERICA
Deloitte.

SC Awards 2018
Winner

CHANNELNOMICS
SECURITY AWARDS
2018
WINNER

GENERAL DATA PROTECTION REGULATION
★★★★★
GDPR
READY

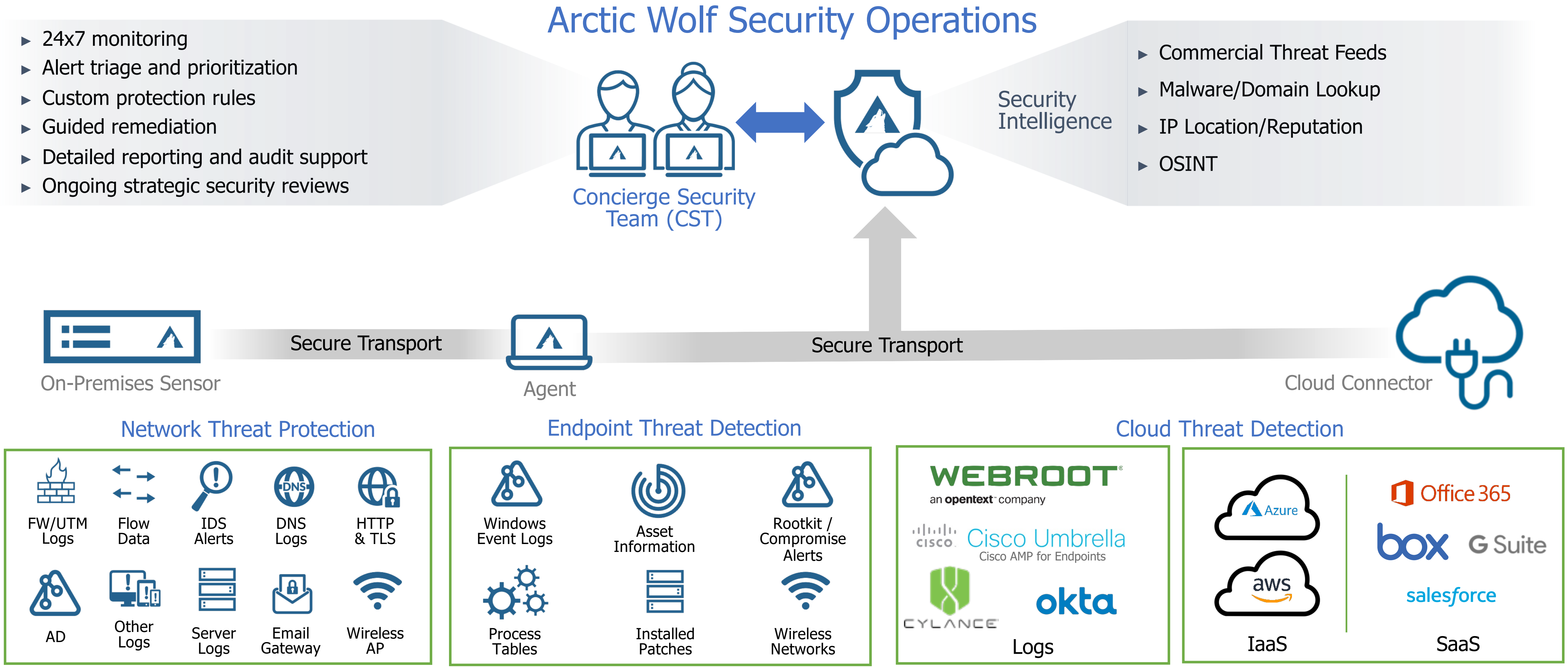
CERTIFIED
ISO 27001
CERTIFIED

Privacy Shield
Compliant

SOC 2
TYPE 2
AICPA
SOC

Classification: Public

Managed Detection and Response Architecture



Arctic Wolf Security Operations

- 24x7 monitoring
- Alert triage and prioritization
- Custom protection rules
- Guided remediation
- Detailed reporting and audit support
- Ongoing strategic security reviews

Concierge Security Team (CST)

Security Intelligence

- Commercial Threat Feeds
- Malware/Domain Lookup
- IP Location/Reputation
- OSINT

On-Premises Sensor

Secure Transport

Agent

Secure Transport

Cloud Connector

Network Threat Protection

FW/UTM Logs

Flow Data

IDS Alerts

DNS Logs

HTTP & TLS

AD

Other Logs

Server Logs

Email Gateway

Wireless AP

Endpoint Threat Detection

Windows Event Logs

Asset Information

Rootkit / Compromise Alerts

Process Tables

Installed Patches

Wireless Networks

Cloud Threat Detection

WEBROOT an opentext company

Cisco Umbrella

Cisco AMP for Endpoints

CYLANCE

okta

Logs

Azure

aws

IaaS

Office 365

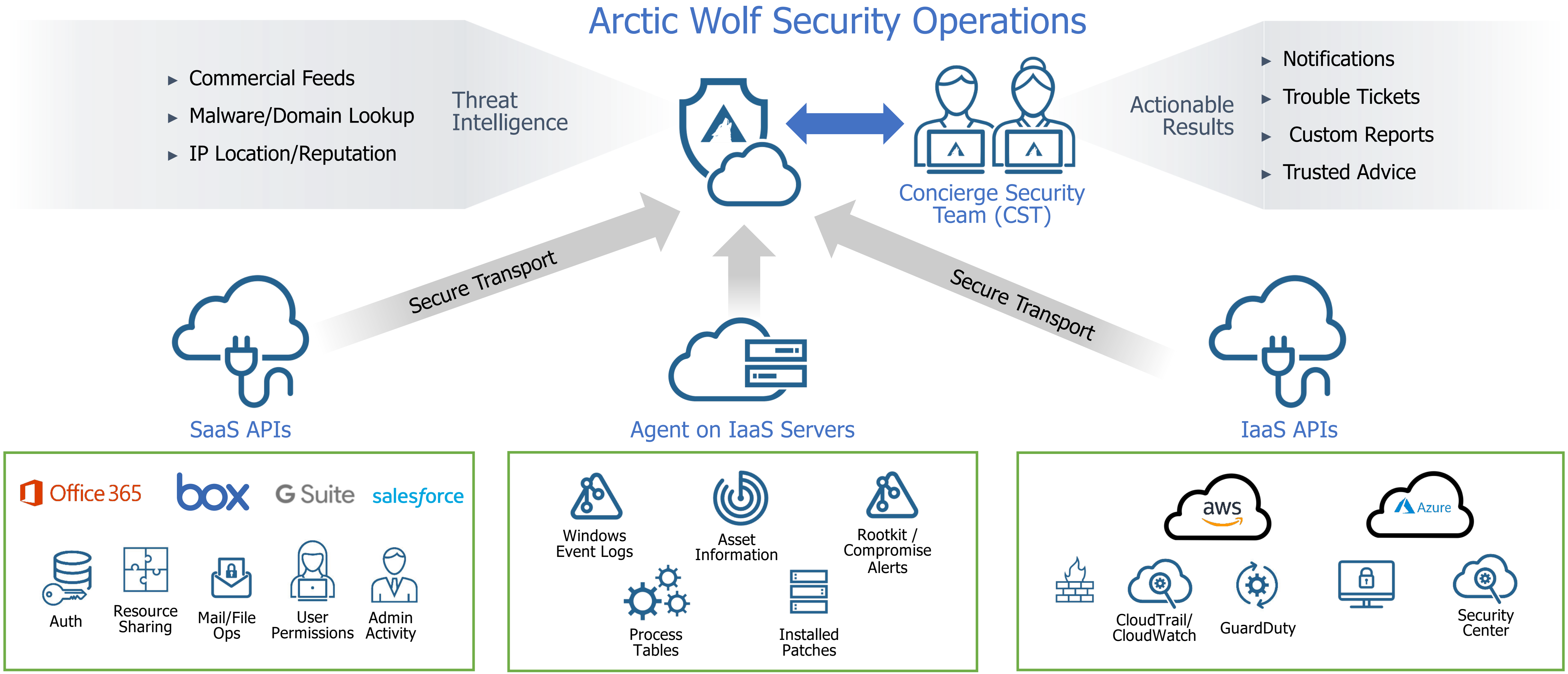
box

G Suite

salesforce

SaaS

Managed Cloud Monitoring Architecture



Arctic Wolf Security Operations

Threat Intelligence

- Commercial Feeds
- Malware/Domain Lookup
- IP Location/Reputation

Concierge Security Team (CST)

Actionable Results

- Notifications
- Trouble Tickets
- Custom Reports
- Trusted Advice

Secure Transport

Secure Transport

SaaS APIs

Agent on IaaS Servers

IaaS APIs

Auth

Resource Sharing

Mail/File Ops

User Permissions

Admin Activity

Windows Event Logs

Asset Information

Rootkit / Compromise Alerts

Process Tables

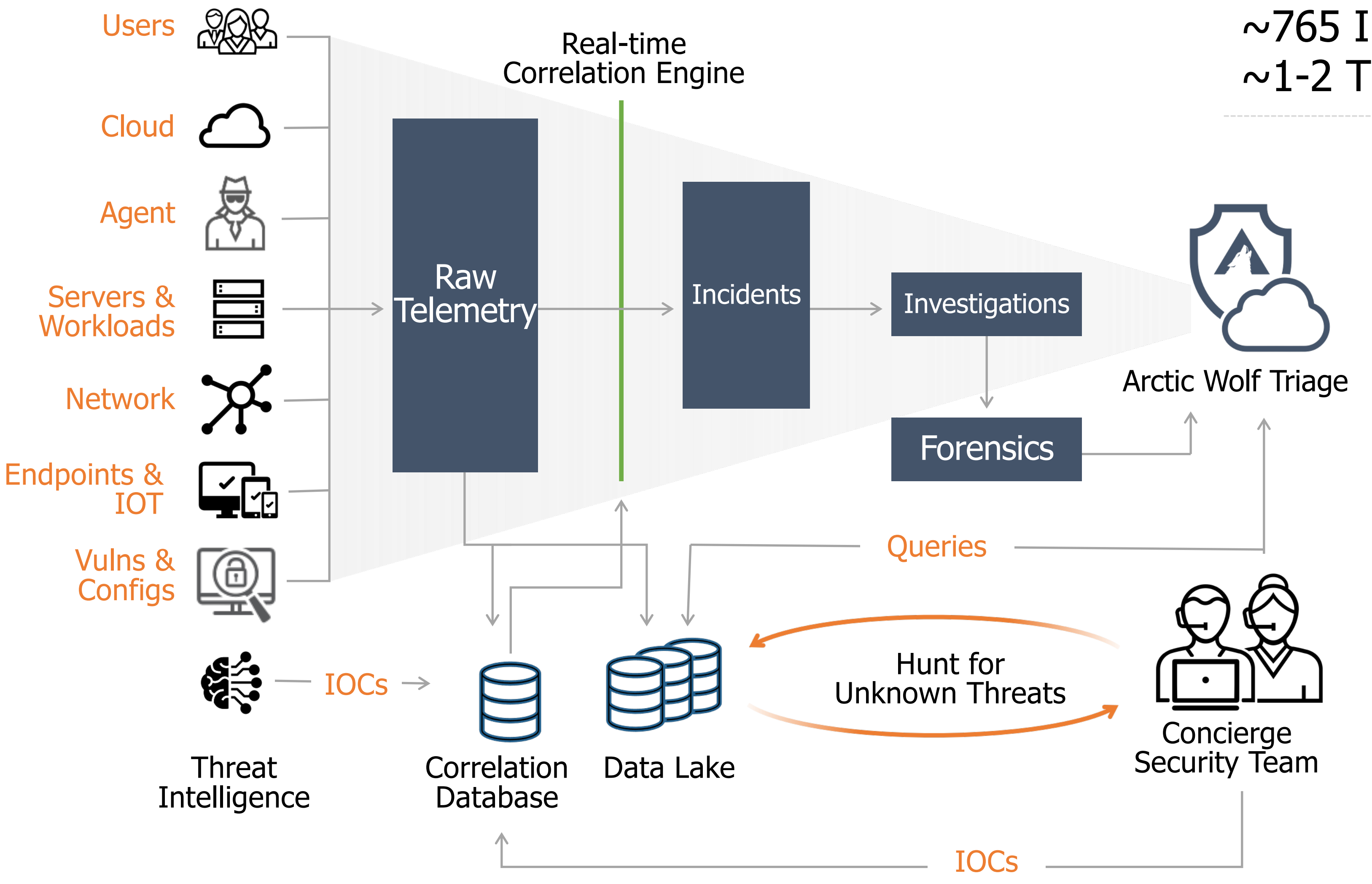
Installed Patches

CloudTrail/ CloudWatch

GuardDuty

Security Center

Arctic Wolf SOC Process



~165M Observations/Week
~765 Investigations/Week
~1-2 Tickets/Week

450 Users
150 Servers
4 Sensors

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

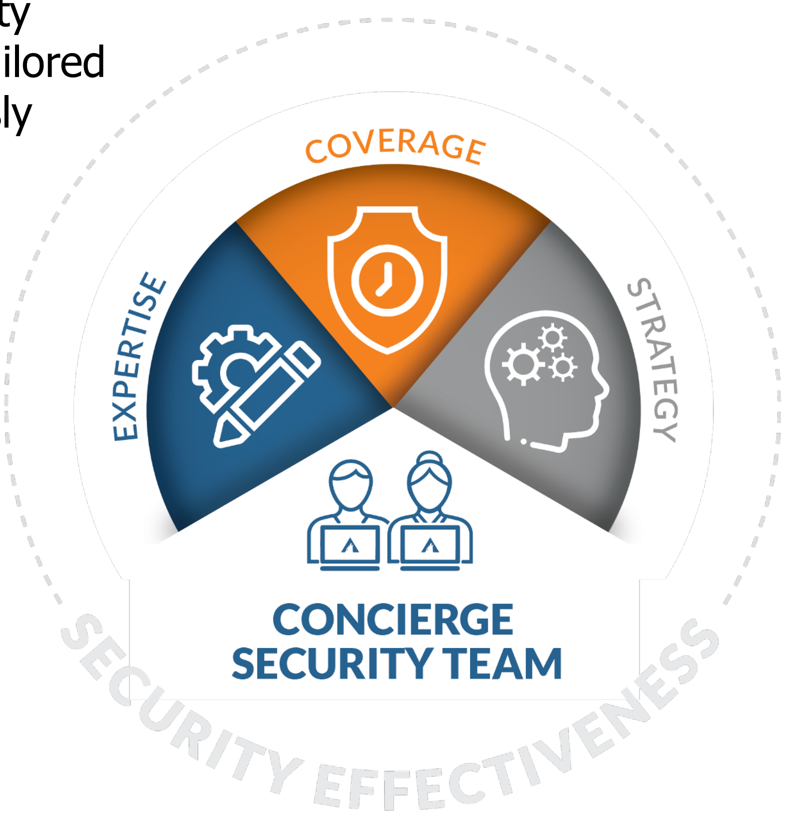
Concierge Security Team (CST)

The Arctic Wolf® Concierge Security® Team (CST) continuously monitors security events enriched and analyzed by the Arctic Wolf® Platform to provide your team with coverage, security operations expertise, and strategically tailored security recommendations to continuously improve your overall posture.

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
- **Proactive Threat Hunting**
  - Daily hunting for suspicious activity across your environment
- **Informed Incident Insights**
  - Filter out the noise to reveal what happened, and what to do about it



COVERAGE

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

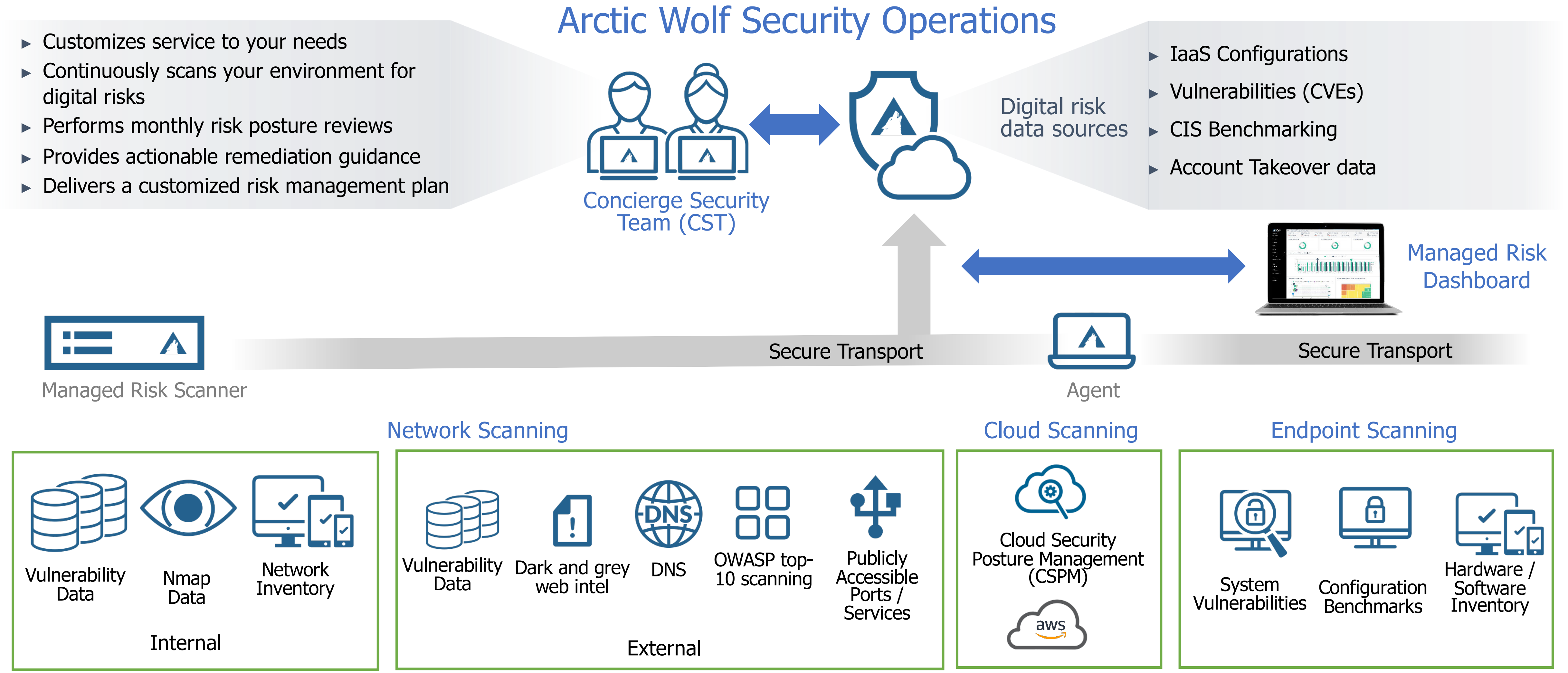
- **24x7 Continuous Monitoring**
  - Your environment is monitored around the clock for threats and risks
- **Five-Minute Response**
  - Detect and alert on critical events within five minutes
- **Real-Time Remediation**
  - Rapidly contain incidents and get detailed guidance on remediation

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

Managed Risk Architecture



Arctic Wolf Security Operations

- Customizes service to your needs
- Continuously scans your environment for digital risks
- Performs monthly risk posture reviews
- Provides actionable remediation guidance
- Delivers a customized risk management plan

Concierge Security Team (CST)

Digital risk data sources

- IaaS Configurations
- Vulnerabilities (CVEs)
- CIS Benchmarking
- Account Takeover data

Managed Risk Dashboard

Managed Risk Scanner

Secure Transport

Agent

Secure Transport

Network Scanning

Internal: Vulnerability Data, Nmap Data, Network Inventory

External: Vulnerability Data, Dark and grey web intel, DNS, OWASP top-10 scanning, Publicly Accessible Ports / Services

Cloud Scanning

Cloud Security Posture Management (CSPM)

Endpoint Scanning

System Vulnerabilities, Configuration Benchmarks, Hardware / Software Inventory

Classification: Public

Predictable Pricing

Users

Employees and SaaS Application User

Servers

Physical + Virtual Count

Sensors

One for Each Firewall

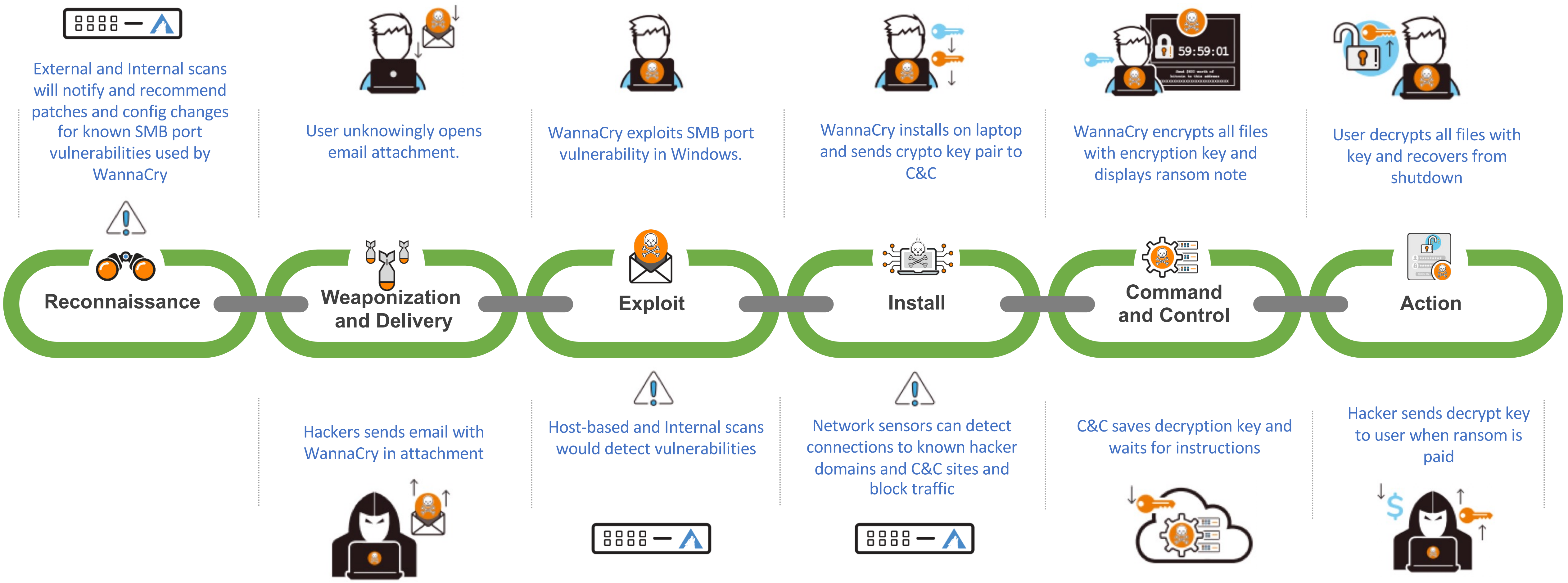
Personal | Predictable | Protection

ARCTIC WOLF

Questions

WannaCry Kill Chain

- How Arctic Wolf CyberSOC services can detect ransomware throughout the kill chain



Reconnaissance

External and Internal scans will notify and recommend patches and config changes for known SMB port vulnerabilities used by WannaCry

Weaponization and Delivery

User unknowingly opens email attachment.

Hackers sends email with WannaCry in attachment

Exploit

WannaCry exploits SMB port vulnerability in Windows.

Host-based and Internal scans would detect vulnerabilities

Install

WannaCry installs on laptop and sends crypto key pair to C&C

Network sensors can detect connections to known hacker domains and C&C sites and block traffic

Command and Control

WannaCry encrypts all files with encryption key and displays ransom note

C&C saves decryption key and waits for instructions

Action

User decrypts all files with key and recovers from shutdown

Hacker sends decrypt key to user when ransom is paid