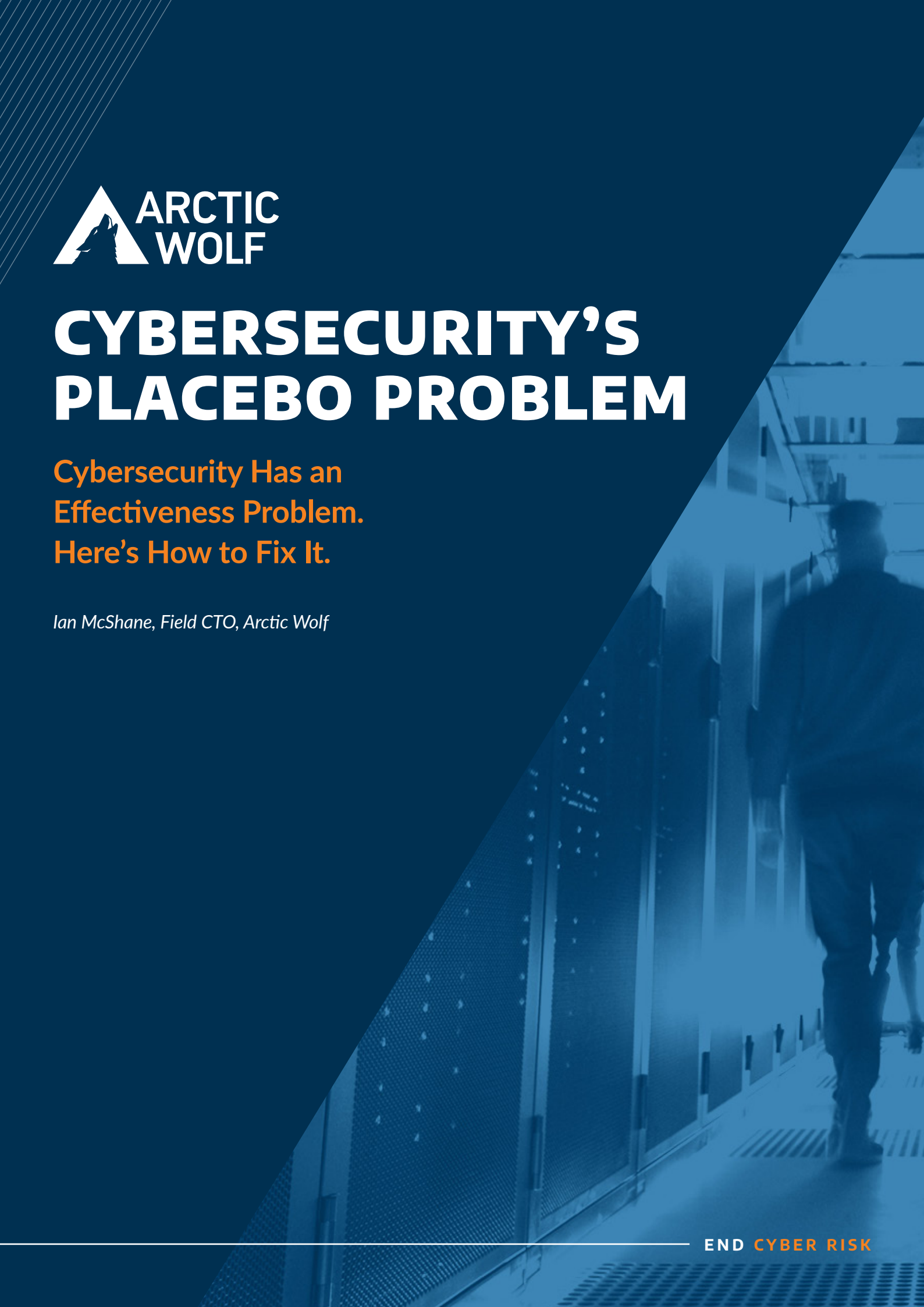
ARCTIC WOLF

CYBERSECURITY'S PLACEBO PROBLEM

Cybersecurity Has an Effectiveness Problem. Here's How to Fix It.

Ian McShane, Field CTO, Arctic Wolf



END CYBER RISK

Are You Unintentionally Riding Your Luck When it Comes to Cybersecurity?

The cybersecurity industry has an effectiveness problem – security leaders already know this: 87% say their organisations are currently failing to address cybersecurity risks.

Most organisations have an array of tools in place, but they're still not secure. Their risk level is still just as high as it would be without those tools. It's pure blind luck that a significant attack hasn't yet hit them. In other words, it's security by chance, not by choice.

87% *of security leaders believe their organisations are falling short*

Despite spending huge amounts of money on cybersecurity, most organisations' cybersecurity posture isn't effective. It does nothing, or very little, to reduce risk. In fact it creates a placebo effect: "We bought some expensive tools, so we must be safer than most, right?" But all too often that sense of security is just an illusion.

So what can we do to improve the situation?

We believe there are **two key steps** you can take to build a better security posture:

STEP ONE
Only consider new tools and products once you've made full use of your existing cybersecurity investments.

STEP TWO
Take a workflow and operations-first approach that complements the tools you already use and the people you already have.

> *All too often a sense of security is just that – an illusion*

You can start on this two-step process without consuming excessive time or resources. It will result in a significant reduction in the level of cybersecurity risk facing your organisation.

But how do you put these ideas into practice? This guide will show you how to make them a reality.

How Do We Know That Cybersecurity Isn't Effective?

So many tools, so much money spent. But these tools are mostly a band-aid, a temporary fix for a point-in-time problem. They're a tactical approach that does not solve the key strategic problem.

A survey of IT leaders and security in the UK (*conducted by Sapio research on behalf of Bitdefender*) found that more than 73% think their organisation is more at risk of a cyber attack because they are under-resourced.

All organisations are at risk of attack. It's only a matter of time until they are breached – after all, *59% of organisations* admit to having been breached in the last year. This is likely a low estimate, too. A fact that makes IT leaders understandably uncomfortable.

In the *Arctic Wolf 2020 Autumn Report*, we found that there was an additional 40-day increase between a vulnerability being disclosed and a patch being deployed. This increases the likelihood of an incident occurring. What's more, it can take up to *207 days* to detect an incident or breach within an organisation.

What Can We Do About It?

What if there were a different way to develop a stronger security posture without having to start from scratch? Here at Arctic Wolf, we urge organisations to put a stop to the cycle of adding more and more cybersecurity tools. We all need to change our thinking and adopt an operational security mindset. Only then can we begin to reduce cybersecurity risk.

The Evolution of Security Strategies

1990s – 2000s: FOCUSING ON ENDPOINT PROTECTION

For many years organisations have been pursuing endpoint protection – identifying and preventing attacks at the endpoint itself. These disparate suites of tools could be effective, but they lacked the cohesion of more advanced, collaborative platforms such SIEMs.

2010s – 2020s: ADVANCING TO SIEM

Security Information and Event Management (SIEM) platforms go beyond just endpoint protection and collate security event data from multiple sources and layers. This provides data analysis and protection to north-south and east-west traffic, but SIEM platforms have fallen short of their promise to provide cybersecurity observability and incident response. They generally offer a poor user experience and are often little more than log collection and storage tools.

2020s ONWARDS: A NEXT-GENERATION APPROACH WITH SECOPS

You still need the protection, response and control elements of an endpoint protection platform, and you still need the data storage and analytics that you hoped to get from SIEM tools. But you also need an organisational approach to security that helps you better manage and reduce cybersecurity risk. It's called 'Security Operations', and we'll explain what it means in the next section.

The SecOps Framework

Security Operations is a way of working to ensure security is baked into every process and action. The USA's *National Institute for Standards and Technology (NIST)* provides a definition and practical guidelines for effective security operations. It has developed the following SecOps framework as a way to reduce security risk:

IDENTIFY

You need an accurate picture of your threat exposure, developing an organisational understanding of risk to your systems, assets and data.

- Identify which of your enterprise's activities are mission-critical.
- Identify document information flows and understand where data is located.
- Identify ALL of your hardware and software.
- Identify roles and responsibilities.
- Identify internal and external threats and risks.

PROTECT

You need to be confident that safeguards are in place and configured properly.

- Protect access to assets and information with appropriate user account security.
- Protect data with encryption when in storage and in transit.
- Protect data by making regular backups.
- Protect your organisation by ensuring software is patched and updated and firewalls/SIEM tools etc. are in place.
- Protect your data by training users to be aware of all types of cybersecurity risks – and make it a mandatory condition of employment.

DETECT

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

- Detect early by ensuring you regularly test and update your detection processes.
- Detect attacks by analysing patterns in software and networking logs.
- Detect the unexpected by having a clear idea of what 'normal' traffic flows look like in your organisation.
- Detect and communicate: if a breach is detected, talk to stakeholders and work fast to understand the extent of the attack.

RESPOND

You need to respond to threats and intrusions quickly and efficiently.

- Respond rapidly by regularly testing your response plan and improving it based on the results gathered during each test.

RECOVER

You need experience and capabilities to ensure you can get back to business fast, and implement improvements.

- Recover quickly by staying in touch with stakeholders, be it customers, employees, suppliers or any other group.
- Recover your reputation with a carefully considered public relations plan.
- Update your recovery plans accordingly as you learn more about the process.

This framework is widely accepted as the best way to approach security. But how can you deploy it most effectively?

What Is Security Operations (SecOps)?

Security Operations is the concept that security isn't just about tools or isolated actions – it needs to be an entire way of operating. Every process, every action, every workflow across every part of your organisation (not just IT) needs to consider the Identify, Protect, Detect, Respond and Recover framework described here.

6 Ways to Improve the Effectiveness of Your Security Operations Framework

You've seen the SecOps framework and what it means. But here are six practical steps you can take to make it a reality in your organisation.

01 | Optimise What You Already Have

Get the most from your existing tech stack and send your security event data to the cloud (whenever possible) for storage and rapid analysis. Don't be tempted to rip and replace your security tools for newer, shinier offerings. In most cases, your existing software and security tools will provide the protection and control you need.

02 | Embrace Security Operations

As we saw in the SecOps guidelines above, you need to focus on a complete security operations framework. You need broad coverage across attack types and attack surfaces. Crucially, do not rely only on tools. Assess current security challenges, risks and workflows and ask yourself 'how have I implemented controls and when was the last time these were tested?'

03 | Build Resilience

Don't be reluctant to seek external expert guidance. Aim for 24/7 protection; implement tactical efforts that make a difference today, and strategic actions that work towards a long-term initiative. Work with people who know your industry and know your organisation to help understand risk factors and solidify your defences – make sure they know the risks as well as you do. Wider knowledge and understanding helps keep everyone safe.

04 | Check Your Visibility

How much can you see? Ask yourself are you able to observe your entire infrastructure? One blind spot can outweigh the benefit of all other data sources so how would you find out about vulnerability?

05 | Always Educate And Research

Are you staying current with attack trends? Take opportunities to learn and improve, teaching staff best practices and what cyber risks look like. In other words, make your staff a point of access control.

06 | Strive To Constantly Improve

Are you checking your environment for threats? If you know a new format to put in place, then do it. Use your research to understand attackers' prime targets within your company. What are your vulnerable entry points for attackers? What do attackers want? Understand this and you can work to reduce your risk exposure.

How to Do More with What You Already Have

At Arctic Wolf, we are vendor agnostic. This means we work with what you already have, using your existing investments to improve your organisation's security. Our cloud-native data platform allows us to collect every event and log we need, going against the industry trend that charges customers for collection, ingestion and storage.

Security Operations with Arctic Wolf includes unlimited data ingestion and no add-ons (such as data capacity extras). So the price of your Security Operations is always 100% predictable.

Introducing The Arctic Wolf Platform

We blend human expertise with a SecOps framework to deliver services across the entire Security Operations framework, including detection response, vulnerability management, cloud monitoring and security training.

Good Security Is a Journey, not a Destination

What you can do next:

1. Switch your mindset from tools to operations.
2. Take a proactive stance and embrace security operations.
3. Shift to a holistic security platform.
4. Address all elements of the SecOps framework to make it work.
5. Explore SecOps materials, such as Arctic Wolf and Forrester's SecOps webinar.

The Arctic Wolf Triage Team Investigates Alerts

- The AW Triage Team: You'll be assigned a team of security experts who will continually optimise your security posture for your environment paired with a team of security experts to learn your unique requirements, we bridge that well-known skills gap. The Arctic Wolf Triage Team will become part of your security team.
- Centralise all data in our cloud-native security analytics platform for 24x7 storage, enrichment, analysis and investigation.
- Leverage your existing technology stack to gain broad visibility across attack surfaces: endpoint, network, cloud, identity, and human.

Watch the SecOps Webinar Featuring Forrester

Paul McKay, Principal Analyst,
Security and Risk Team , Forrester

Ian McShane, Field CTO,
Arctic Wolf

Guest speaker Paul McKay, Principal Analyst on the Security and Risk Team at Forrester, and Ian McShane, Arctic Wolf Field CTO, discuss:

- Legacy security tech stacks and Managed Security Service Providers have fallen short of their promise to provide reliable cyber defence.
- More organisations are re-evaluating their expectations in light of an increasingly sophisticated threat landscape.
- Leading IT teams are considering new approaches, including Managed Detection and Response, to address business-critical SecOps challenges.

WATCH ON-DEMAND

ARCTIC WOLF

FIND OUT WHY YOU'RE BACKED BY THE PACK WITH ARCTIC WOLF

See how we're reducing cybersecurity risk. Explore SecOps and Arctic Wolf's solutions in more detail.

REQUEST A DEMO

END CYBER RISK

Contact Us

arcticwolf.com/uk

ask@arcticwolf.com