ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

Two Simple ways to dramatically improve your security posture and insurability

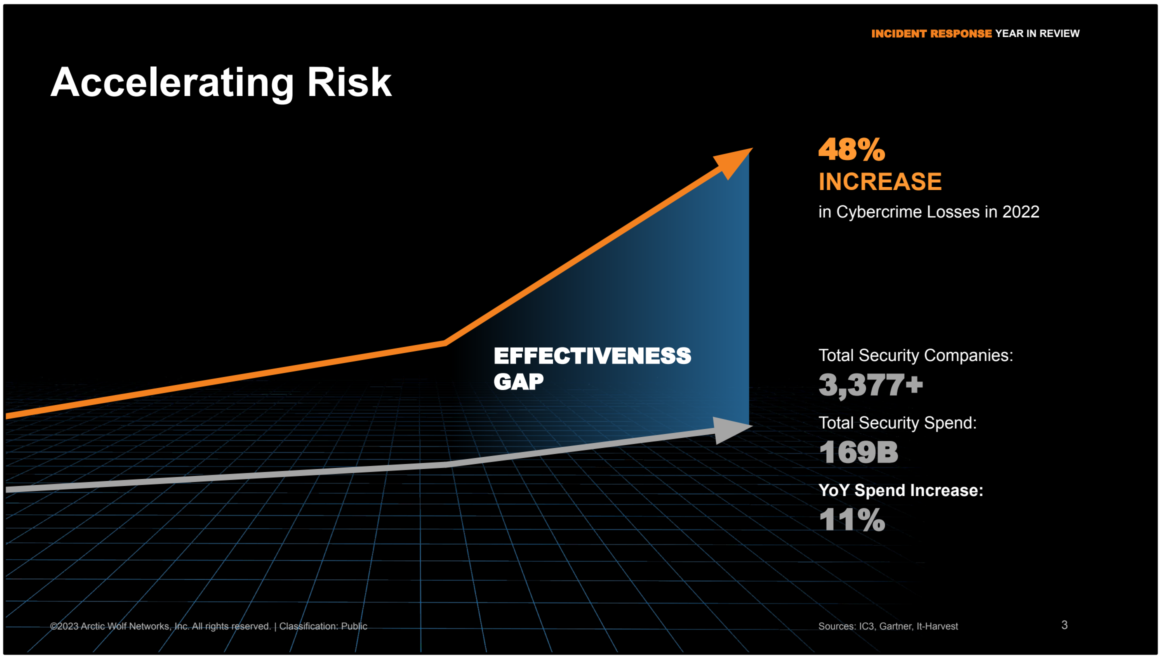
Tim DeWaard | RVP Sales Engineering

AGENDA

Cyber Insurance

Breaches and IR

What to do



INCIDENT RESPONSE YEAR IN REVIEW

Accelerating Risk

48%
INCREASE
in Cybercrime Losses in 2022

Total Security Companies:
3,377+

Total Security Spend:
169B

YoY Spend Increase:
11%

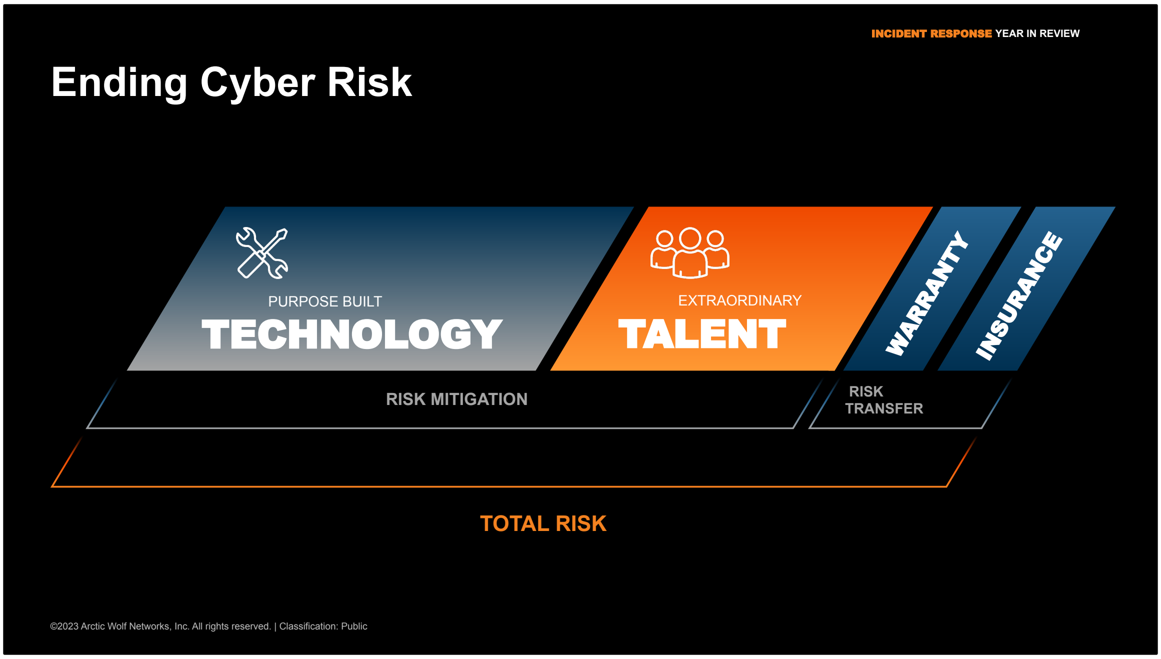
Sources: IC3, Gartner, It-Harvest

3

It’s not just that the we are still seeing a lot of cyber risk in the market – the problem is that cyber risk is actually accelerating a higher rate than investment.

We know IT and security leaders are trying to do the right thing. They are investing money, time and energy into trying to protect themselves. We have over 3,000 security companies, mostly tool vendors, to choose from. And with nearly 170B being spent at 11% year over year growth, the problem doesn’t seem to be on the buyer side of things. As an industry we are getting a negative return on investment. Something must change. Security operations is how we break the cycle.

Damage caused by cyber crime
$3 trillion in damages to global businesses in 2015
$6 Trillion in 2020
$8.6 Trillion in 2022
Projected $10.5 Trillion in 2025



INCIDENT RESPONSE YEAR IN REVIEW

Ending Cyber Risk

PURPOSE BUILT

TECHNOLOGY

EXTRAORDINARY

TALENT

WARRANTY

INSURANCE

RISK MITIGATION

RISK TRANSFER

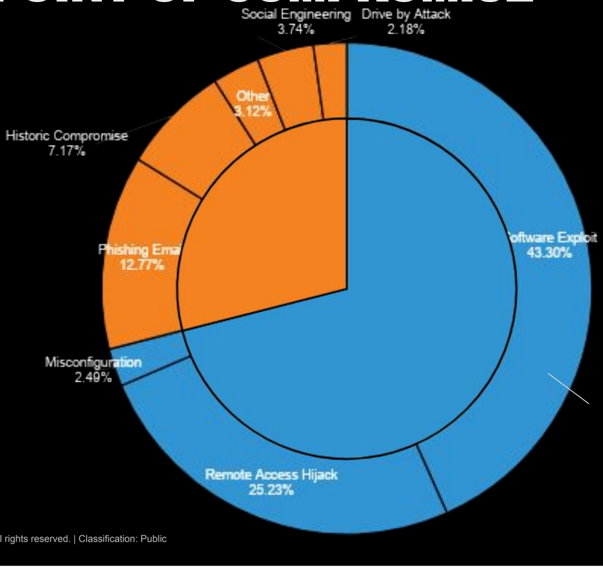
TOTAL RISK

This effectiveness gap we see is because most people start in on trying to solve their problem with tools and technology. Tools and technology are important and necessary, but alone are not enough. Technology must be purpose built to combine with extraordinary talent. It's this combination of the two working together that proves the means to actually mitigate risk by reducing likelihood and impact.

Now having a fully operationalized security operations solution will get you pretty far. We think about 98% of the way there. But what do you do with the last 2%? The answer is though a combination of warrants and insurance, the goal should be to transfer the remainder of your risk to someone else.

This holistic approach that combines risk mitigation and risk transfer is how we end cyber risk for our customers.

ROOT POINT OF COMPROMISE



Arctic Wolf Incident Response

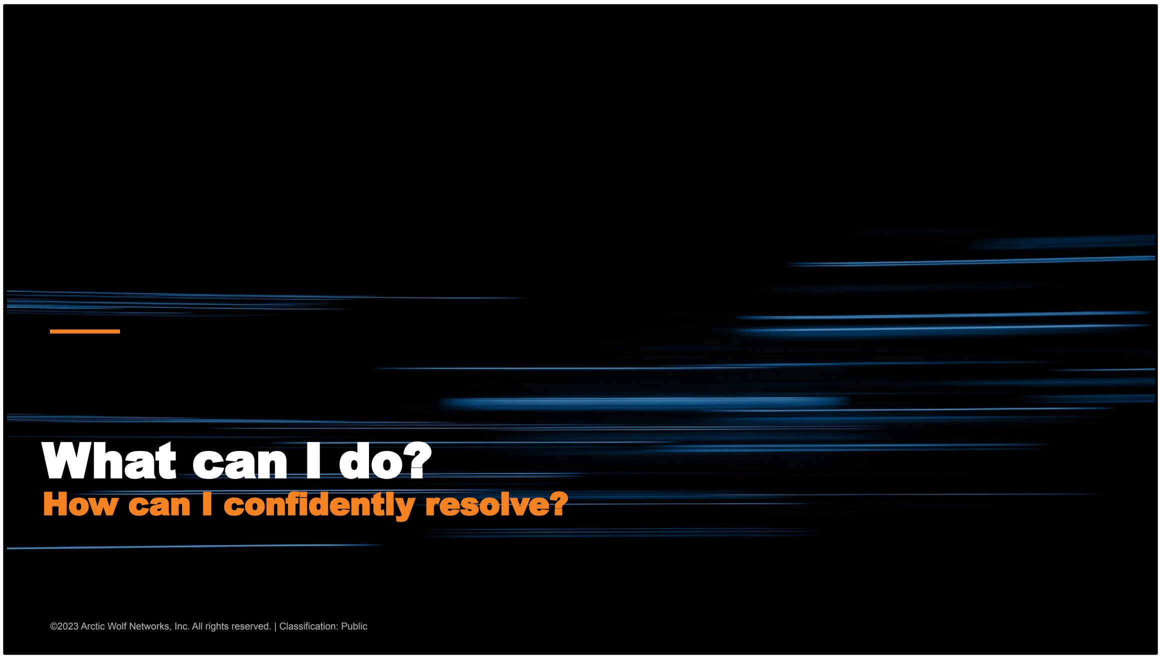
INCIDENT RESPONDERS:
~100

CORE SERVICES:
- Digital Forensics
- Restoration & Remediation
- Threat Actor Negotiation

CASES:
MORE THAN 1,000 / YEAR

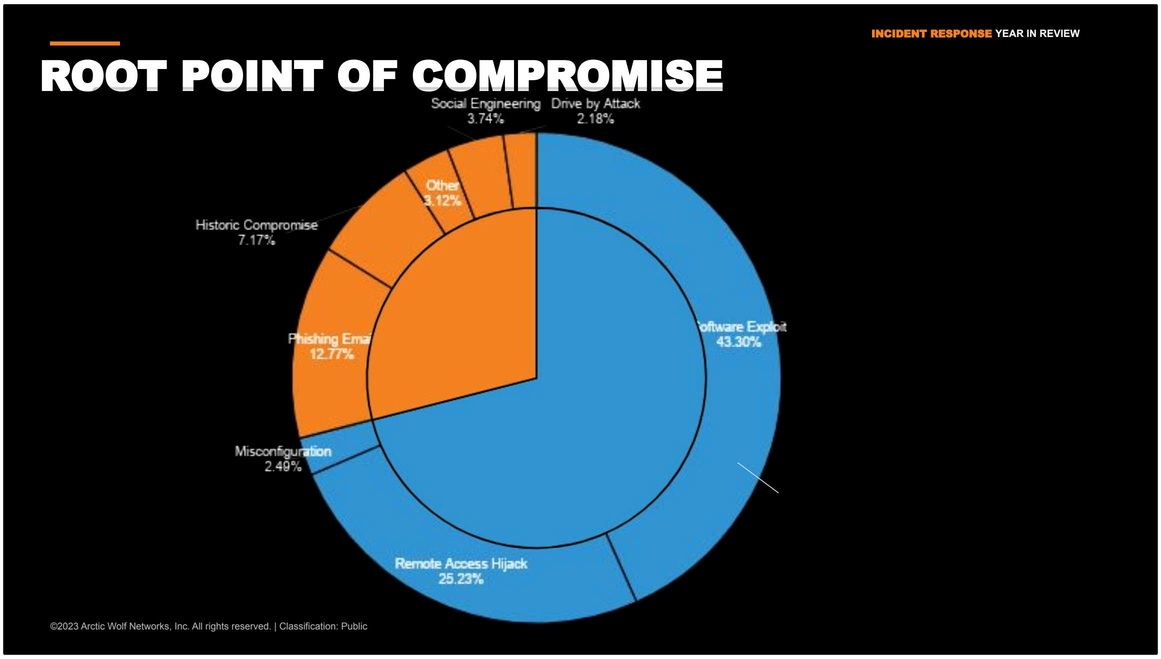
RESPONSE EXPERIENCE:
ALL THREAT TYPES

Insurance Partners
Over 30 Panels



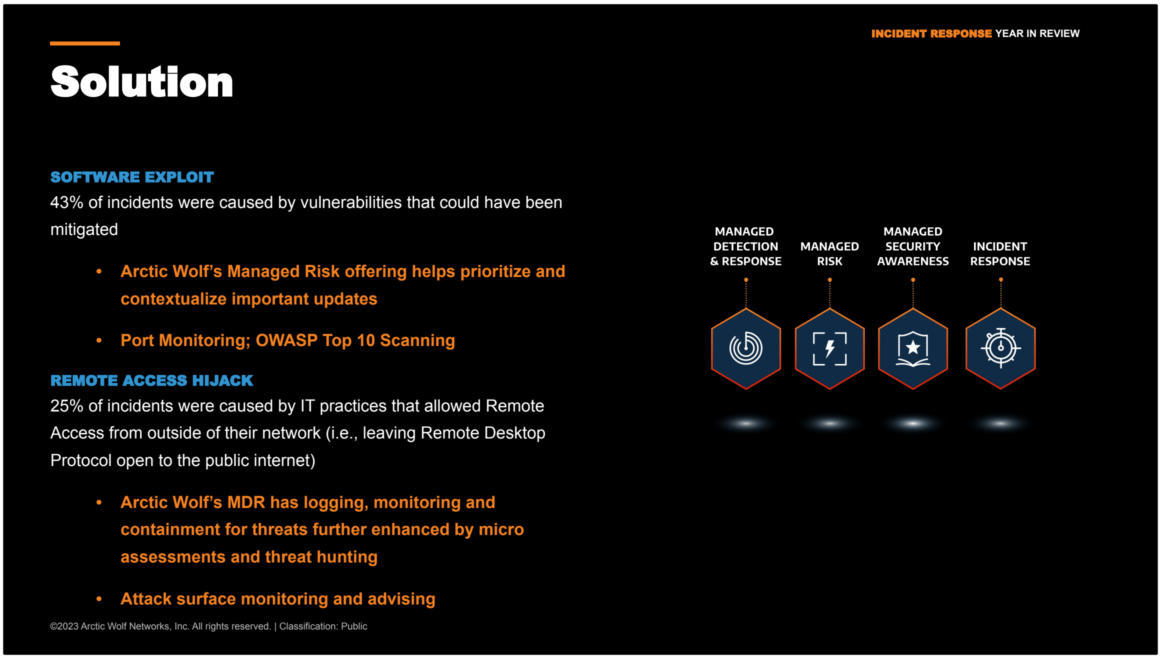
What can I do?

How can I confidently resolve?



INCIDENT RESPONSE YEAR IN REVIEW

ROOT POINT OF COMPROMISE



Solution

SOFTWARE EXPLOIT

43% of incidents were caused by vulnerabilities that could have been mitigated

- **Arctic Wolf’s Managed Risk offering helps prioritize and contextualize important updates**
- **Port Monitoring; OWASP Top 10 Scanning**

REMOTE ACCESS HIJACK

25% of incidents were caused by IT practices that allowed Remote Access from outside of their network (i.e., leaving Remote Desktop Protocol open to the public internet)

- **Arctic Wolf’s MDR has logging, monitoring and containment for threats further enhanced by micro assessments and threat hunting**
- **Attack surface monitoring and advising**

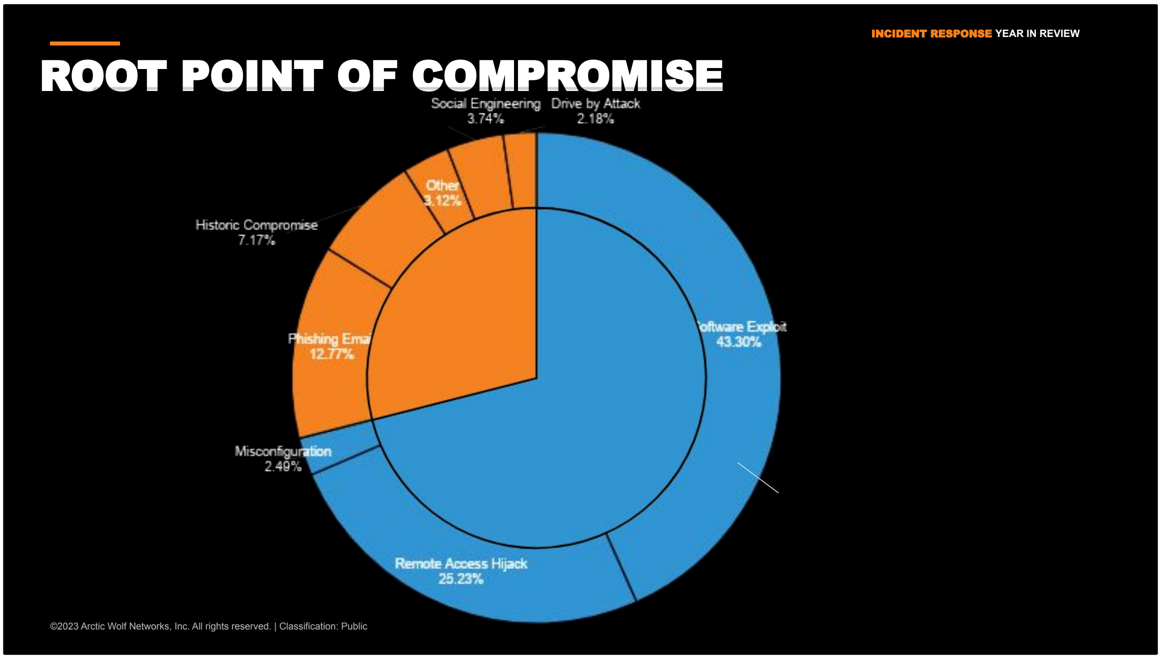
MANAGED DETECTION & RESPONSE

MANAGED RISK

MANAGED SECURITY AWARENESS

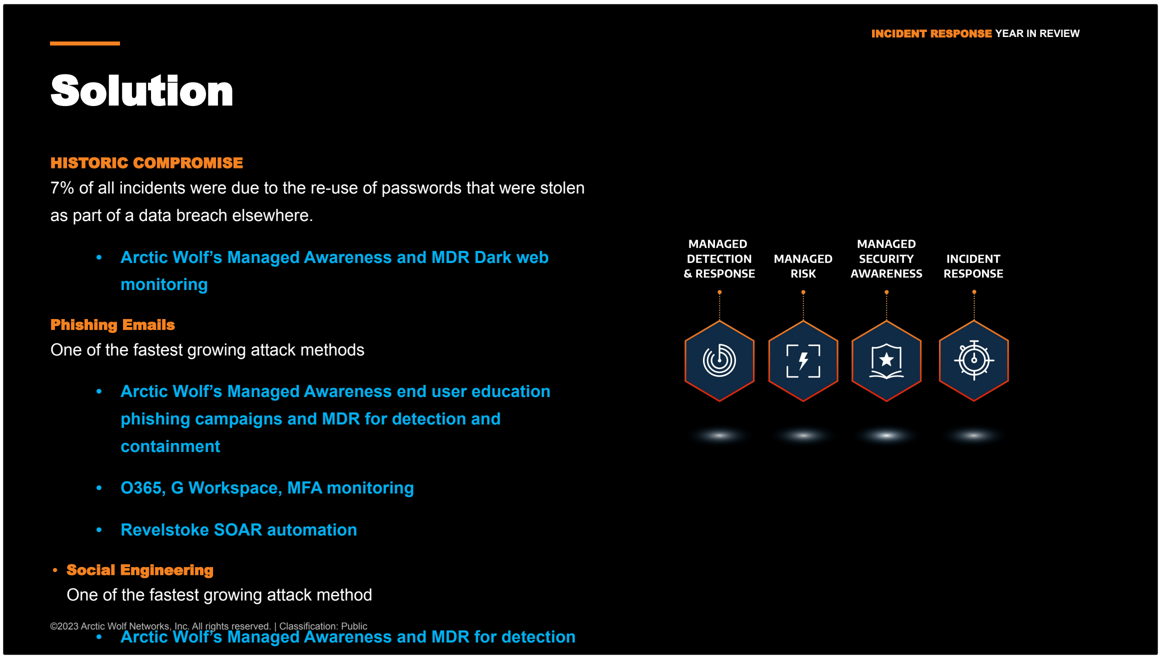
INCIDENT RESPONSE

●



INCIDENT RESPONSE YEAR IN REVIEW

ROOT POINT OF COMPROMISE



Solution

HISTORIC COMPROMISE

7% of all incidents were due to the re-use of passwords that were stolen as part of a data breach elsewhere.

- **Arctic Wolf's Managed Awareness and MDR Dark web monitoring**

Phishing Emails

One of the fastest growing attack methods

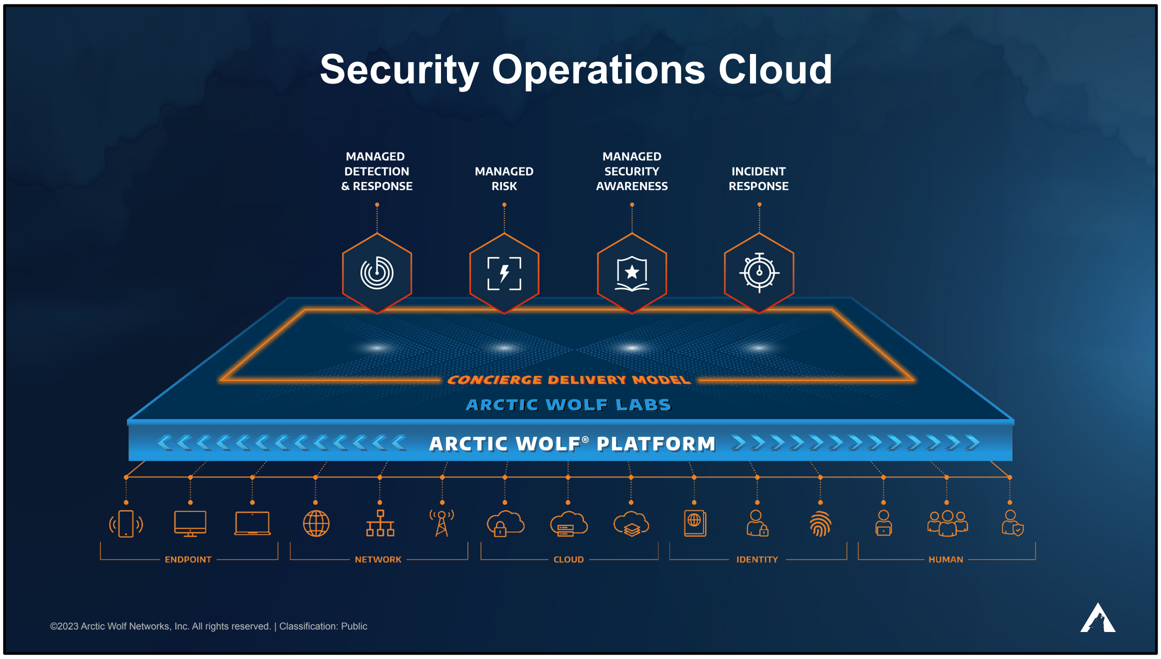
- **Arctic Wolf's Managed Awareness end user education phishing campaigns and MDR for detection and containment**
- **O365, G Workspace, MFA monitoring**
- **Revelstoke SOAR automation**

- **Social Engineering**

  One of the fastest growing attack method

  - **Arctic Wolf's Managed Awareness and MDR for detection**

•



Security Operations Cloud

How we do this in outline is the following:

1. Leverage your existing technology stack to gain broad visibility across attack surfaces: endpoint, network, cloud, identity and human. **Key differentiator:** we are vendor neutral; we work with what you already have. No rip and replace. And we have our own AW security stack, agent, sensors, scanners to augment your stack as needed.

2. We send all that telemetry to our platform which is built on an open XDR architecture, solving the biggest challenge organizations face in cybersecurity: collecting and storing security data across attack surfaces in real time; enriching, analyzing, and investigating this data; and using both humans and automation to respond decisively to threats and attacks. Centralize all data in our cloud-native security analytics platform for storage, enrichment and analysis. This helps with compliance but is also the foundation of our threat detection capability. As data streams in via our sensors, scanners and agents, we enrich it with Arctic Wolf Labs threat intelligence and process it through an ever-increases number of threat detection engines.

1. with threat intelligence and process it through an ever-increases number of threat detection engines. Our Arctic Wolf Labs team leverages incoming data from the Arctic Wolf platform, alongside threat intelligence from external sources, to help our customers stay protected despite an ever evolving threat landscape.

2. Next we build solutions on that platform, but the key differentiator for us is that **the solutions are delivered using a Concierge Delivery Model.** This is an approach where we look to tailor our platform and services and tailor them to your needs and your business**.** We pair you with a team of security experts who not only monitor the data but also learn your organization and unique requirements so well that they can optimize all our solutions for maximum effectiveness in your environment. We also include concierge centric technologies that allow you to interact act with the Arctic Wolf platform and services directly.
   Key differentiator: they work with you on tactical day-to-day items while also helping you with security strategy and ensuring that you advance along your security journey.

   Today the solutions they deliver are:

   Managed Detection and Response provides 24×7 monitoring helping you detect, respond, and recover from modern cyber attacks. Additionally, we have add-on modules covering Cloud Detection and Response, enhancing the security of your IaaS and SaaS assets. And we also offer Data Exploration where customers can explore historical logs and analyzed data while working with their CST to understand the results
   and take action when needed.

- Managed Risk enables you to define and contextualize your attack surface coverage across your networks, endpoints, and cloud environments; provides you with the risk priorities in your environment; and advises you on your remediation actions to ensure that you are benchmarking against configuration best practices and continually hardening your security posture.

- Managed Security Awareness prepares your employees to recognize and neutralize social engineering attacks and human error. There is also an additional module Compliance Content Pack (15 compliance courses covering e.g. PCI, HIPAA, FERPA, Title X, Sexual Harassment etc etc) which integrates compliance training with your security awareness program.

And finally, we round our customers Security Program and Security Operations by offering Incident Response. This includes digital forensic, threat actor communication, and business restoration services.

Now, let’s take a look, in a little more depth, to the key elements of the Arctic Wolf approach to ending Cyber Risk via Security Operations

Thank You

ARCTIC WOLF