



THE LEADER IN **SECURITY OPERATIONS**

Cyber Insurance and Arctic Wolf



Odin Olson

Vice President of Business Development

- Alliances, OEM, M&A at Arctic Wolf
- Almost 20 Years in Cyber Security



David Kruse

Director, Business Development

- Digital Forensics, Incident Response, and Insurance expert
- Former Insurance Cyber Practice Leader
- CISR

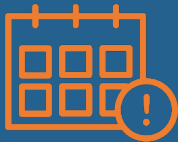




Cyber-attacks are **up by 93%.** –Information Week



In 2020, more than **61% of companies** were subject to ransomware demands. -Mimecast



In a recent Hanover Insurance Group study on cyber insurance, 60% of respondents said it would **take 2 days to become unprofitable** if they lost access to critical systems/data.

-Hanover Insurance Group



What Isn't Cyber Insurance?

Property Insurance

General Liability Insurance

Directors & Officers



What isn't Cyber Insurance?

Sounds like Cyber Insurance. Sounds Like Technology

- **Electronic Data Processing Property Coverage**
- **Electronic Data Liability**
- **Tech Errors & Omissions (E&O)**
- **Data Compromise/Data Breach Liability**



What Cyber Insurance Is...

Cyber liability insurance can cover costs associated with data breaches and cyber attacks on your business. Those costs can include such things as lost income due to a cyber event, costs associated with notifying customers affected by a breach, costs for recovering compromised data, costs for repairing damaged computer systems and more.

Travelers Cyber coverage can be a crucial safeguard against the devastating financial consequences of a cyber attack. Travelers offers customized insurance solutions depending on your business' level of risk, with coverage options available to address:

- forensic investigations,
- litigation expenses,
- regulatory defense expenses/fines,
- crisis management expenses,
- business interruption,
- cyber extortion, and
- Betterment.



This insurance helps you respond to a breach if PII or PHI gets lost or stolen, whether it's from a hacker breaking into your network, or an employee accidentally leaving their laptop at a restaurant.

If your small business is the victim of a breach, data breach coverage can help pay to:



Notify affected customers, patients or employees

Hire a public relations firm

Offer credit monitoring services to data breach victims

Cyber Insurance

Cyber Insurance can include coverage for first and third party losses

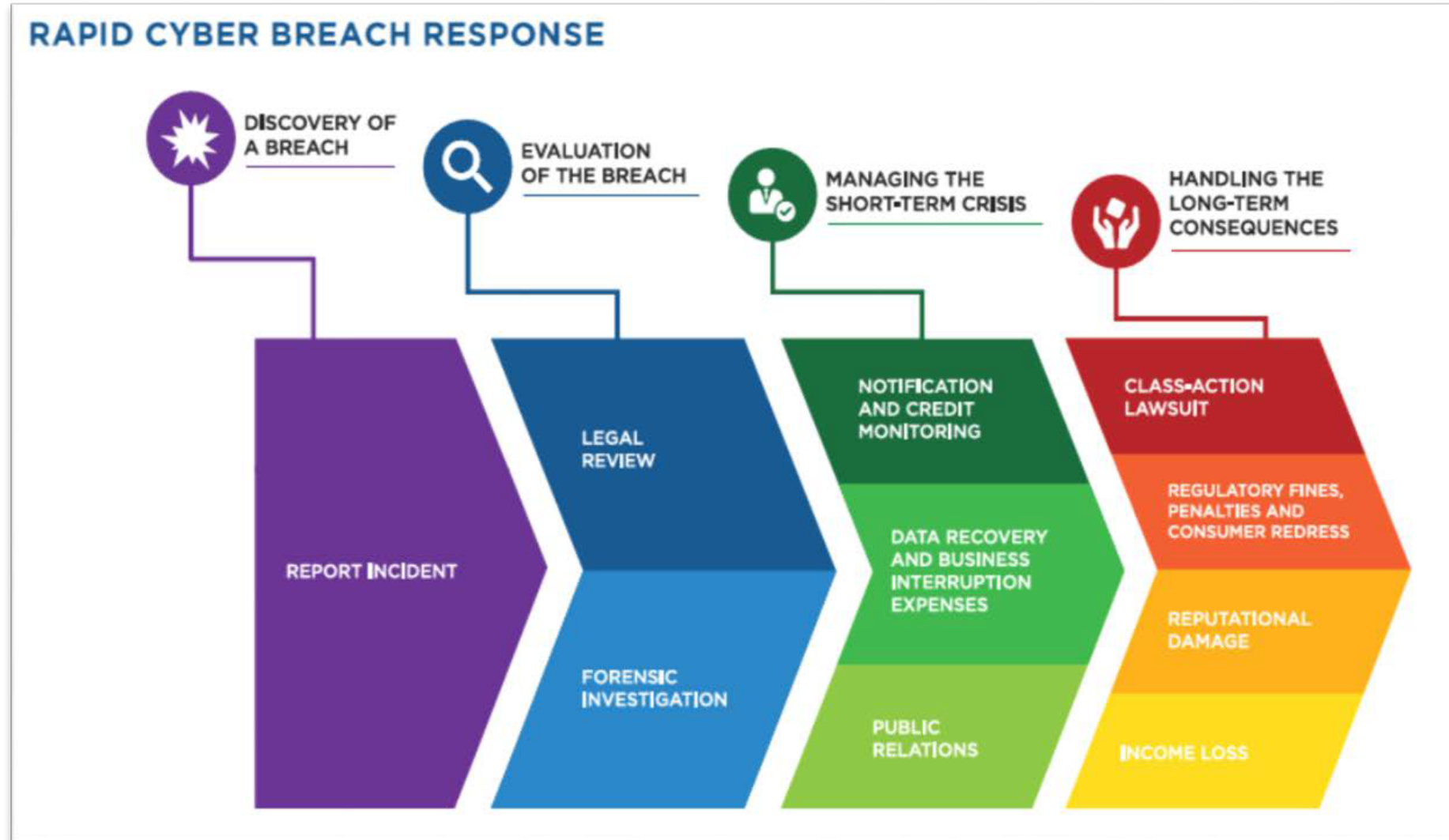
First Party losses

- **Ransomware**
- **Extortion**
- **Phishing Scams**
- **Operational Interruption**
- **Asset Corruption**

Third-Party losses

- **Privacy Lawsuits**
- **Regulatory Investigations**
- **Regulatory Fines**
- **Online Libel/Slander/Defamation**

How the policy works in the event of a claim



Myths Of Cyber Insurance

1. My property policy **covers my computers**, so I'm all set.
2. I have general liability insurance, so I don't need this.
3. Cyber insurance is **too costly** for us.
4. My money is **better spent on security controls**.
5. My IT department takes care of security, so we're not at risk.
6. Cyber insurance coverage is **very narrow in scope**, so it's not worth it.
7. All cyber insurance **policies are pretty much the same**.
8. Cyber Insurance **never pays out**.



Policy Pitfalls

1. Low sublimits for first-party losses
2. Due-diligence conditions
3. Nasty call-back provisions
4. Not triggering extra breach response costs
5. Named malware sublimits
6. Limited/excluded coverage for non-panel providers
7. Cyber Terrorism excluded

Limit(s) of Liability for each Policy Year:

- (a) \$1,000,000 for all **Data Compromise**
- (b) \$1,000,000 for all **Claims**. This Limit is:
☒ part of and not in addition to the Limit of Li
☐ a separate Limit and in addition to the Limit

Subject to the following Retentions:

Insuring Agreement I.A:	\$5,000	Eac
		Rej
Insuring Agreement I.A:	24 hours Waiting Period	Eac
Insuring Agreements I.B:	\$5,000	Eac

Prior & Pending Litigation Date (applicable to Insuring Agreement I.B):

Premium: \$3,675

Retroactive Date (applicable to Insuring Agreement I.B): 6/5/2010



Cyber Insurance Challenges

What is happening in the Market

Reduced Coverage

- Reduction in overall benefits, which includes ransomware carveouts, while having insufficient security
- "We continue to carefully reduce cyber limits, include tougher T&Cs, b/c of ransomware, 'systemic' cyber risk"
– [AIG CEO](#)

Increased Rates













- Pricing for cyber insurance is increasing
- It is not uncommon to have rates **doubling**

New Requirements

- Cyber insurance providers are requiring additional **security tools and controls** in place to continue insurability
- "In Q2 2021, underwriting tightened significantly for troubled lines like Cyber...Additionally, capacity contracted for both of those lines, with more than 80% of respondents reporting a decrease in capacity for Cyber." – [CIAB Q2 2021 Cyber Report](#)



Insurance Company Security Controls

Key Control	Arctic Wolf Solution	Key Control	Arctic Wolf Solution
MFA-Controlled Access		Protected Privileged Accounts	
Secured & Tested Backups		Secured Endpoints	
Managed Vulnerabilities		Logged & Monitored Network	
Patched Systems & Applications		Phishing-Aware Workforce	
Filtered Emails & Web Content		Hardened Device Configuration	
Protected Networks		Prepared Incident Response	



Solves for



Strengthens or supports



What Can you do?

Read/evaluate your policy if you have one

- Technical stakeholder input
- Legal and risk stakeholder input

Start early

- Don't wait for your broker
- You may need time to search, and time to implement controls

Be prepared to deploy technology – reach us if you need referrals

- MFA is table stakes
- EDR or equivalent is nearly as common a requirement

Build a case – underwriting is an application AND the story

- Write a cover letter to go with the application
- Be prepared with context about the business and controls in place today



What Can you do? continued

Get a team together – individual expertise should be shared

- Legal, risk, IT, security, Finance

Understand your actual risks/level

- Use a third party to assess risk
- Quantify as best as you can
- Get the right policy for the business

Consider what your broker offers

- You may want to do some of your own searching
- Get second opinions

Connect with Peers

- Pricing
- Coverage
- Brokers and Carriers





Security Operations for Microsoft Products and Services

Visibility

- Arctic Wolf provides unified security visibility across Microsoft tools with a suite of key integrations
- Arctic Wolf's security operations process delivers actionable security outcomes atop Microsoft alerts

Reporting

- Arctic Wolf's standard and custom reporting provides clear technical and executive visibility into Microsoft security, risks, threats, and incidents

Guidance

- Arctic Wolf's Security Journey and ongoing concierge model provides clear guidance on security best practices for Microsoft users



Microsoft Product Integrations

ARCTIC WOLF SECURITY OPERATIONS CLOUD

IDENTITY



Active Directory

Active Directory is the leading enterprise identity management tool and a key security data source

ENDPOINT



Microsoft Defender provides visibility into processes and events across devices

IAAS



Azure data helps detect attacks on cloud and provide intel for cloud security posture management

SAAS



Office 365 data can help detect BEC, phishing, and other SaaS attacks

CASB

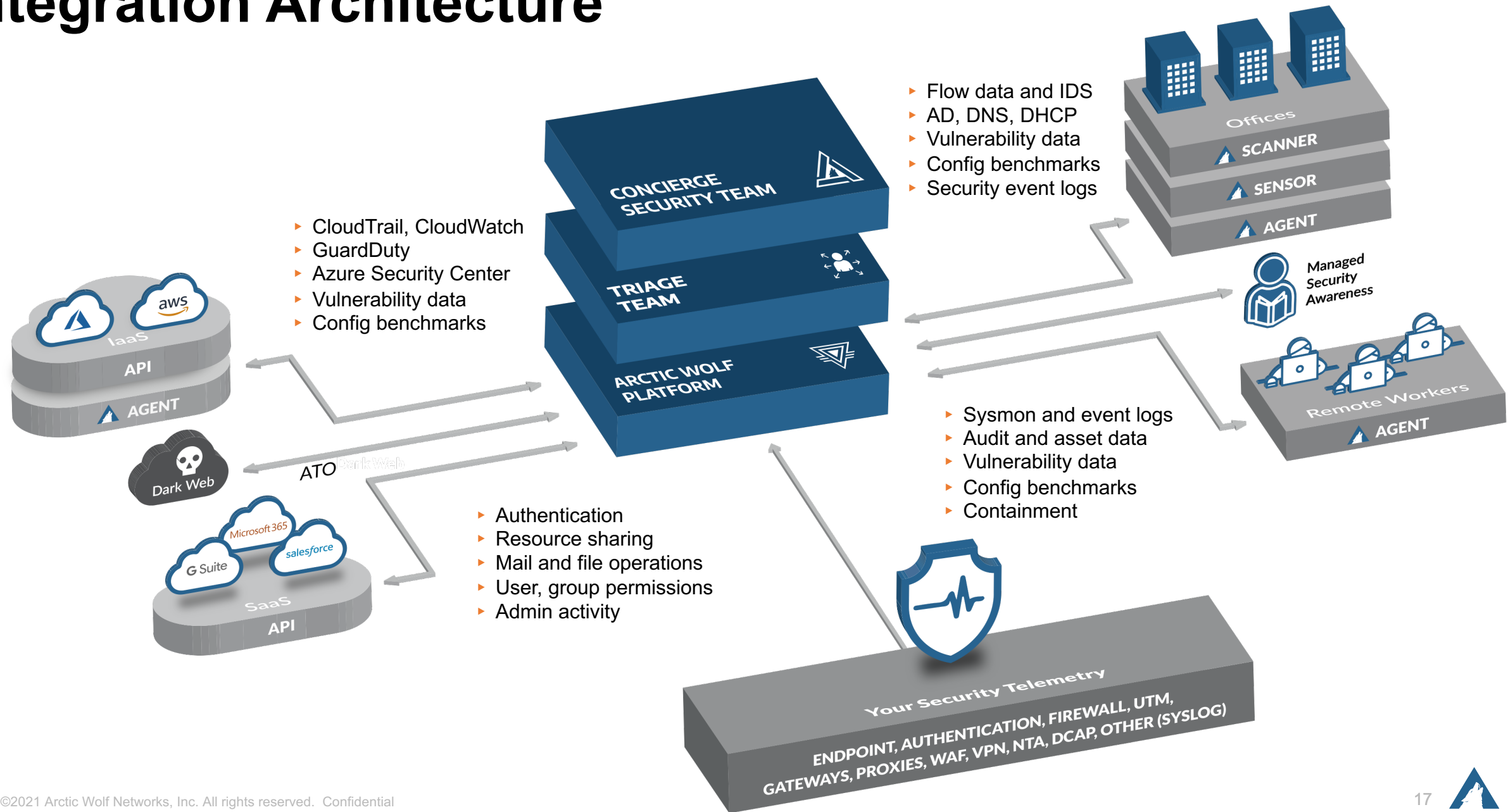


Defender for Cloud Apps provides security visibility into cloud apps and resources

← Microsoft Security Data →



Integration Architecture



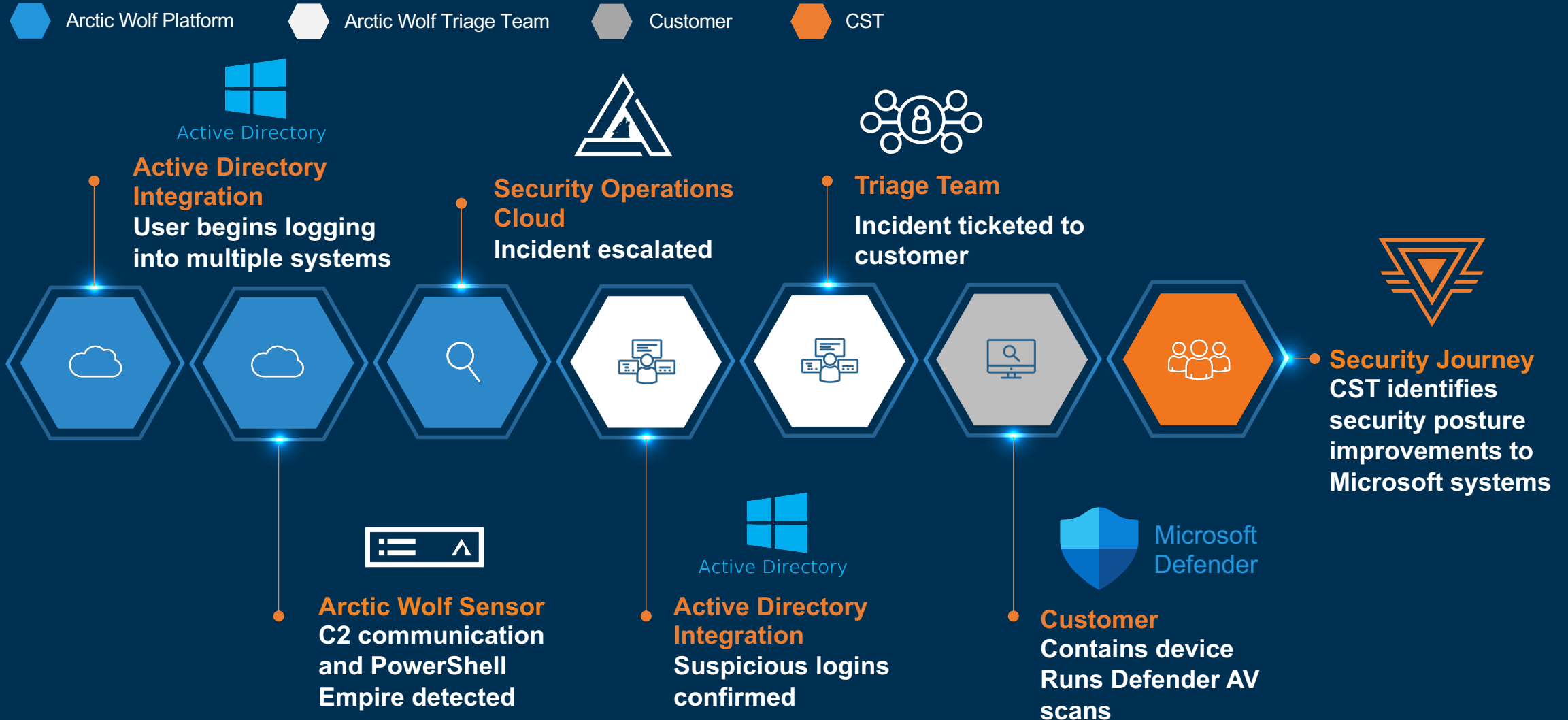


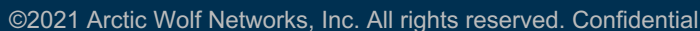
INCIDENT TIMELINES

Microsoft Integrations



Ransomware Attack – Local Government





Key Takeaways – Microsoft and Arctic Wolf



Existing Technology

Active Directory, Defender,
Azure, Office 365



Concierge Integrations

Designed, configured, delivered



Deploys in 60 Days

Ready to secure your customers



Key Takeaways – Cyber Insurance

Cyber Insurance plays an important role in overall risk management, and despite the myths, every organization should endeavor to **get covered**.

Technical Controls, Security Tooling and Operations play a vital role in continued ability to access coverage available in the market. The market is rapidly evolving.

Start Early, with the **full team** you'll need to be successful and you'll likely avoid headaches, and land with a policy that best serves your organization

