ARMIS®

THE STATE OF CYBERWARFARE

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

COUNTRY-BY-COUNTRY ANALYSIS

ITALY

TABLE OF CONTENTS

INTRODUCTION

If you've reviewed the global **Armis State of Cyberwarfare and Trends Report: 2022-2023**, you know that it's critical for business and IT leaders to understand the evolving threat landscape surrounding cyberwarfare, so that they can improve their cybersecurity posture to defend against these attacks. To prepare this report, Armis commissioned a study surveying 6,021 IT and security professionals globally to determine worldwide trends as they relate to security professionals' sentiments on cyberwarfare, attack patterns, cyber spending, and more. Responses were gathered between September 22, 2022 and October 5, 2022.

Armis utilized data from its award-winning Asset Intelligence and Security Platform to verify the survey results against real-world data trends. Proprietary data from the Armis platform collected June 1, 2022 through November 30, 2022 confirmed that cyberattacks haven't slowed, only worsened. Threat activity against the global Armis customer base increased by 15% from September to November when compared to the three months prior. Further, Armis identified the largest percentage of threat activity against critical infrastructure organizations, with healthcare organizations the second most targeted when compared to various industries.

In addition to these global findings, Armis has prepared regional findings and country-by-country analysis to offer unique, localized insights which may be more impactful for individual readers depending on where they physically are based and the counties in which their business operates. **For this country-by-country analysis, we will zoom in on the findings pulled from the 500 respondents who shared insights for our survey that are based out of Italy and work across industries including healthcare, manufacturing, retail, financial services, and more.**

SUMMARY OF FINDINGS

Digital Transformation, a new way of work, improved everybody's life and more than ever, business workflow. A digital approach has been implemented in all sectors, creating new opportunities to focus on the company's core but as always, there is a downside that the report illustrates. Looking at Italian companies, 61% of respondents among IT and security professionals saw a cyberattack in their company. Italy currently shows a reasonable amount of attention to cybersecurity, with more than 85% of respondents claiming that their organization has measures in place to respond to cyber threats, although there are many areas still to be improved.

Overall, Armis identified three key trends when analyzing responses from IT and security professionals from Italian companies when compared to other global respondents from EMEA, the U.S., and APJ. Below, we dive deeper into those findings and the trends they're indicative of.

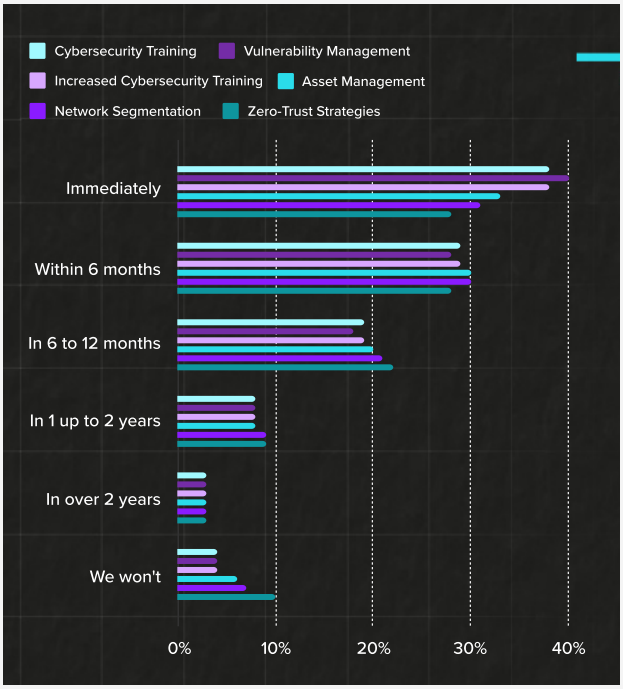
EMEA

Through the course of 2022, the EMEA region has been shocked by the invasion of the sovereign nation of Ukraine. With the geopolitical instability associated with physical warfare and cyberwarfare, shockwaves of consequences are arriving throughout the area. Unpredictability in the food supply, the infamous energy crisis, and a wave of cyberattacks focused against the most critical functions of society, are all contributing to changes in spending and priorities across numerous industries. The report confirms the rise in cyberattacks, bringing to light that almost 3 in 5 organisations (58%) experienced one or more cybersecurity breaches. And 25% of respondents confirmed that there has been an escalation in the number of threats to their organisation.

Measures are being taken to ensure protection, but to date, still less than half (44%) of IT and security professionals agree that their organisation has programs and practices in place to respond to cyberwarfare threats. Respondents depicted their company as ill-prepared as there are some relevant issues to be addressed:

- Only 46% of IT and security professionals in EMEA strongly agreed on knowing who to contact if they notice suspicious activity.
- Only 76% of IT and security professionals in EMEA said they collaborate with others in the industry when it comes to sharing information about threats, below the U.S. and APJ averages. Although being a high number, this indicates that there is still work to be done if all areas are to be shielded from cyberattacks.
- Only 33% of IT and security professionals in EMEA have reported an act of cyberwarfare to the authorities, below the US (63%) and APJ (61%) levels.
- Almost 2 in 10 (18%) of IT and security professionals in EMEA said their organisation does not have a contingency plan in place if cyberwarfare is detected.
- Only a third (33%) of IT and security professionals have a validated cyberwarfare plan with best practice frameworks, to be appropriate and proportionate.
- Moreover, less than half (49%) of companies are educating employees as a common practice, or restricting network admin rights (40%). Fewer still have cybersecurity practices implemented such as creating a security-focused work culture (37%), investing in cybersecurity insurance (31%), and implementing a Cyber Risk Framework (31%).

There is a disconnect between confidence levels of preparedness for cybersecurity attacks (84%) and reality, and investment is needed to close that gap, both for tools and services. When asked to select when they will invest in certain aspects, the following responses were given by IT professionals:



REGULATION IS PUSHING TOWARDS THE FUTURE

Governments, security services and related competent authorities continue to put great emphasis on the need for an improved cybersecurity posture, and the imperative necessity for a more cyber resilient strategy. The recent EU Cyber Resilience Act builds on the EU's existing Cybersecurity Directive of 2016, thus updating the bloc's requirements for enhanced cybersecurity by member states. Prior to this EU Cyber Resilience Act, much of the pressure when it came to cybersecurity was put on users of these products, both enterprises and individuals alike. Now, the manufacturer will share a larger part of this responsibility as well. Accountability can go a long way in helping to make improvements across the board. The EU also released NIS2, adding many more verticals into the spotlight and introducing fines, sanctions, and penalties, for not doing proper risk management, basic cyber hygiene, and taking undue delays in corrective action.

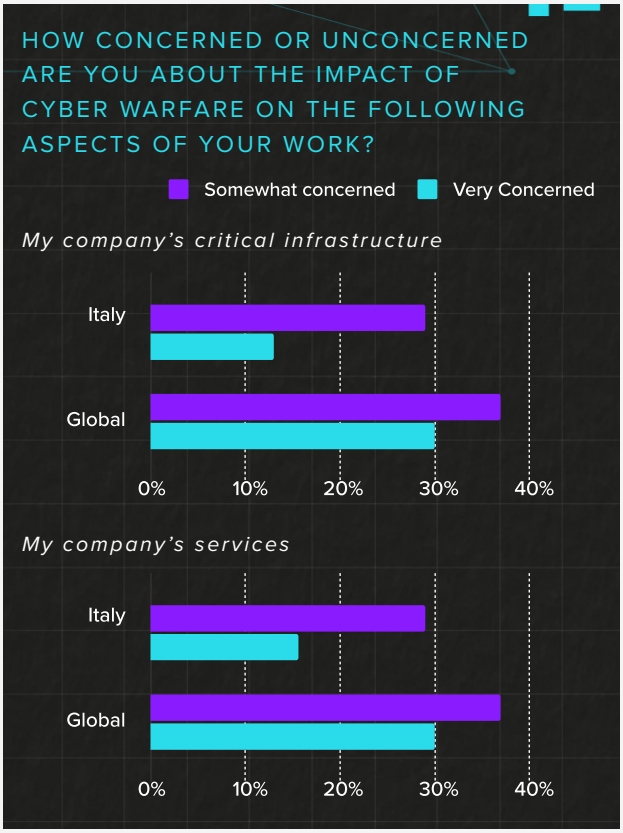
The emergence of regulations is a great conversation starter and will certainly help address that gap of investment in certain tools and prioritise their importance, but there is still a long way to go to secure the critical vulnerability gaps introduced by the exponential proliferation of connected assets. 37% of respondents agree that connected devices are a top priority in the event of a cyberwarfare attack.

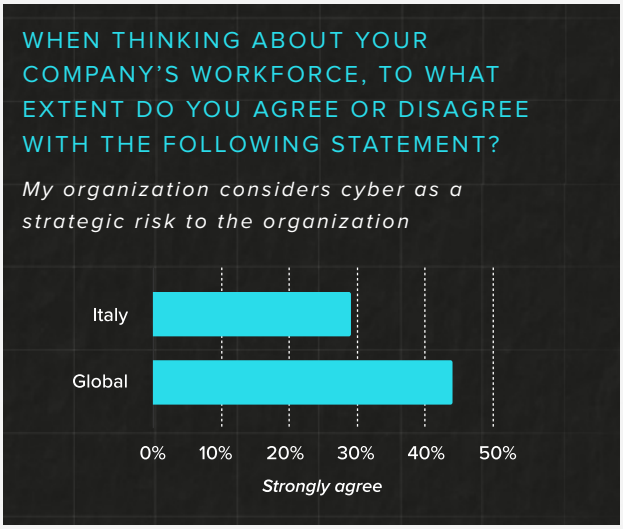
Beyond the internal efforts, it is believed amongst IT professionals that the European Union and its member states should also boost cooperation with other allies around the world. More than half (61%) stated that they would support conscription into a cyber defence league if their country were drawn into a cyberwar conflict.

ITALY TRENDS FROM THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

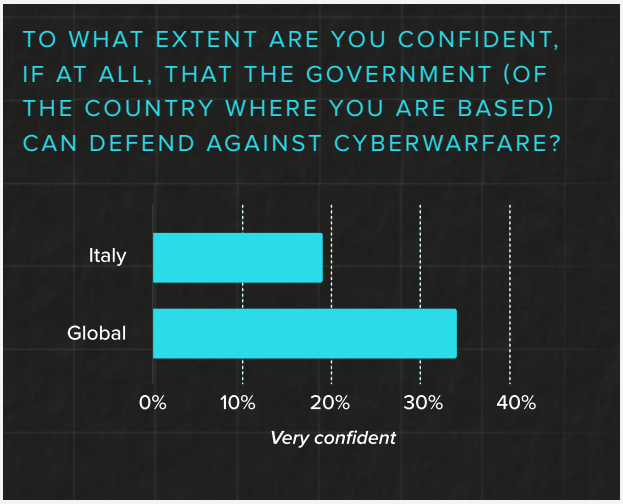
CONCERNS DIFFER FROM THE REALITY IN VIEW OF THE GEOPOLITICAL CONTEXT

Compared to the rest of the world, Italy is on average less concerned about the impact of cyberwarfare regarding the company's critical infrastructure and its services. When asked regarding awareness of the risks that cyberwarfare poses, 29% of Italian respondents reported a low consideration of cyberattacks as a strategic risk for the organization, this figure is significatively lower compared with the 44% of respondents globally. More emphasis needs to be placed on the risks associated with an event of this magnitude to stimulate awareness among security professionals.

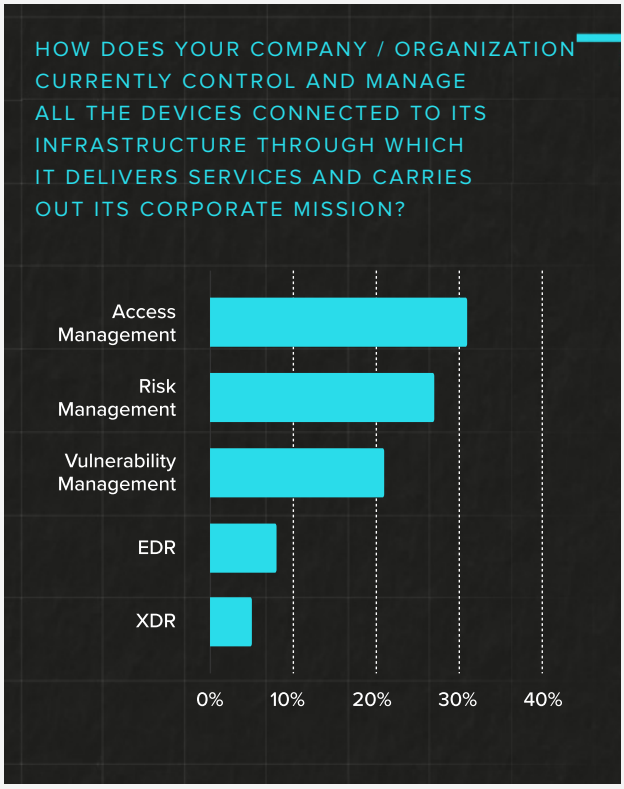




The research also touched on trust in the government regarding defense in the face of a cyberattack, which showed interesting results. Globally, 33.5% feel very confident about the commitment of their government organizations, whereas only 18% of respondents in Italy have the same confidence.

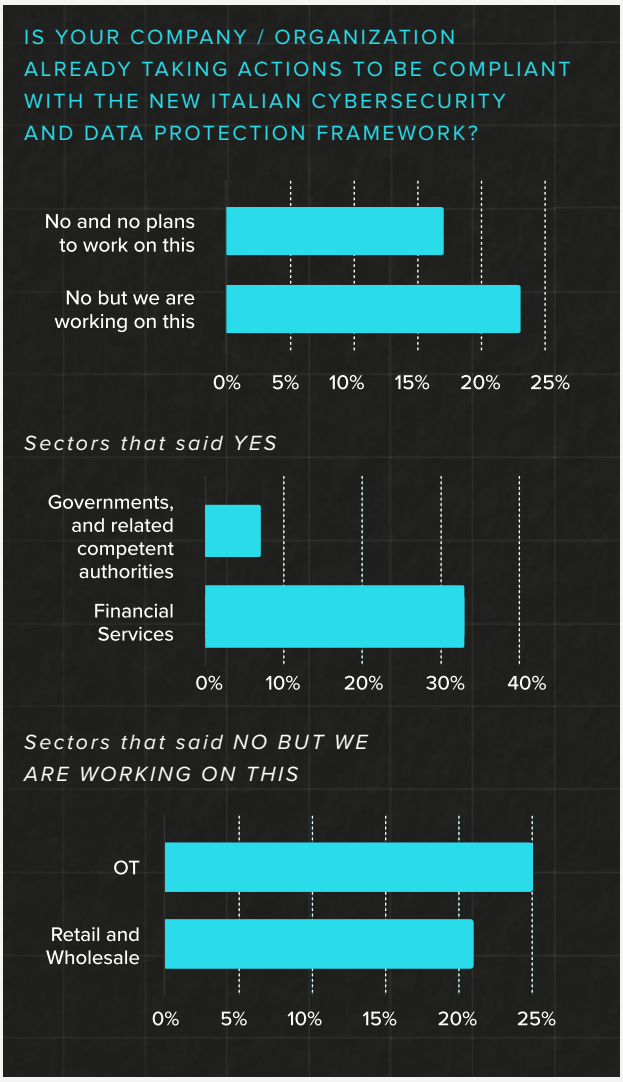


Furthermore, a minority say their company currently controls and manages all the devices connected to its infrastructure through which it delivers services and carries out its corporate mission via access management (31%), risk management (27%), or vulnerability management (21%). Small minorities do this through eDR (8%) or XDR (5%).



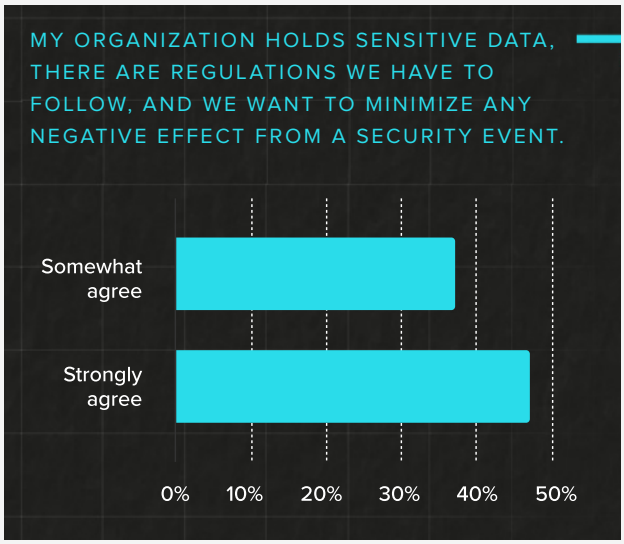
COMPLIANCE IS NOT A PRIORITY: THE ITALIAN DATA PROTECTION FRAMEWORK AND CYBERSECURITY

Italy created the National Framework on Cybersecurity and Data Protection, a benchmark adopted by highly different types of organizations as a tool to coordinate their defense strategy against cyber. Despite this, over 2 in 5 (41%) say their company is not taking action to be compliant with the new Italian CyberSecurity and Data Protection framework, and only 7% say they have a compliant plan. The most proactive sector is finance and banking, with 33% of respondents saying they have implemented a fully compliant plan. In general, there is less concern within organizations belonging to the OT and retail sectors, as the percentage of entities that have not yet implemented a plan, or planning to do so, is 25% and 21%, respectively.



This is perhaps even more concerning when considering that over 4 in 5 (84%) IT professionals surveyed agree that their organization holds sensitive data, there are regulations they have to follow, and they want to minimize any negative effect from a security event. Data protection is an imperative

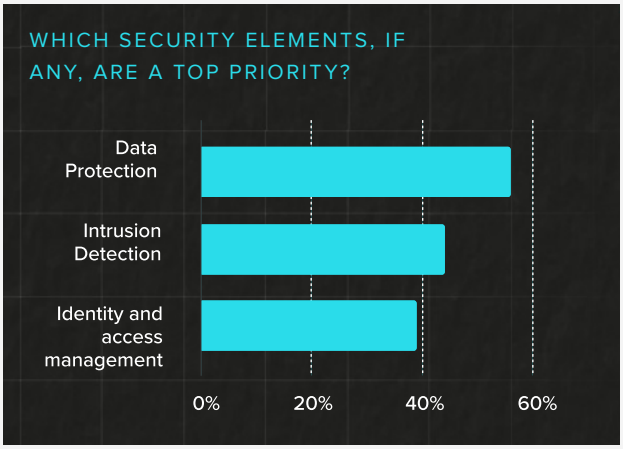
for any EU country, and although awareness of its importance is clear there seems to be a disconnect with actual compliance with the rules.

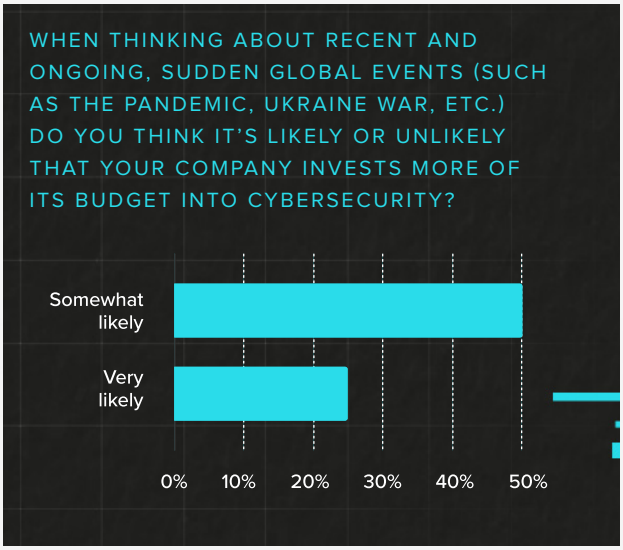


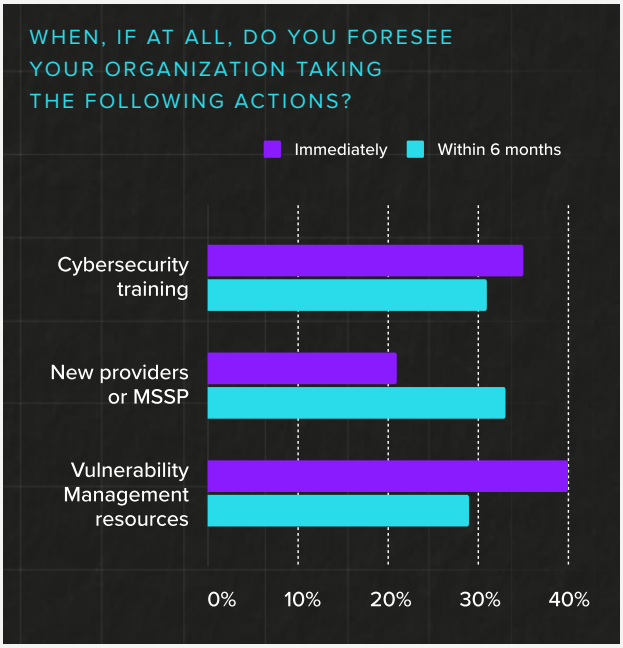
THE SECURITY POSTURE NEEDS TO BE STRENGTHENED

Italian organizations' are improving their approach to cyberthreats, but there are still measures to be taken. The main focus lies on Data Protection, Intrusion Detection, and Identity and Access Management, which respondents voted as their current top priorities, while prevention of possible supply chain attacks and machinery monitoring appear secondary.

Future prospects seem to be reassuring and encouraging, as the sample of respondents foresee more investments from their organizations in relevant cybersecurity measures. Respondents anticipate investments in cybersecurity training immediately (35%) or within six months (31%); in new providers 21% immediately and 33% within six months; and in vulnerability management resources 40% immediately and 29% within six months.







WHY DO THESE FINDINGS MATTER?

The results of the Armis State of Cyberwarfare and Trends Report: 2022-2023 demonstrate organizations' growing concern about the increasing frequency and severity of cyberattacks, as well as the threat of cyberwarfare. The increasingly complex and sophisticated threat landscape is impacting diverse areas of business, across all industries. However, there is still a different pace and priorities in designing and adopting cybersecurity strategies.

> *"Cyberwarfare is the future of terrorism on steroids, providing a cost-effective and asymmetric method of attack that requires constant surveillance and expense to defend against," ... "Clandestine cyberwarfare is quickly becoming a thing of the past. Today, we are already seeing brazen cyberattacks by nation-states, often with the intention of gathering information, disrupting operations, or completely destroying data. Based on these trends, all organizations should consider themselves potential targets of cyberwarfare attacks and protect their assets accordingly."*
>
> **NADIR IZRAEL**
> CTO AND CO-FOUNDER AT ARMIS

> *"It is clear from the results of this report that Italian organizations do not share the concerns of most other countries with regard to the threat of cyberwarfare and have a long way to go with their compliance efforts," ... "Both of these issues are addressable by increased asset visibility, vulnerability management, and ongoing risk assessment. Armis is uniquely positioned to assist Italian organizations in reaching compliance and improving their security postures."*
>
> **NICOLA ALTAVILLA**
> COUNTRY MANAGER OF ITALY & MEDITERRANEAN AREA, ARMIS

WHAT CAN YOUR ORGANIZATION DO TO PROTECT ITSELF?

So, what can organizations do? Early detection and continuous monitoring is the best way to improve your organization's security posture and remediate quickly. After all, if you don't know you have a problem, you can't fix it. Similarly, if you can't see an asset, you can't protect it. This is where Armis can assist.

ARMIS ASSET INTELLIGENCE PLATFORM

The **Armis Asset Intelligence Platform** provides unified asset visibility and security across all asset types, including information technology (IT), internet of things (IoT), operational technology (OT), internet of medical things (IoMT), cloud, and cellular-IoT — both managed and unmanaged. Delivered as an agentless software-as-a-service (SaaS) platform, Armis seamlessly integrates with existing IT and security stacks to quickly deliver the contextual intelligence needed for improving an organization's security posture, without disrupting current operations or workflows. Armis helps customers protect against unseen operational and cyber risks, increase efficiencies, optimize the use of resources, and safely innovate with new technologies to grow their business – no matter the threat, cyberwarfare or other.

Register today for a Security Risk Assessment to learn which assets are most vulnerable to attack. Use these insights to prioritize your risk mitigation strategy and ensure full compliance with regulatory frameworks that require you to identify and prioritize all vulnerabilities.

To request a custom demo from Armis, please visit: armis.com/demo.

To dive deeper into the findings of the Armis State of Cyberwarfare and Trends Report: 2022-2023 on a global scale, please visit: **armis.com/cyberwarfare.**

THE STATE OF
CYBERWARFARE

ABOUT ARMIS

Armis, the leading asset visibility and security company, provides the industry's first unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G. Armis provides passive cyber asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in California.

armis.com

info@armis.com

20230110-1

ARMIS®