ARMIS®

THE STATE OF CYBERWARFARE

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

COUNTRY-BY-COUNTRY ANALYSIS

USA

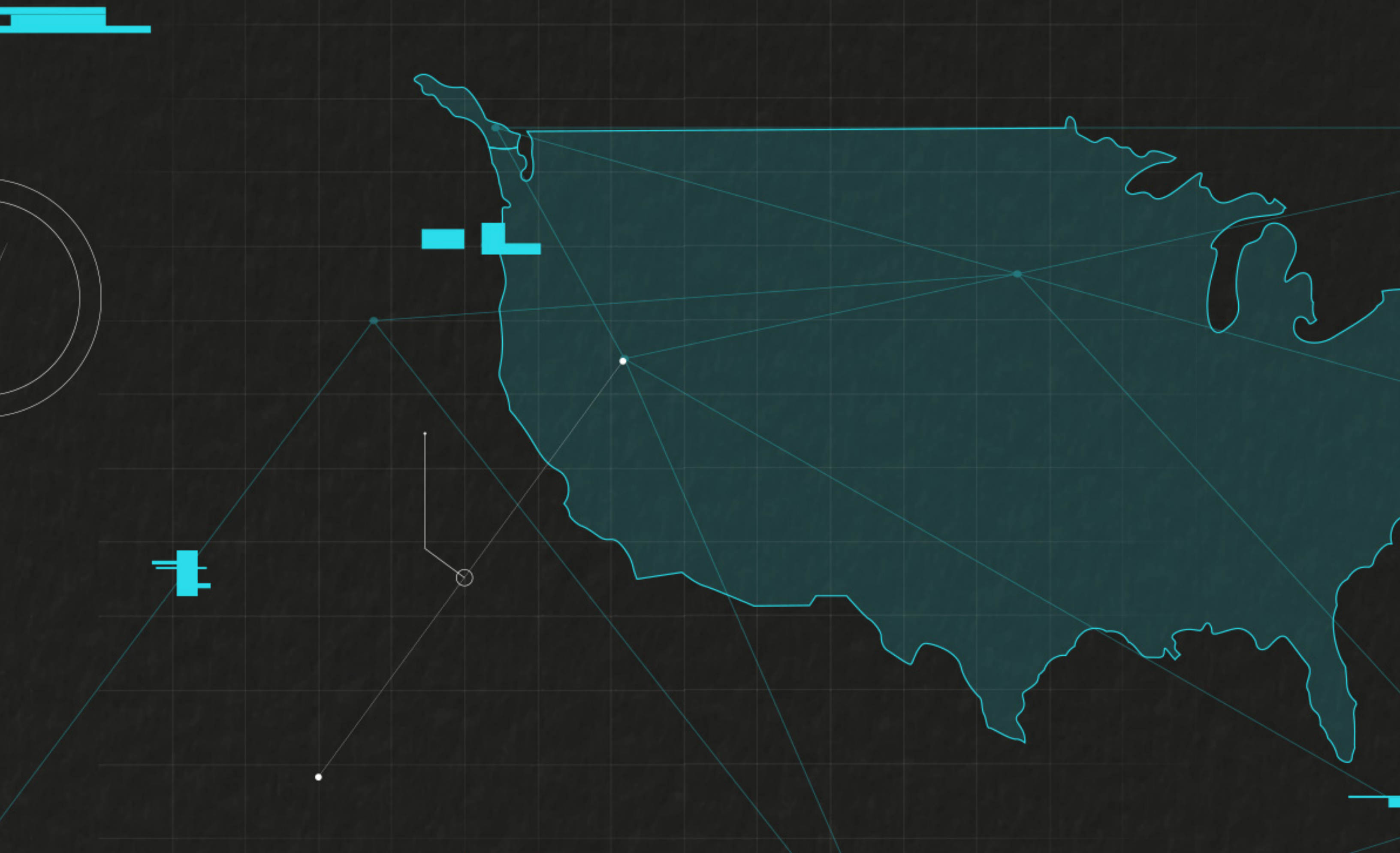


TABLE OF CONTENTS

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 1,000 respondents who shared insights for our survey that are based out of the United States of America and work across industries including healthcare, manufacturing, retail, financial services, and more.**

SUMMARY OF FINDINGS

Overall, Armis identified six key trends when analyzing responses from IT and security professionals from American companies when compared to respondents from countries in EMEA and APJ regions. Organizations across industries – from manufacturing to healthcare – are feeling the impact of cyberwarfare on their business. A significant percentage of IT and security professionals surveyed in the U.S. are concerned about the impact of cyberwarfare. As cyberwarfare threats and attacks are on the rise, some industries are more prepared than others. Below, we dive deeper into these findings and the trends they're indicative of.

ARMIS®
ADVANCED VULNERABILITY MANAGEMENT
ASSESS THE RISK ASSOCIATED WITH EVERY ASSET AND PRIORITIZE REMEDIATING CRITICAL VULNERABILITIES.
LEARN MORE
www.armis.com

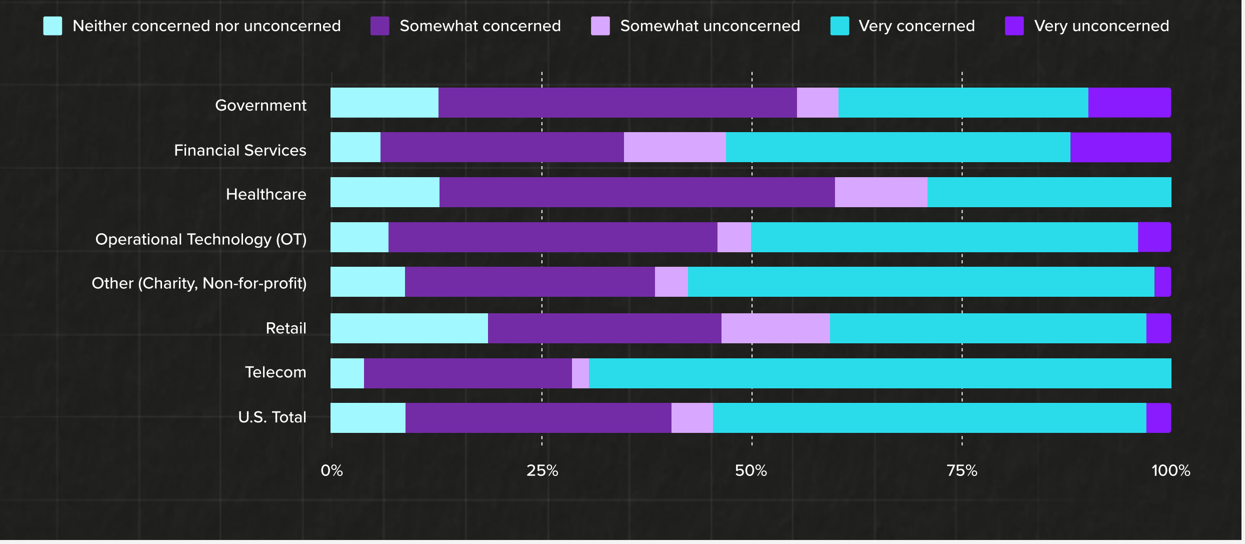
U.S. TRENDS FROM THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

CYBERWARFARE ATTACKS AGAINST U.S. COMPANIES ARE ON THE RISE

Cyberattacks are a reality for businesses, as more than 7 in 10 (73%) of IT professionals surveyed in the U.S. say their company has experienced one or more cybersecurity breaches. In fact, more than 2 in 5 (45%) IT professionals surveyed in the U.S. said they had experienced more threat activity on their network between May and October 2022 when compared to the six months prior.

Adding to an already tumultuous threat landscape, concerns over cyberwarfare abound, with 84% of IT professionals in the U.S. stating that they are concerned about the impact of cyberwarfare on their organization/company as a whole. What's more, 63% of U.S. respondents have had to report an act of cyberwarfare to authorities.

HOW CONCERNED OR UNCONCERNED ARE YOU ABOUT THE IMPACT OF CYBERWARFARE ON YOUR ORGANIZATION AS A WHOLE?

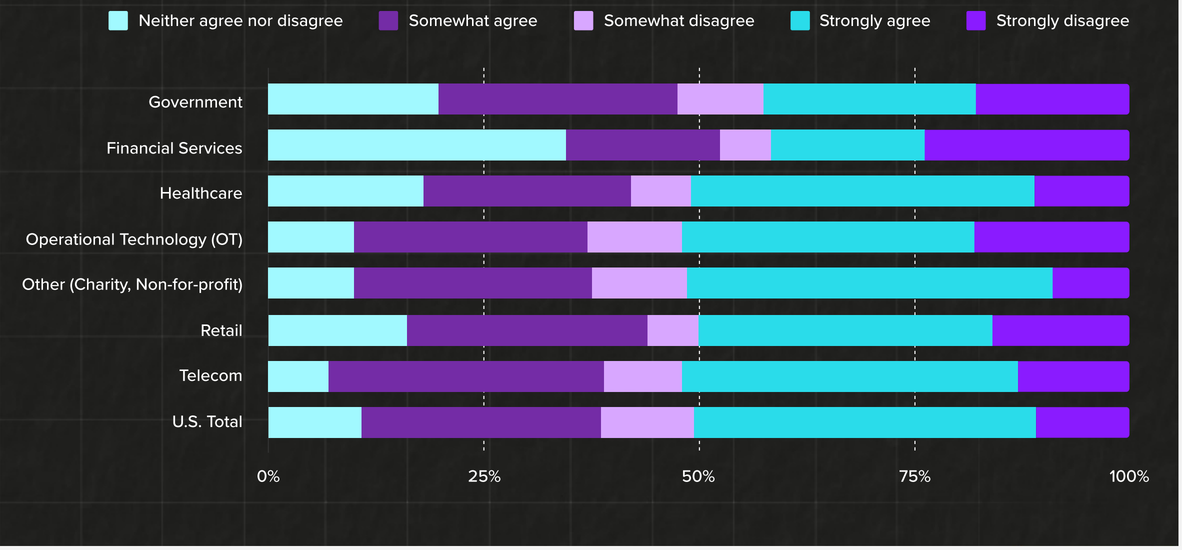


A FEAR OF CYBERWARFARE IS DRIVING BUSINESS DECISIONS

As companies fear the widespread damage of cyberwarfare, a staggering 70% of U.S. respondents stated that they believe cyberwarfare is more damaging than physical warfare. Organizations in the U.S. are not only fearful, but they are acting upon their fear, with 67% of respondents stating they agreed when asked if their organization has stalled or stopped digital transformation projects due to the looming threat.

TO WHAT EXTENT DO YOU AGREE OR DISAGREE WITH THE FOLLOWING STATEMENTS ABOUT YOUR ORGANIZATION'S CYBER SECURITY PROCESSES:

"My organization has stalled or stopped digital transformation projects due to the threat of cyber warfare."

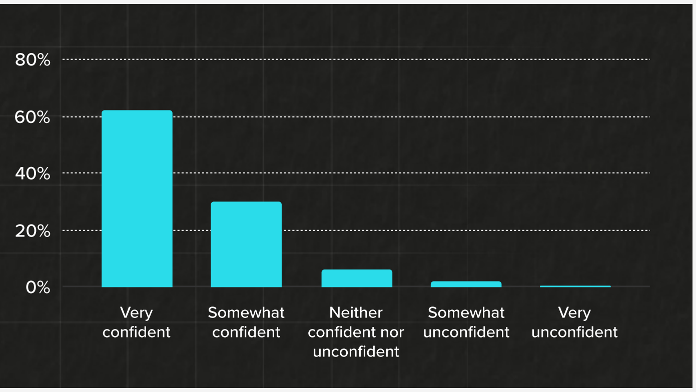


CYBERWAR PREPAREDNESS VARIES ACROSS INDUSTRIES

The full findings from Armis demonstrate a wide variation in levels of preparedness for a cyberwarfare attack across industries. The telecommunications industry appears to be the most prepared for cyberwarfare, with 63% stating that they have an appropriate and proportionate plan that is validated with best practice frameworks. On the opposite end, those from the financial services industry are the least prepared when compared to other sectors, with only 47% of respondents answering the same.

The threat of cyberwarfare touches more than just business operations. Despite **CISA's declaration** that there was no evidence of any cyber-related compromise to the electoral process in the 2022 midterm elections and their ongoing dedication to preventing election hacks – 79% of U.S. respondents answered "yes" when asked if cyberwarfare could affect the security of an electoral process. IT and security professionals stated that they are the most concerned about data breaches resulting in the loss of voter information (38%), as compared to a voter operations attack (22%) or ransomware attack (16%).

TO WHAT EXTENT ARE YOU CONFIDENT, IF AT ALL, THAT THE U.S. GOVERNMENT CAN DEFEND AGAINST CYBERWARFARE?



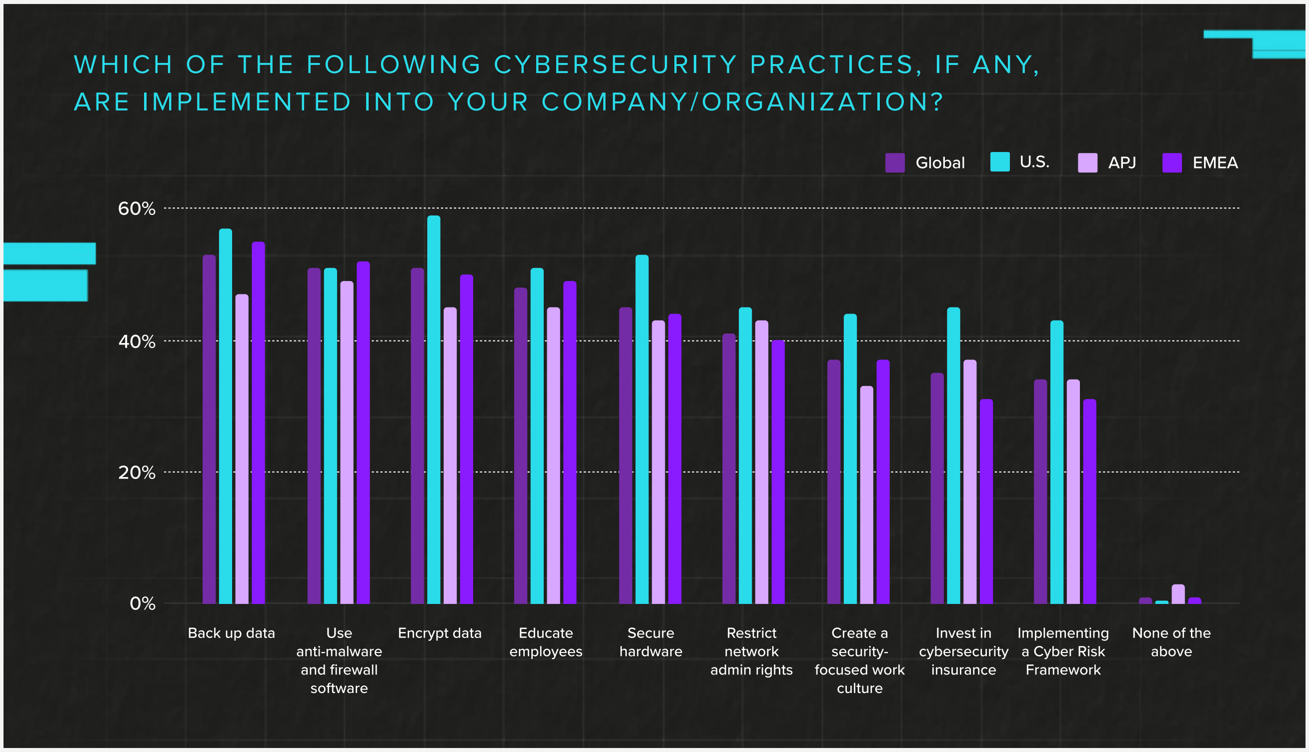
Despite the growing threat of cyberwarfare and the impact it has on businesses, U.S. respondents also showed optimism. Businesses are showing confidence in both their country and their organization’s ability to defend in the event of an attack — with the majority (62%) of U.S. organizations strongly agreeing that they have programs and practices currently in place specifically designed to respond to cyberwarfare threats. Similarly, this confidence shone through when asked about the government’s ability to thwart these types of attacks, with 62% stating they are very confident that the U.S. government will be able to defend against cyberwarfare.

Even though the average of 62% indicates strong confidence in the U.S. government, there’s a wide range of sentiment between respondents from different industries. Of those respondents who are very confident, telecommunications was the highest (80%), followed by organizations grouped as “other” (charity, not-for-profit, technology, etc.) (67%). Organizations from the retail industry showed the lowest confidence, with only 41% of respondents feeling very confident that the U.S. government can defend against cyberwarfare.

U.S. LEADS WHEN IT COMES TO CYBERSECURITY HYGIENE, BUT STILL LACKS SECURITY NON-NEGOTIABLES

The need for strong cybersecurity hygiene is well recognized, as 91% of respondents in the U.S. agreed with the statement that their “organization holds sensitive data, there are regulations their organization has to follow, and they want to minimize any negative effect from a security event.” While this may seem like table stakes, adequate action is rarely being taken. For example, only half (50%) of IT professionals surveyed are increasing cybersecurity training with immediate effect at their organization. Fewer are immediately implementing network segmentation (46%) or Zero-Trust strategies (43%).

As for specific cybersecurity practices in place, fewer than 3 in 5 U.S. organizations are encrypting data (59%) or backing up data (57%), and even fewer are securing hardware (53%), using anti-malware and firewall software (51%), educating employees (51%), or restricting network admin rights (45%). The numbers go even lower for investing in cybersecurity insurance (45%), creating a security-focused work culture (44%), and implementing a Cyber Risk Framework (43%).



U.S. COMPANIES ARE LOOKING TO OUTSOURCED PROVIDERS FOR HELP

In an effort to mitigate risk, organizations are rethinking their cybersecurity spending. Eighty-nine percent of IT pros in the U.S. stated that, when thinking about recent and ongoing, sudden global events (such as the pandemic, Ukraine war, etc.) it is likely that their company invests more of its budget into cybersecurity. However, as the skills shortage continues to be a real problem for the industry, businesses are looking for ways to partner with MSSPs or new providers that can help them to maximize the value of the security investments they are already making. Fifty-six percent of IT and security professionals in the U.S. strongly agreed that their organization collaborates with others in their industry when it comes to sharing information about threats, compared to 36% in EMEA.

Lack of headcount is contributing to businesses rethinking their approach. More than 2 in 5 (45%) IT and security professionals surveyed in the U.S. foresee their organization finding a new cybersecurity provider(s) or MSSP immediately. It's critical that vendors are aware of spending trends and where organizations are most in need of their services so that they can ensure they're delivering the right solutions. The use of external providers varies greatly by industry — In the U.S., organizations including charities, not-for-profits, and technology companies particularly rely heavily on external providers to support their cybersecurity processes (47%), while only 28% of government respondents answered the same.

DECISION-MAKERS STILL STRUGGLE WITH HOW TO ADDRESS RANSOMWARE ATTACKS

Ransomware continues to plague businesses across industries, and decision-makers are still grappling with how to address it head-on. The question of whether to pay continues to be hotly debated, despite the FBI and Homeland Security advising all organizations to never pay a ransom. Nearly half (47%) of the IT professionals surveyed in the U.S. said their organization's policy on paying ransoms in the event of a ransomware attack is to always pay, with only 13% stating that their policy is to never pay.

Following the 2021 attack on Colonial Pipeline which exposed vulnerabilities within the nation's critical infrastructure, the government dove in head first to address the problem of cybersecurity, including issuing an executive order designed to boost cyber defenses for federal networks and the beyond. As the government continues to weigh in on the ransomware problem, IT and security professionals in the U.S. shared mixed feelings on the responsibility of the public versus the private sector in addressing it. Still, 83% percent of respondents agree that the government should be involved when private companies are deciding whether to pay a ransom.

ARMIS
SEE AND SECURE EVERY ASSET
YOU CAN'T PROTECT WHAT YOU CAN'T SEE.
LEARN MORE

WHY DO THESE FINDINGS MATTER?

In the wake of a shifting threat landscape, businesses have a long way to go when it comes to being fully prepared for the threat of cyberwar. As defenses grow stronger, so do attackers, and businesses need to ensure they are taking the proper steps to adapt now. The cyberwarfare threat is halting technological advancement from the implementation of digital transformation projects. A proactive approach to security which includes developing a proper plan with full, contextualized asset visibility that is tested regularly is a step in the right direction for businesses as they work to protect against this growing threat.

> *"The U.S. has been rolling towards a cybersecurity turning point for the past several years, and these survey results reveal we've now arrived. Organizations across the country are grappling with the best ways to address both the immediate threat of ransomware and the looming threat of cyberwarfare, and the drastic variation in preparedness shows we have much work to do, from both the private and public sectors," … "Approaching cybersecurity strategies requires getting comprehensive input from all key constituents in the C-suite, business operations, IT teams, and security teams – and ensuring organizations have full visibility of everything on their network."*
>
> **CHRIS DOBREC**
> VP OF PRODUCT AND SOLUTIONS AT 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®