SECUR-SERV

Tribute's Recommended IT Solutions Partner Since 1999

Cybersecurity: What's Next?

Presenter

Dave Koopmans
Manager, Solutions Engineering

Learning Outcomes

Basics: Understand the minimums involved in Security

Layers: Look at defense in layers

Monitoring: What does it take to monitor security

Proactive: Look at the strategy of proactive security

What's Next: How to prepare for the unknown

A Look at the Complexity of Cybersecurity

- The Weakest Link…….
- Company Size
- Access to Data
- Work From Home
- Policies

Agenda

1. Identification of a security breach
2. Effective security tools and solutions
3. What to do if you have experienced a breach
4. How to know if you are safe from attacks
5. Cybersecurity layers
6. Cloud Security
7. Policies

How to Tell If You Have Experienced a Security Breach

SECUR-SERV

- File integrity checking software
- Third-party monitoring services
- Operating system and application logs
- Network logs
- Staff or customers noticing irregularities in your systems/services
- Information disclosures from a vulnerability alert

Question

On average, how many days does it take to identify and contain a cyber breach?

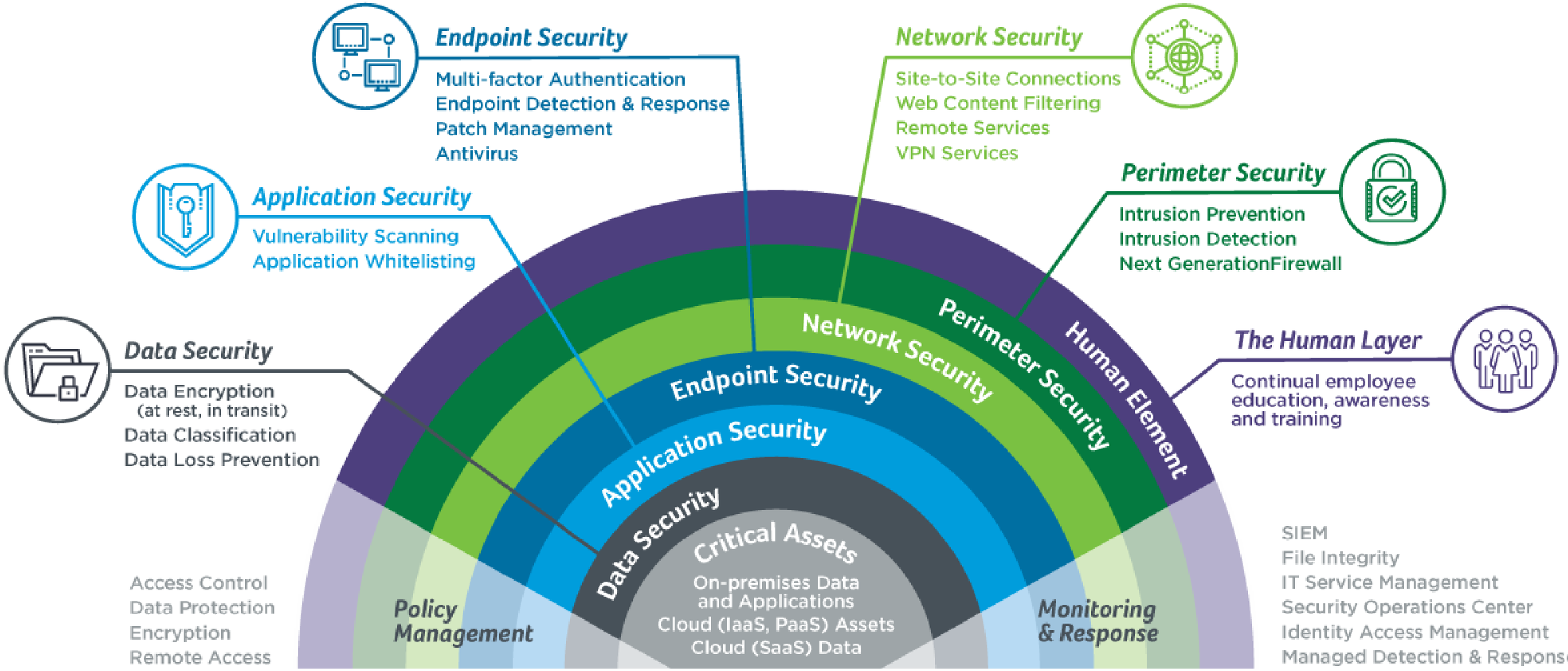
287 days

2022

Layers of Cybersecurity

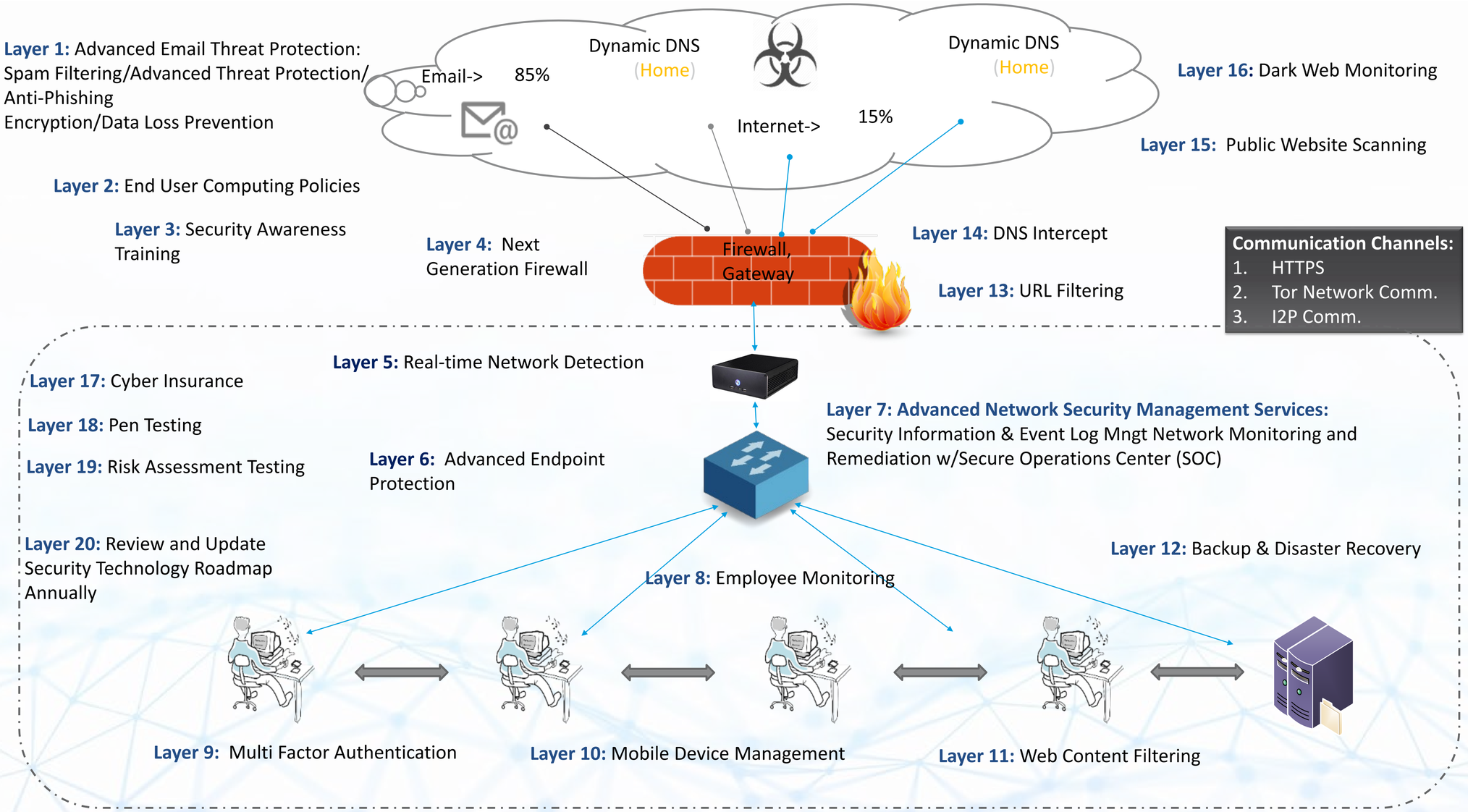
SECUR-SERV

Layered security provides depth in protecting mission-critical assets with a focus on prevention, detection, and response.



Critical Assets | Data Security | Application Security | Endpoint Security | Network Security | Perimeter Security | Policy Management | Monitor and Respond

Advanced Security Layered Approach



Perimeter Security

SECUR-SERV

Solution Type	Opportunity	Questions
Intrusion Prevention	Network Perimeter Protection	How is the network perimeter currently protected?
Intrusion Detection	Perimeter Detection	How is the perimeter currently managed?
Next Generation Firewall	Perimeter Management	How is the integrity of the perimeter monitored?

Perimeter Security is defined as controlled access to network resources via identity (authentication) and detection, includes physical security.

Network Security

SECUR-SERV

Solution Type	Opportunity	Questions
Site-to-Site Connections	Multiple Locations	How does the staff connect from one location to another?
Web Content Filtering	Network Security	Who has access to the network?
Remote VPN Services	WIFI Access Concerns	How do employees remotely access the network?

Network Security is defined as protocols and procedures to ensure unauthorized access to the network and the data flowing through it.

Endpoint Security

Solution Type	Opportunity	Questions
Multifactor Authentication	Password vulnerabilities and spoofing	Does the business need to reduce brute-force password attacks?
Endpoint Detection and Response	Knowing about and responding to threats	Does the business have a proactive or reactive stance?
Patch Management	Windows 10 and third-party updates	Who is managing updates? Auto settings do not update W10
Antivirus	Need detection and response to complete endpoint security	How are you alerted on AV issues?

Endpoint Security is the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns.

Application Security

Vulnerability Scanning	Whitelisting	Security Awareness Training
Application Tracking Software, Firmware, and Protocols	Adapting environment to access line-of-business resources	Want users and administration to be fully-vested in security
Are application network layer gaps assessed?	Are users permitted to access, install, or update applications?	How does the organization train users to protect the environment from potential threats?

Application Security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.

Data Security

SECUR-SERV

Solution Type	Opportunity	Questions
Data Encryption	Sensitive Information	What kind of sensitive data does the organization store?
Data Classification	Data Tracking	Does the organization track data access and review tracking logs?
Data Loss Prevention	Security Breach	Who in the organization is responsible for data security?

Data Security means protecting digital data from destructive forces and from the unwanted actions of unauthorized users, such as a cyberattack or a data breach.

Critical Assets

SECUR-SERV

Valuable

Essential

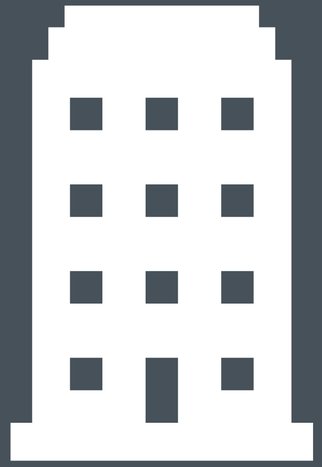
Proprietary

Organization

Resources

Products

Systems



Critical Assets are defined as items essential to the ongoing operation of an organization. If these assets become inoperable or unavailable, the organization's ability to function would be seriously impacted, or potentially, completely debilitated.

Opportunities

Does the business have a **current list** of critical assets?

How are these assets currently **protected** against cyber attacks?

What impact would **asset failure** have on the business?

Policy Management

SECUR-SERV

Policy Management refers to enforcing the policy (rules and regulations) of the organization that pertain to information and computing. Primarily focusing on database access and network resource issues: which users have access to what data and how network traffic is prioritized.

Access Control	Who manages the organization's security policies?
Data Protection	Do the existing policies meet the organization's current needs?
Encryption	How does the organization's manage policies?
Remote Access	Are the policies accessible in the event of an emergency?

Monitor and Respond

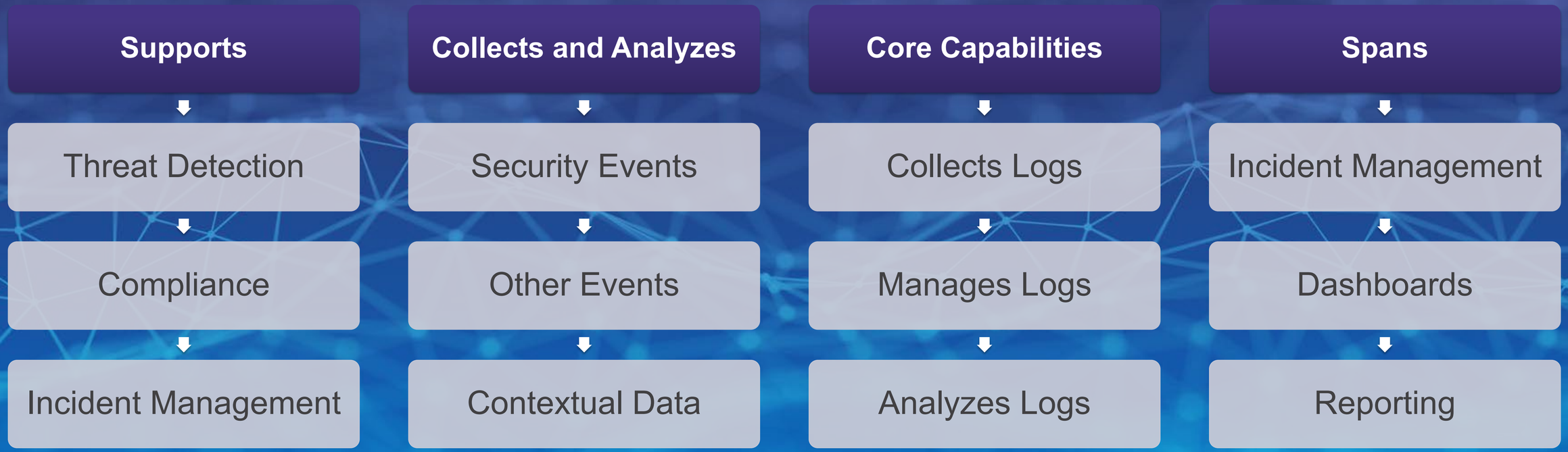
SECUR-SERV

Monitor and Response is the ability to track and measure anomalies in the network environment and respond to any such events.

- File Integrity
- IT Service Management
- Security Operations Center
- Identity Access Management
- Managed Detection and Response

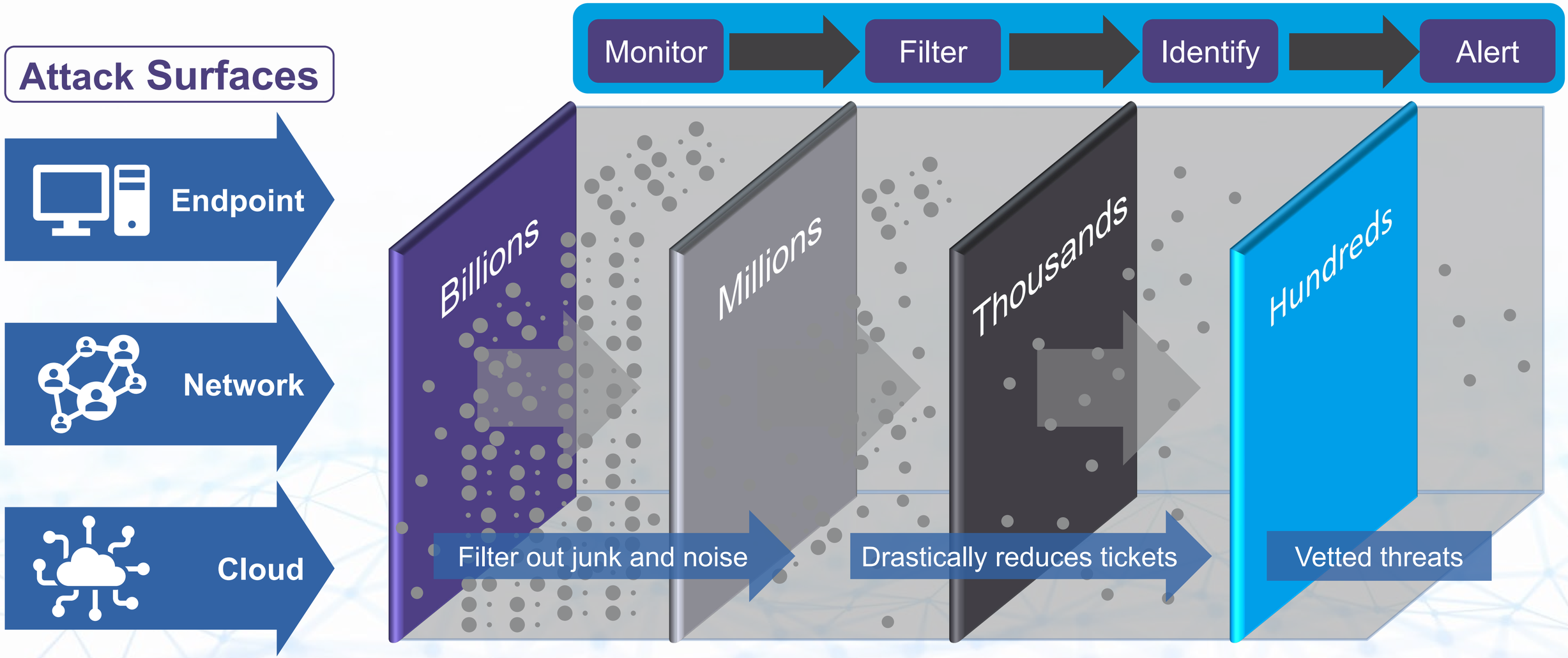
- Does the organization have a security event response plan service?
- Who provides the company's current security event response plan service?
- What elements does the security event response plan include?
- Who in the organization is responsible for security event management?

Security Incident and Event Management – SIEM



Solution Platform

SECUR-SERV

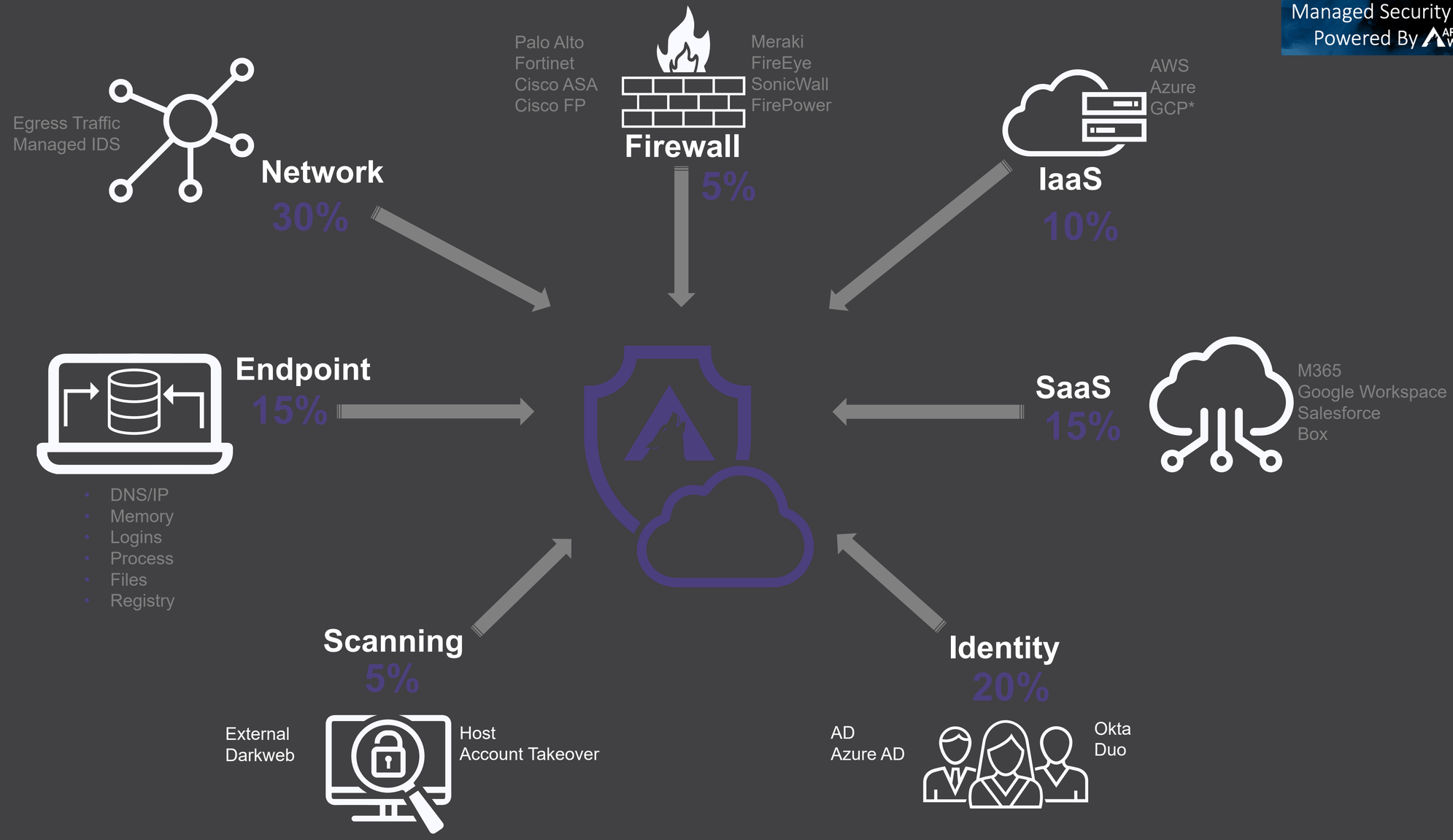


SECUR-SERV

Managed Security Operations
Powered By ARCTIC WOLF

Arctic Wolf Broad Visibility

Percentage of Ticketed Incidents from Telemetry Sources



AW Security Operation Workflow

THE ARCTIC WOLF PLATFORM

FW/UTM Logs
Flow Data
DNS Logs
Active Directory
Vulnerability Data
IDS Alerts
Nmap Data
Wireless AP

Office 365
okta
aws
Azure
WEBROOT
Windows Defender ATP
MANY MORE

System Vulns
Wireless Networks
Process Tables
Applications Installed
Sysmon monitoring
Containment

Arctic Wolf Physical Sensor
Integrations (API/Syslog)
Arctic Wolf Agent

THE ARCTIC WOLF TRIAGE TEAM

THREAT INTEL FEEDS
TRIAGE BOARD
~300 per week
1-2 tickets per week!
TICKET
VERIFIED POSITIVE

TRIAGE SECURITY ANALYST I & II
TRIAGE SECURITY ENGINEER III
Deep Investigations
On-demand virtual support

CONCIERGE SECURITY TEAM

REMEDIATE & RECOVER
SECURITY JOURNEY

The customer's Concierge Security Team reviews the incident with the customer team. Any learnings will be used to further harden the customer's environment against future attacks by customizing the customer's deployment.

~85M per week
INGEST
PARSE
LOG STORAGE

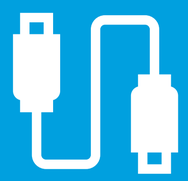
MDR and VA Comparison

SECUR-SERV

	Acronym	Definition	Primary Capabilities
	MDR Managed Detection and Response	Outsourced cybersecurity services designed to protect data and assets even if a threat eludes common organizational security controls.	• **Reactive** • Threat hunting • Alert response • Incident response
	VA Vulnerability Assessment	Proactively eliminates risks and reduces exposure while providing visibility into the Cloud (EVA) and network (IVA) infrastructure.	• **Proactive** • Assesses risks • Closes gaps in security posture • Reduces likelihood of attacks

SECUR-SERV

Endpoint Security Review

Acronym	Definition	Primary Capabilities
	**EDR** Endpoint Detection and Response	Records and stores endpoint-system-level behaviors using analytics to detect suspicious activity, block malicious activity, and provide restoration remediation suggestions.	• Detect security incidents • Contain incident at endpoint • Investigate security incidents • Provide remediation guidance
	**NGAV** Next Generation Antivirus	Prevent all types of attacks, known and unknown, by monitoring and responding to attacker tactics, techniques, and procedures (TTPs).	• Machine learning and AI • Kill and quarantine • Offline functionality • Rollback
	**MDR** Managed Detection and Response	Outsourced cybersecurity services designed to protect data and assets even if a threat eludes common organizational security controls.	• Threat hunting • Alert response • Incident response
	**XDR** Extended Detection and Response	SaaS-based security threat detection and incident response tool that integrates security products into a single security operations system, unifying all licensed components	• Managed by SOC experts • Correlation of multiple security controls

SECUR-SERV

Managed Security Operations Powered By ARCTIC WOLF

Where companies want to be

Scantron Managed Security Operations

GAP

Where most companies are today

BUSINESS RESILIENCE

Proactive

Confident

Compliant

Insurable

DEFENSE-IN-DEPTH

Endpoint (AV, AEP)

DLP / SSL Inspection

Anti-DDoS / IPS / CASB

PERIMETER

Firewalls

SPAM / Web Filters

WAF / Proxy

BASIC

Passwords / AD

Patch Management

Backups

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

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

SECUR-SERV

What to Do If You Have Experienced a Breach

How to Know If You Are Safe From Attacks

SECUR-SERV

- Do you assess your cybersecurity program ensuring it is delivering what you need it to deliver?
- Do you currently engage in security assessments?
- Do you scan for vulnerabilities?
- Do you have a SIEM to monitor the entire infrastructure?
- Have you trained your users to identify potentially malicious activity?
- What specific types of attacks might be targeting your organization?
- Do you know how to properly respond to an attack? Does your organization?

Email Security Basics

SECUR-SERV

SPAM Protection

- Whitelist and Blacklist

Email Encryption

- TLS

Data Loss Prevention (DLP)

Email Archiving

Email Backup

Multi-factor Authentication (MFA)

- Vendor and deployment options
- 99% reduction is account take-overs

Advanced Email Security

Advanced Threat Protection (ATP)

URL Protection

Sandboxing

- Link or attachment

Security Awareness Training

Email Hardening

- DNS Records – SPF, DKIMM, DMARC
- Disable defaults – POP, IMAP, PowerShell

Conversion to Cloud - Considerations

SECUR-SERV

What infrastructure do you have today?

- Is it secure?
- How reliable is your internet?
- How much bandwidth do you have?
- What applications are NOT going to the cloud?
- Do you have an active directory domain?
- What are your backup – BC/DR needs?
- How do you print today – network or local?
- Do you have a cloud goal?
- OpEx versus CapEx

What is Cloud Computing?

SECUR-SERV

LOCATIONS

Shared resources among a community of users

Public Cloud

Service that is controlled and exclusive to the user

Private Cloud

Ability to move workloads between private and public platforms.

Hybrid Cloud

SERVICES

IaaS
Infrastructure as a Service

Outsource the elements of infrastructure like Virtualization, Storage, Networking, Load Balancers

PaaS
Platform as a Service

Core hosting operating system and optional building block services that allow you to run your own applications

SaaS
Software as a Service

Consumed as a service only for the applications needed

Pros +

- Scale and Cost
- Choice and Agility
- Encapsulated Change Management
- Next Generation Architectures

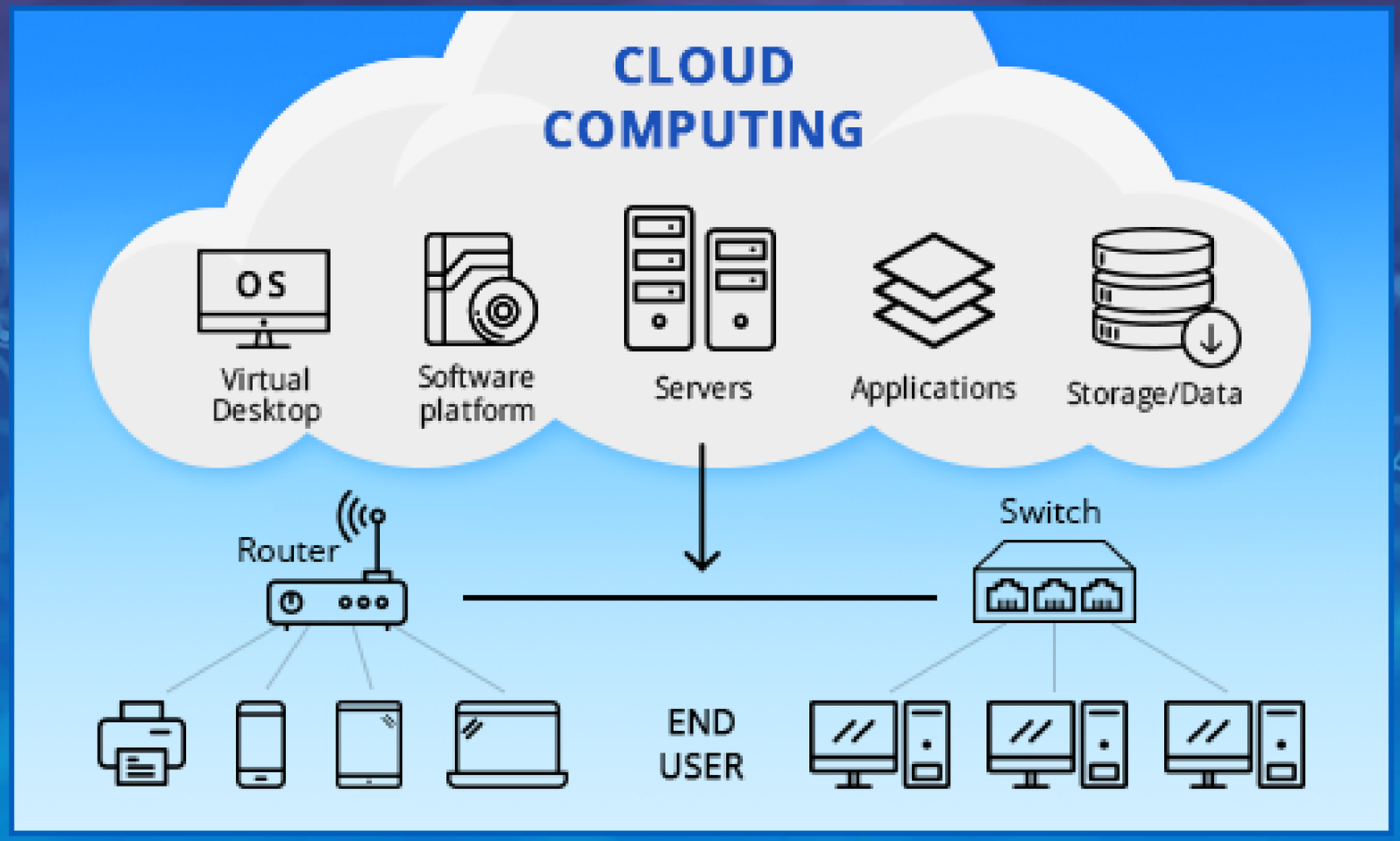
Cons -

- Lock-in to service
- Security (Hacking)
- Lack of control and ownership
- Reliability

What Do You Need?

SECUR-SERV

What is needed for the user	• Type of device • Type of connection
What is needed for security	• Endpoint security • Network security
What the cloud removes if you are 100% cloud	• Server(s) • Backups* • Updates*



Cybersecurity Scenarios

SECUR-SERV

Email Hacks – caused by

- Weak Passwords
- Passwords found on other site hacks
  - Re-using passwords
- No Email MFA
  - Reduces this by 99%

Email Phishing – caused by

- Lack of Security Awareness Training
- Lack of Advanced Threat Protection
- Email Tennant not hardened
  - Removing defaults creating SPAM records in DNS

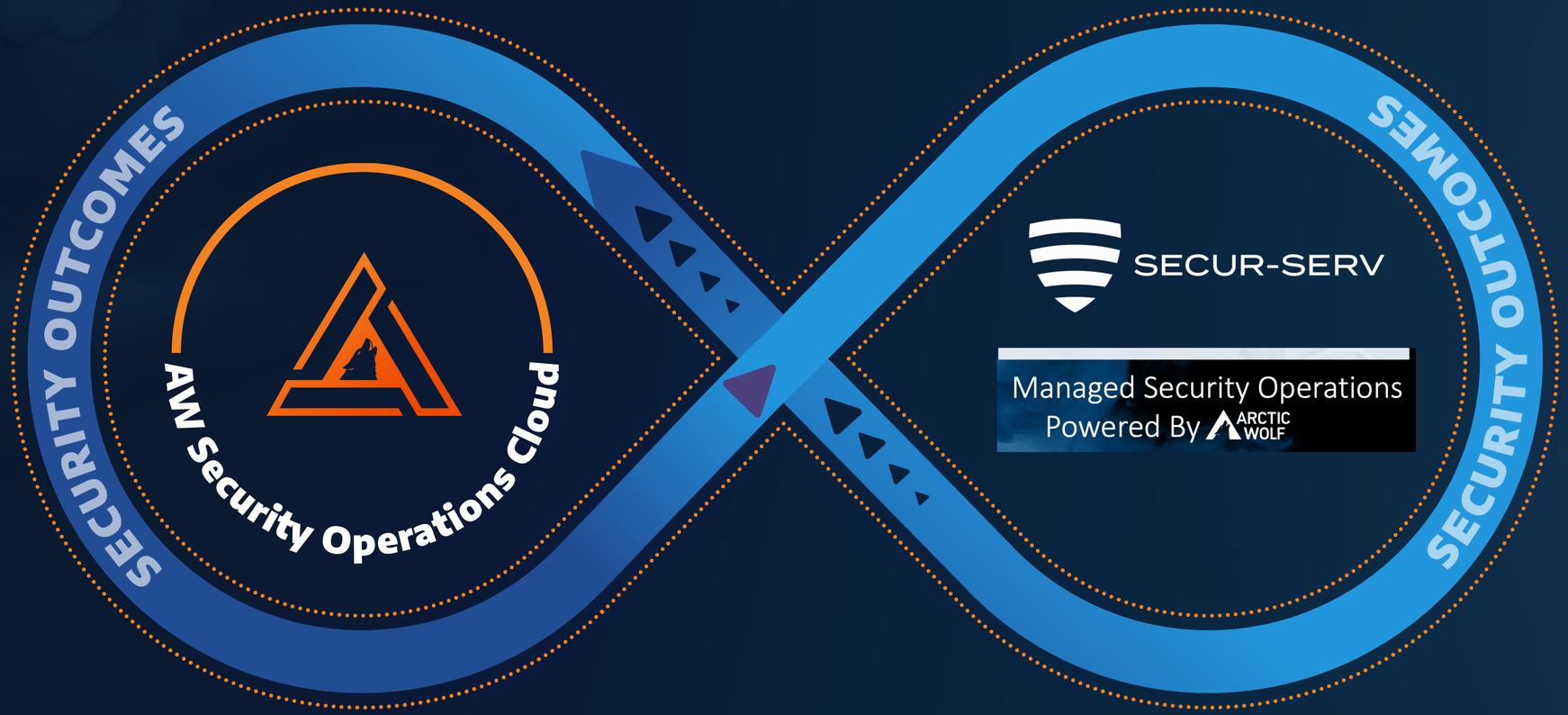
Ransomware/Malware – caused by

- 90% email hacks or phishing
- DNS Web Filtering not in place
- NextGen Firewall not in place
- NextGen Antivirus not in place
- Monitoring not in place

Being Protected vs being Targeted

- All Endpoints are targets
  - Internal and external users and vendors
- Software Vulnerabilities due to lack of patching
- Bad actors on your network for most of a year
- MFA not in place on all remote and local logins

The Collaborative Model



Benefits

- Dedicated security operations resources (Arctic Wolf and Secur-Serv)
- Tailored tuning & optimization to your business context
- Deliver threat intelligence and situational awareness
- Implement a proactive Security Journey

Security is a Journey; Not a Destination

Customer

SECUR-SERV

Managed Security Operations
Powered By ARCTIC WOLF

- Cyber Risk Reduction
- Ensuring Insurability
- Fast Time Security Value
- Eliminate Blind-spots

Recap

Weakest Link

Cybersecurity Introduction

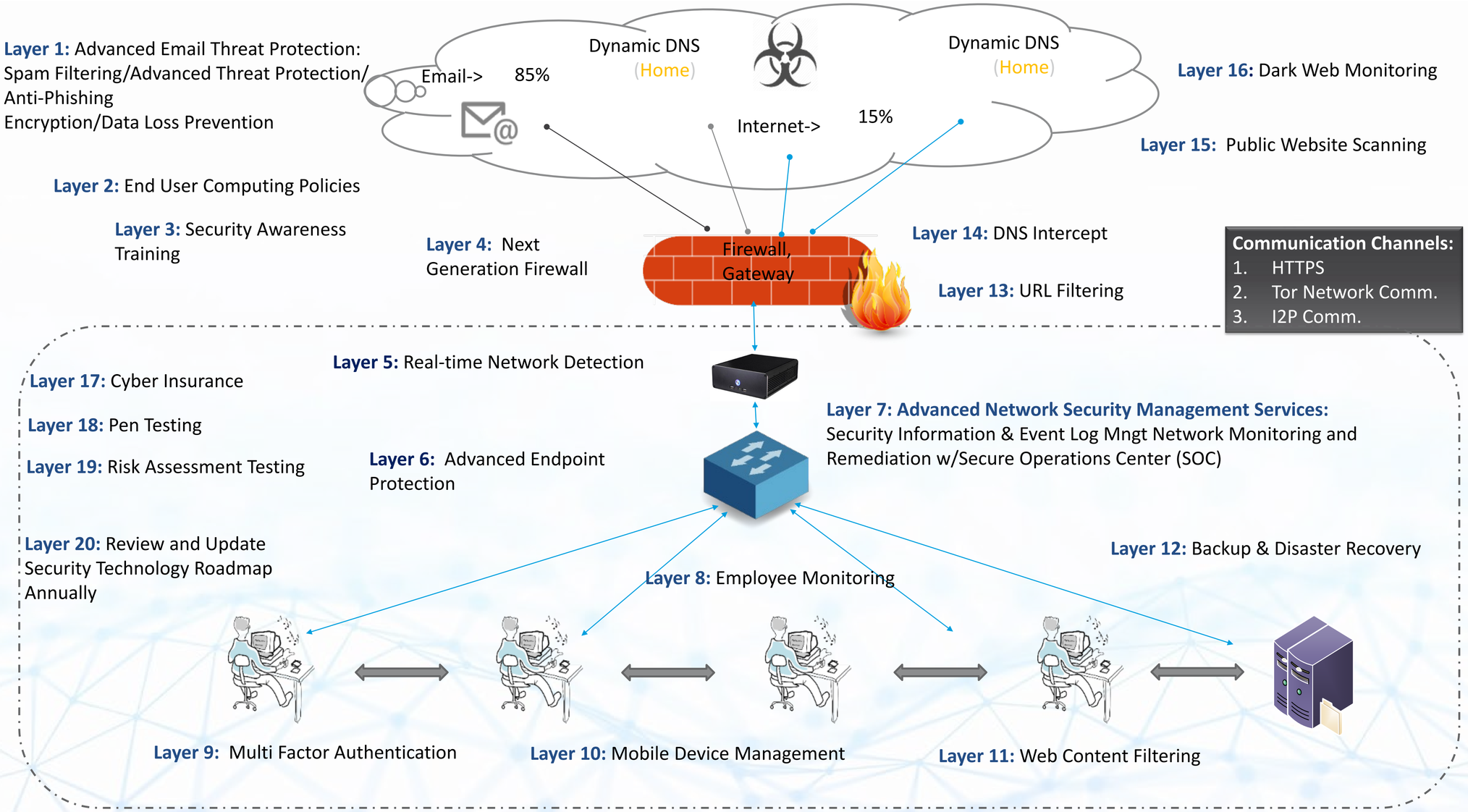
- EndPoint Protection
- Email Protection
- SIEM/MDR

Cybersecurity Layers Graphic

- Each layer has unique Security Requirements

Cloud Computing

Advanced Security Layered Approach



Why Scantron Managed Security Operations?

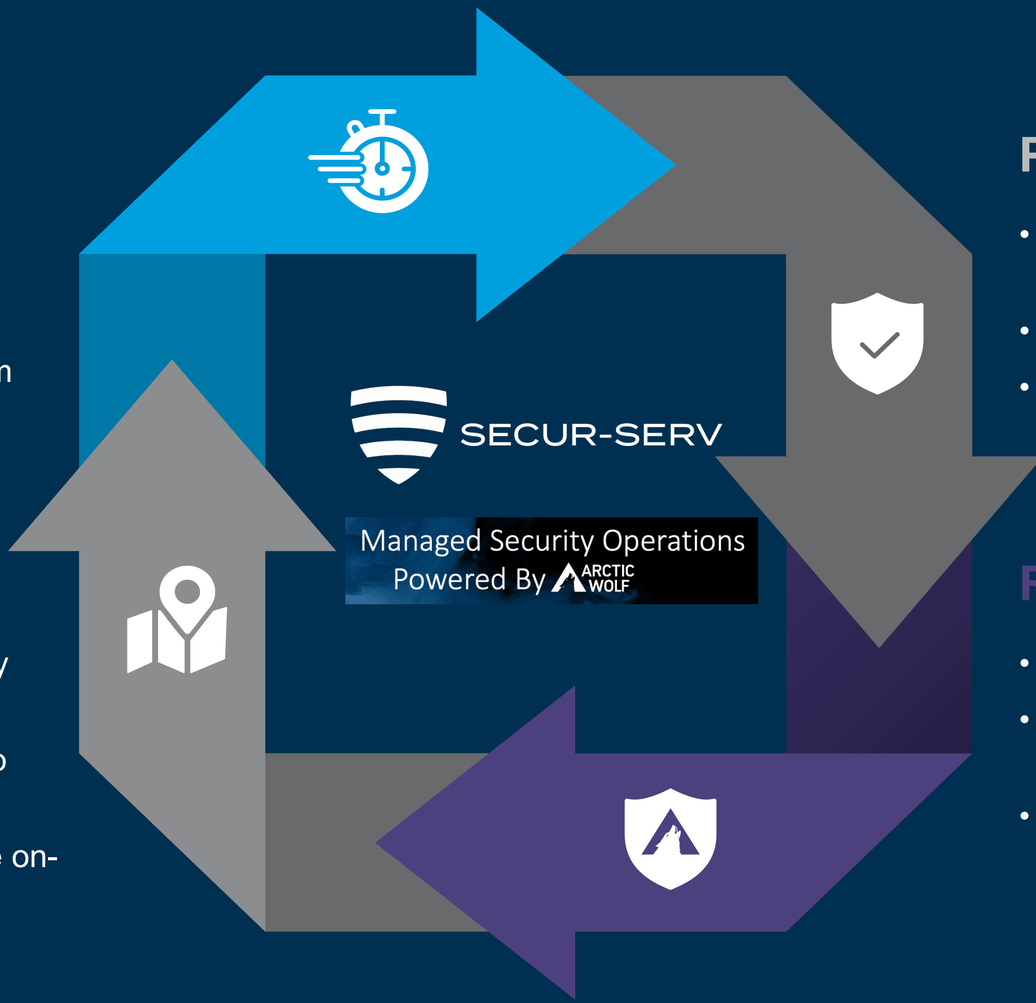
Secur-Serv and Arctic Wolf security experts combine their years of security experience with an innovative Security Operations platform to put your organization on the journey to **End Cyber Risk**

Time to Value

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

Guidance

- Collaborative 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

SECUR-SERV

Questions?