FORTRA™

GUIDE (ALERT LOGIC)

Bridging the Cybersecurity Talent Shortage

Ask corporate leaders about their chief concerns for their business and cybersecurity is likely to be at the top of the list. In a recent survey, CEOs ranked technology-related issues, including cybersecurity, as their second major concern and said they will be maintaining a focus on tech issues.[1]

One reason for this hyperfocus on cybersecurity is breaches. As the number of security breaches increases each year, so, too, does their fiscal impact. The average total cost of a data breach in 2023 was $4.45 million.[2]

To combat these business risks, many organizations are looking to strengthen their security teams and technologies to stay ahead of cybercriminals. According to Gartner, information security spending may reach $215 billion in 2024, an increase of 14.3% over 2023.[3] But there's a major roadblock that stands in the way of enhancing in-house security teams: finding and hiring experienced cybersecurity talent.

CEOs rank cyber risks as the **top threat to growth**, with health risks close behind.[4]

Skilled Cybersecurity Professionals Have Been in Short Supply for Decades

As far back as the early 2000s, analysts have been discussing the shortage of qualified cybersecurity staff who have the unique combination of technical acumen and soft skills, "including a positive attitude, diplomacy, patience, attention to detail, tenacious abstract problem-solving ability, and a strong will."[4] Research from 2023 revealed some of the biggest skills gaps for cybersecurity professionals include cloud computing, application security, risk assessment, analysis and management, and threat analysis.[5]

And even when you find a highly qualified cybersecurity professional, their high salary expectations and other offers they're bound to receive may make closing the deal with them a challenge.

While digital tools, services, and systems have never been more important for business growth, many CEOs and CISOs report their organizations are not prepared for the current threat landscape that comes with an increased adoption of digital technologies.[6] This lack of security exposes their IT estates to a greater risk of cyberattacks — for example, 96% of CISOs report their organization was a victim of a ransomware attack that reached its objective in the past year.[7]

Additionally, the accelerated pace of digital transformation in which many organizations are adopting cloud-first strategies has led to a wider attack surface for industrious cybercriminals. The situation is exacerbated by the cybersecurity industry's pronounced skills and resources gap, with with almost 4 million positions currently open around the world.[8] The 2023 Cybersecurity Workforce Study found that despite adding more than 440,000 workers in the past year, the cybersecurity workforce gap has grown an additional 12.6% in 2023.[9]

75% said the current threat landscape is the most challenging it has been in the past five years.[12]

Taken together, these issues paint a pessimistic picture of a future where businesses do not have access to the cybersecurity expertise they need. But what if the solution to current and future cybersecurity needs is to build a security team using a completely different approach — one that's not dependent solely on in-house resources needing to be constantly hired, trained, and maintained?

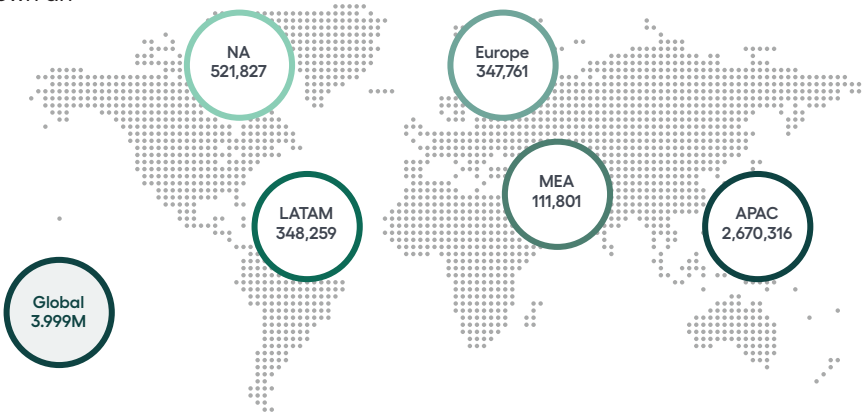
92% of cybersecurity professionals say their organization suffers from skills gaps in one or more areas.[11]

Solution: Managed Detection and Response

The pace of technological advancement is not slowing down. With every innovative technology that your organization adopts, your cybersecurity needs increase. Ask yourself: While a person or team is always needed to protect our IT estate, does it need to be a full-time employee(s)? Do you need an in-house Security Operations Center (SOC) with employees monitoring your environment 24/7, constantly receiving training and professional development to stay aware of the latest technologies and threats?

What if you took a different route to developing a security team to protect your IT estate day and night?

2023 Cybersecurity Workforce Gap by Region



75% of cybersecurity professionals say the current threat landscape is the most challenging it has been in the past five years.[12]

Instead of fighting the constant uphill battle to find elusive new employees with the depth of knowledge and experience to join your company full-time, enhance your team with a partner that's a true extension of your in-house staff — giving you the 24/7 comprehensive security coverage and expertise you need. With Fortra's Alert Logic Managed Detection and Response (MDR) solution, we become an integral part of your team, providing exceptional customer service and a commitment to thoroughly understand your unique business and security needs.

Alert Logic MDR provides you with a dedicated customer success manager as your single point of deep technical competence who develops an intimate knowledge of your security objectives, challenges, and business goals. This is your advocate who works in conjunction with other members of our team — including SOC analysts, threat intelligence researchers, veteran security ops analysts, web application specialists, risk security experts, security content engineer, and application and platform experts — to ensure your business is getting the most measurable service value from your MDR solution. And unlike a member of your in-house staff, your Alert Logic MDR solution isn't available only during standard business hours but is helping ensure your IT estate is secure 24/7 by continuously monitoring for and identifying threats.

Imagine adding an experienced security analyst to your team who has immediate access to a SOC made up of highly skilled professionals with extensive cybersecurity experience, trained on the latest technologies, available and active day and night, 365 days a year. This may be challenging to do through a job posting but easily achieved when you choose Alert Logic MDR.

With the Alert Logic **Total Cost of Ownership (TCO) Calculator**, answer just four questions and gain a clear understanding of what the costs would be to build and train an in-house team to protect and respond to attacks to your organization.

Ready to Strengthen Your Cybersecurity Team?

The need to protect your business from cyberattacks is critical and an always-developing area requiring constant attention. While the global cybersecurity talent shortage makes it difficult to find and hire full-time, highly proficient, and experienced in-house cybersecurity experts, you can create the team you need by partnering with Alert Logic. Your team will be immediately enhanced by collaborating with the only MDR provider that delivers comprehensive coverage for public clouds, SaaS, on-premises, and hybrid environments with a 24/7 approach to customer service.

Learn more about how Fortra's **Alert Logic MDR** solution bridges the cybersecurity skills and resources gap. **Schedule a demo** today.

1. CEOs Turn a Sharp Eye to Workforce Issues and Sustainability in 2022-23
2. Cost of a Data Breach Report 2023
3. Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024
4. ISC2 Cybersecurity Workforce Study, 2023
5. State of Cybersecurity 2022 | ISACA
6. Building Resilience Against Emerging Security Threats
7. The CISO Report
8 - 12. ISC2 Cybersecurity Workforce Study, 2023

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.