ARMIS

**WHITE** PAPER

# SHADOW-IOT – A LARGELY UNDERESTIMATED SECURITY RISK IN GERMANY, AUSTRIA AND SWITZERLAND

## Armis Research Results

# Table of contents

# **INTRODUCTION** - GROWTH DRIVER: THE INTERNET OF THINGS

13.8 billion Internet of Things (IoT) devices are now in daily use worldwide – and the numbers continue to grow. [1] Industry 4.0 is nearly unimaginable without these smart tools, which can help to optimize all areas of a modern company – from supply chain management and production to logistics and sales. In today's era of digitization and networking, virtually no industry can do without the massive use of helpful technology because its implementation results in considerable added value.

### What are IoT devices?

IoT devices are devices that can collect, store, process and – because they are connected to a network – transmit data.

It is estimated that IoT devices will generate seven percent of the EU's gross domestic product by as early as 2025. Each euro invested in this technology can reap up to 12 times its value in productivity gains and time savings. [2]

This is why companies in the DACH region, in particular, have been using IoT technology intensively for many years. Investments in this sector increased by an average of an impressive 42 percent last year. And with good reason: 13 percent of the companies were able to identify device-related added value immediately, and 69 percent could identify it no later than three months after implementation. [3]

## **SHADOW IOT** CALLS NETWORK SECURITY INTO QUESTION

But the massive expansion of IoT use is accompanied by an increased security risk. This is because traditional technical tools, such as endpoint and network security solutions, can localize IoT devices in the corporate network only to a limited degree or not at all. As a result, increasingly many parts of a company's IoT landscape are not under the company's control. In 2017, companies already lacked visibility of approximately 40 percent of all connected IoT devices on average. Estimates now put this figure at approximately 90 percent. This is disquieting because only a minority of IoT devices are adequately protected against unauthorized access.

This so-called "shadow IoT" therefore poses a serious threat to every corporate network. Cybercriminals can easily infiltrate poorly secured and unattended IoT devices, which the hackers can then use as gateways into their victims' networks. Once inside the network, cybercriminals can undetectably cripple the company's digital operations with a DDoS attack, manipulate or steal corporate data, or even misuse the company's hardware for cryptomining. [4]

### Shadow IoT - What is it?

Shadow IoT refers to IoT devices that are connected to a network without being detected and controlled by the network's management. They accordingly pose a significant security risk to the network.

Such attacks also increasingly affect companies in the DACH region. The reason: the proliferation of shadow IoT is also spreading in these corporate networks.

This raises two questions: Are the people responsible for IT in Germany, Austria, and Switzerland genuinely aware of the additional risks they are imposing on their corporate networks? And are they working on suitable solutions to eliminate these risks?

# **ARMIS RESEARCH** – FIVE KEY FINDINGS

The results are now available from a YouGov survey of IT decision-makers in German, Austrian, and Swiss companies. And these findings raise considerable doubts in this regard:

- More than half of the survey's participants believe that shadow IoT is spreading in their company's network.
- But only around 1/3 are convinced that the presence of this shadow IoT represents an increased security risk for their company.
- At the same time, approximately 2/3 are well aware that IoT devices connected to the corporate network transmit and receive corporate data from the outside world that could potentially enter the corporate network.
- Approximately 1/2 believe that IT department staff should solve the shadow IoT problem independently – by manually searching for unknown IoT devices on the corporate network.

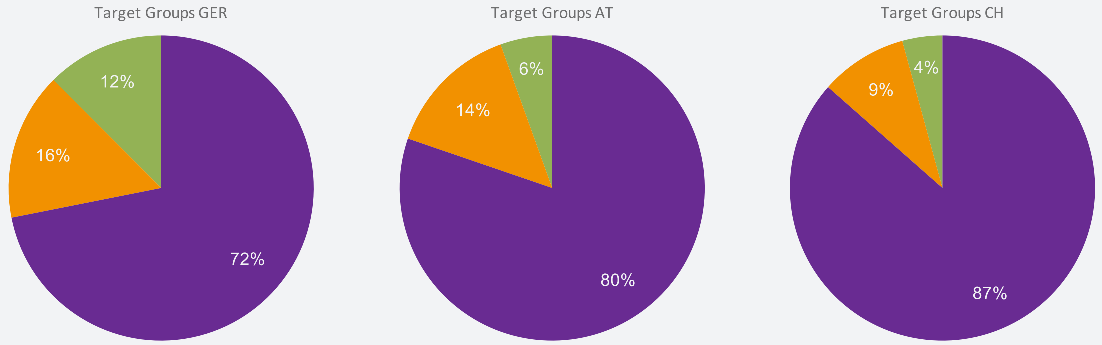
## Technical details of the survey

| | | |
|---|---|---|
| **Institute:** | YouGov Deutschland GmbH | |
| **Location:** | DACH region | |
| **Timeframe:** | Sept. 8 - Sept. 17, 2021 | |
| **Participants:** | Germany | 505 respondents |
| | Austria | 400 respondents |
| | Switzerland | 400 respondents |

● People middle management or higher, but not IT

● People in IT, but below middle management

● People both middle management or higher and IT

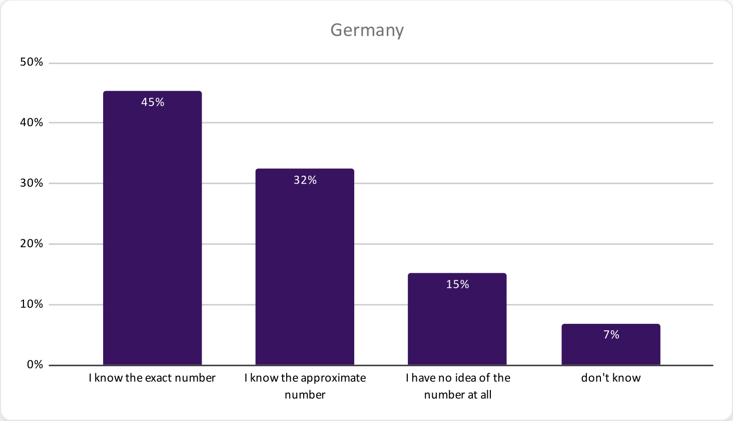


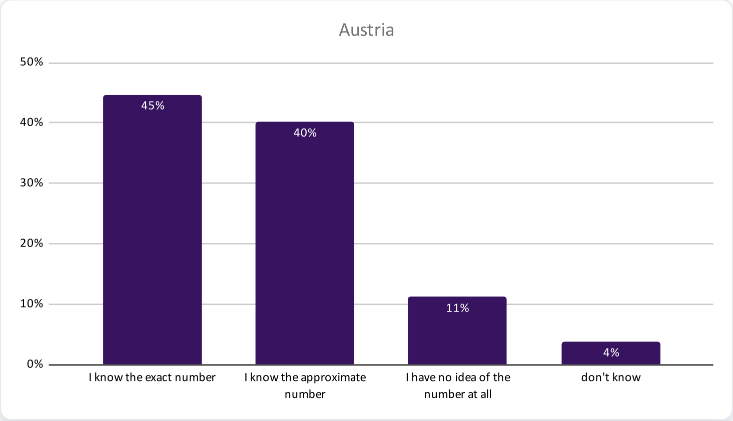
## **QUESTION NO. 1** – IOT DEVICES AROUND US

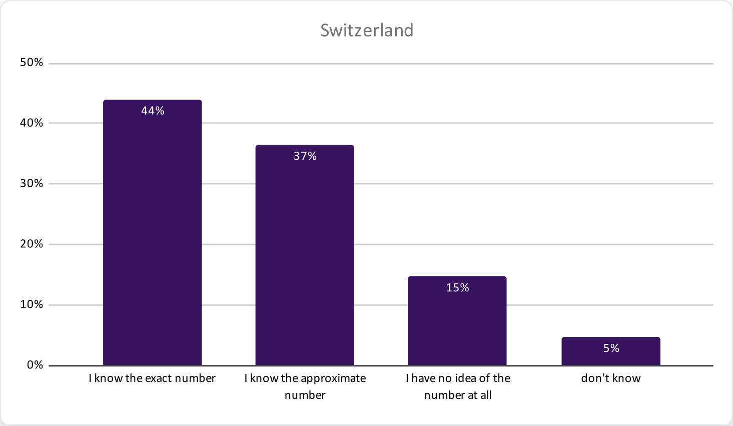
### Do you know the number of smart devices with Internet access (IoT – Internet of Things) that you have in use (e.g., smartphones, tablets, PCs, laptops, printers, headsets, webcams, etc.)?

Evaluation (DACH region, total):

- Around **45 percent** say they know the **exact number** of devices
- Around **36 percent** say they know the **approximate number** of devices
- Around **19 percent** say they are **unable to make a statement** in this regard





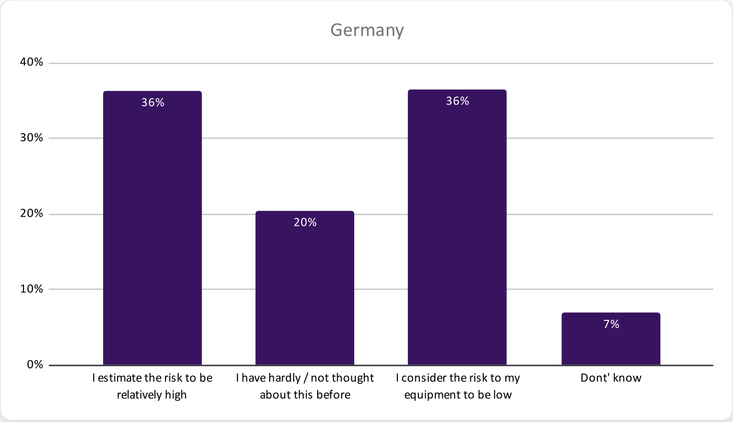


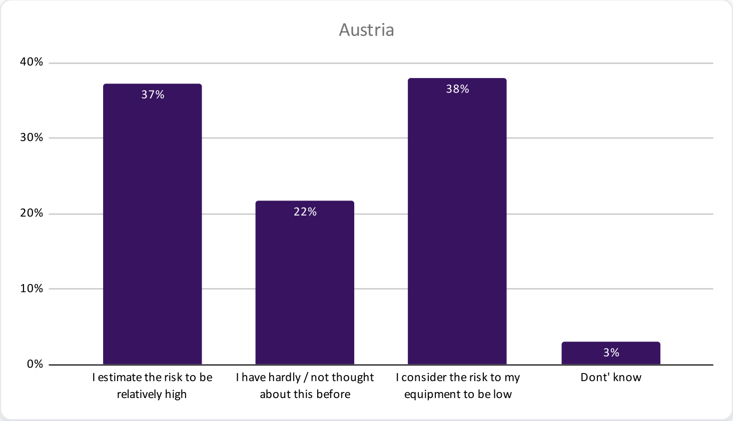
# **QUESTION NO. 2** – THE RISK OF CONNECTED DEVICES

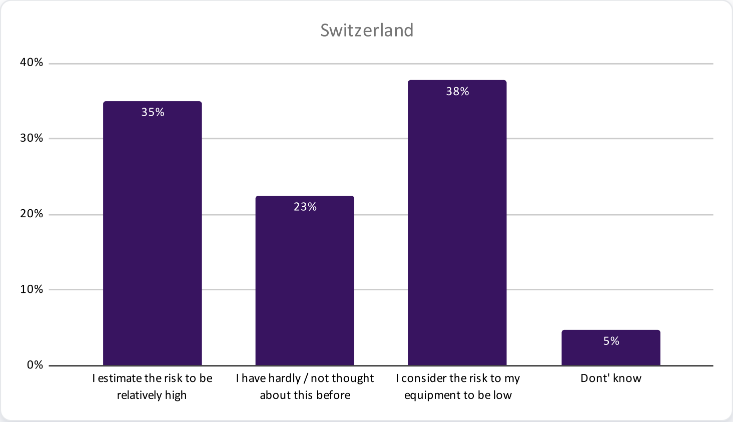
**In terms of protecting your data, how high do you rate the risk that these smart devices are constantly connected to each other and/or to the Internet?**

Evaluation (DACH region, total):

- Around **37 percent** say that they consider the **risk** to be relatively **low**
- Around **36 percent** say that they consider the **risk** to be relatively **high**
- Around **27 percent** say that they are **unable to make a statement** in this regard





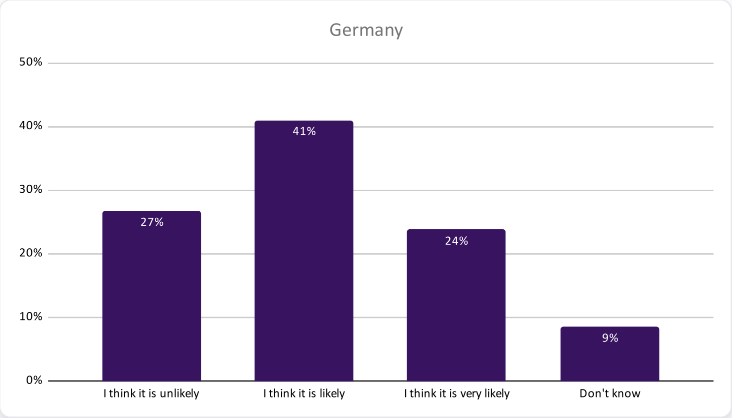


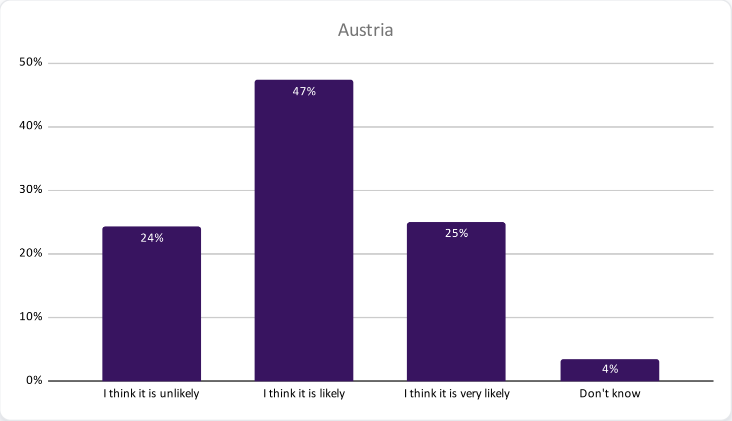
# **QUESTION NO. 3** – THE RISK OF A DATA BREACH

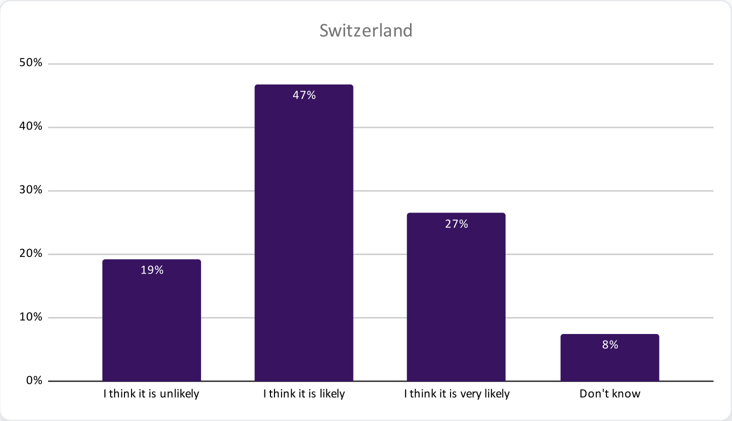
**Do you think it is likely that these smart devices will forward your data via the Internet and that your devices (and thus your data) will also be accessed via the Internet?**

Evaluation (DACH region, total):

- Approximately **70 percent** say they think it is **likely or very likely** that connected IoT devices will share their data
- Around **23 percent** say that they believe it is **unlikely** that connected IoT devices will pass on their data
- Around **7 percent** state that they are **unable to make a statement** in this regard





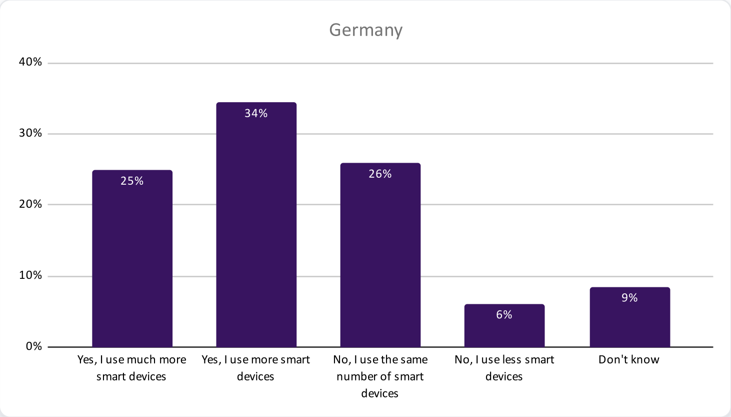


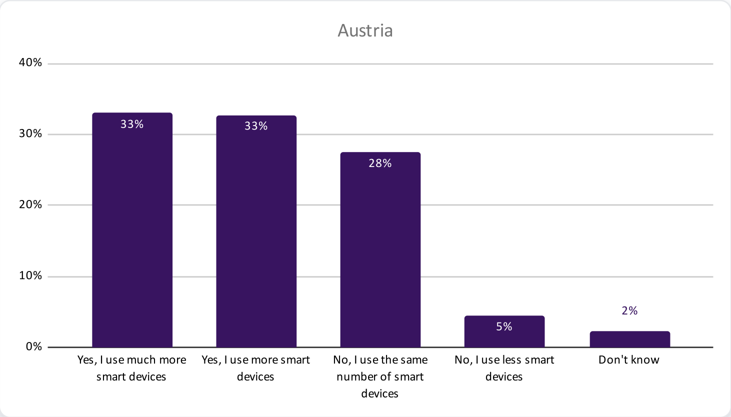
# **QUESTION NO. 4** – INCREASED USE OF IOT

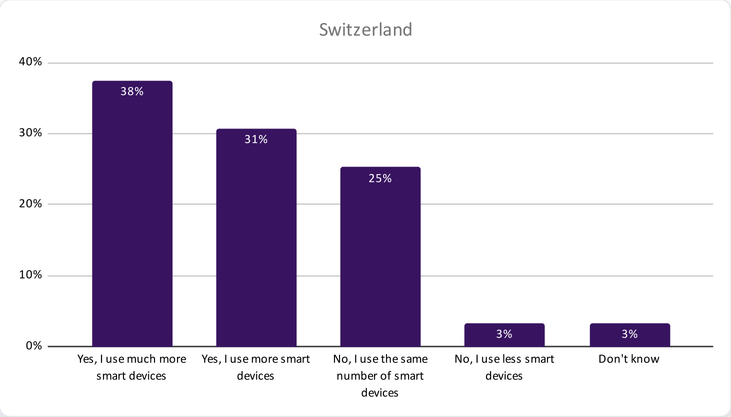
**Would you say that you use more smart devices with Internet access today than you did about five years ago?**

Evaluation (DACH region, total):

- Approximately **65 percent** say that they **use more or much more** IoT devices today
- Approximately **31 percent** say that they **use the same number or fewer** IoT devices today
- Approximately **5 percent** say that they are **unable to make a statement** in this regard





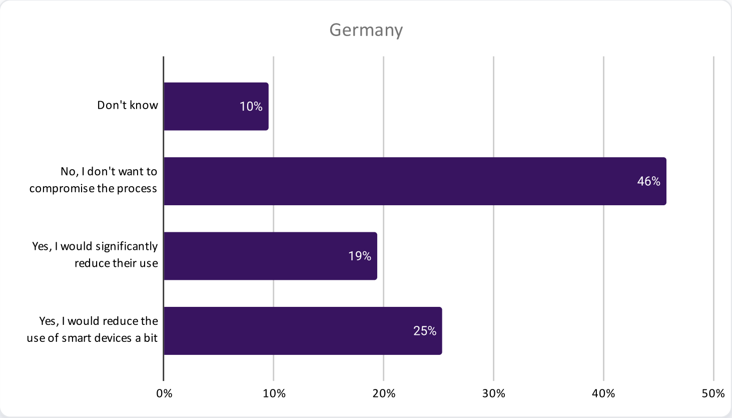


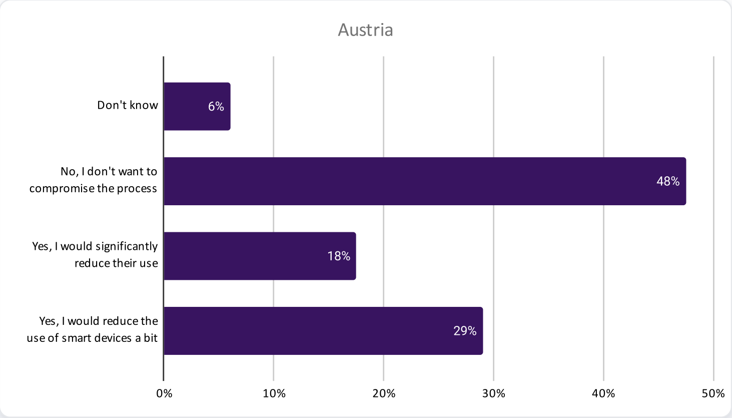
# QUESTION **NO. 5** – A TRADE-OFF

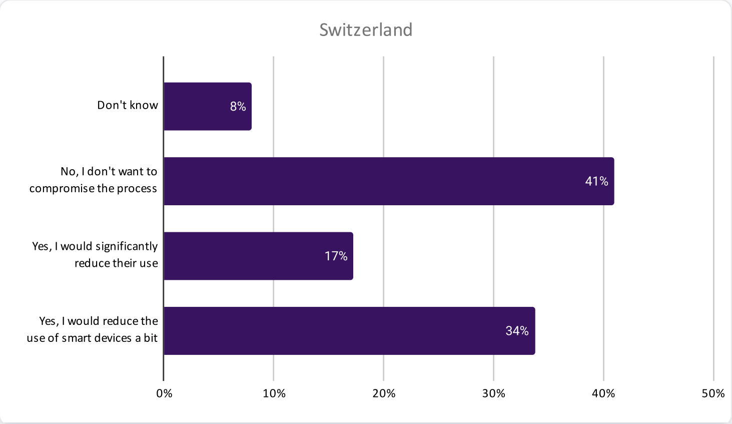
**Would you be willing to reduce the use of smart devices and utilize greater numbers of conventional devices without Internet access in order to increase data security, even if you had to make sacrifices in terms of process simplification or competitiveness?**

Evaluation (DACH region, total):

- Approximately **47 percent** say that they would be **willing to reduce** the number of their IoT devices either **somewhat or significantly**
- Approximately **45 percent** say that they **would not be willing to reduce** the number of their IoT devices
- Approximately **8 percent** say that they are **unable to make a statement** in this regard





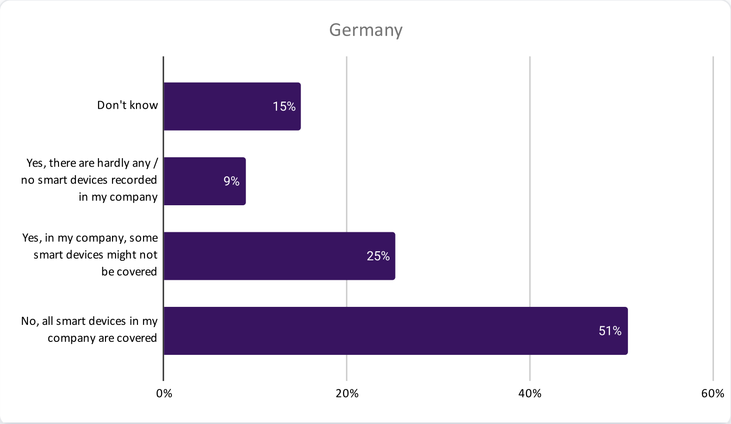


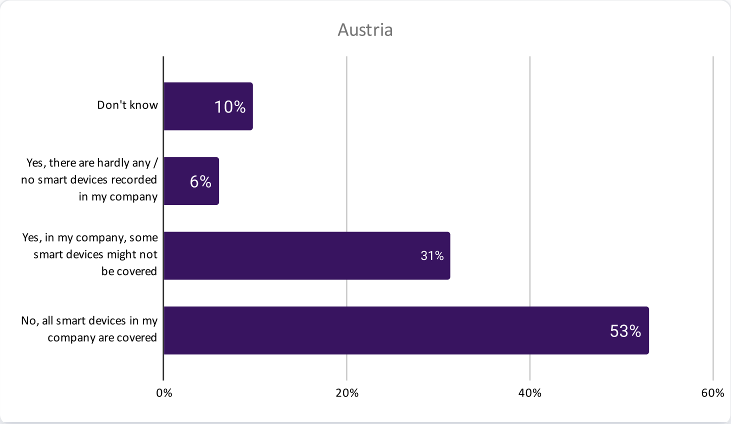
# QUESTION **NO. 6** – ASSET VISIBILITY

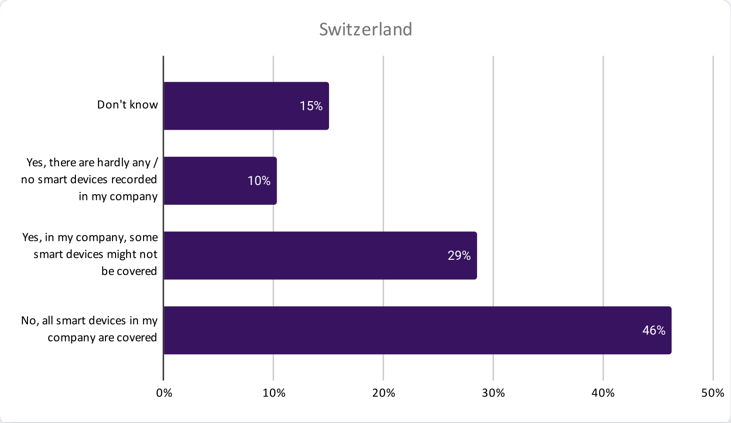
**Do you think it is likely that there are smart devices on your corporate network that are connected to other smart devices and/or to the Internet and are not included in your company's list of smart work devices?**

Evaluation (DACH region, total):

- Approximately **50 percent** say that they believe it is likely that **all IoT devices are known** in their company
- Approximately **37 percent** suspect that there are some **gaps in knowledge**
- Approximately **13 percent** state that they are **unable to make a statement** in this regard





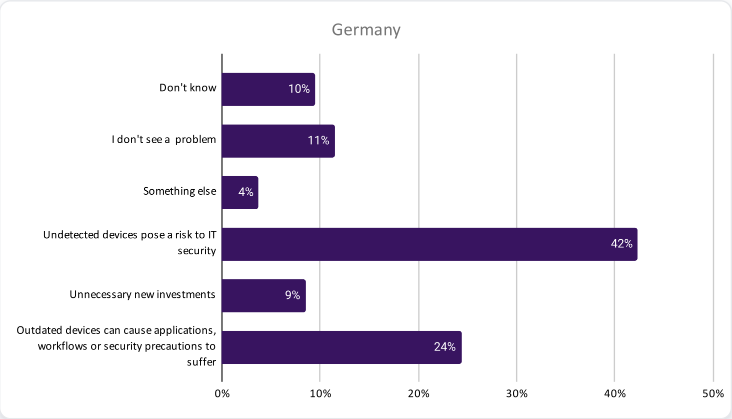


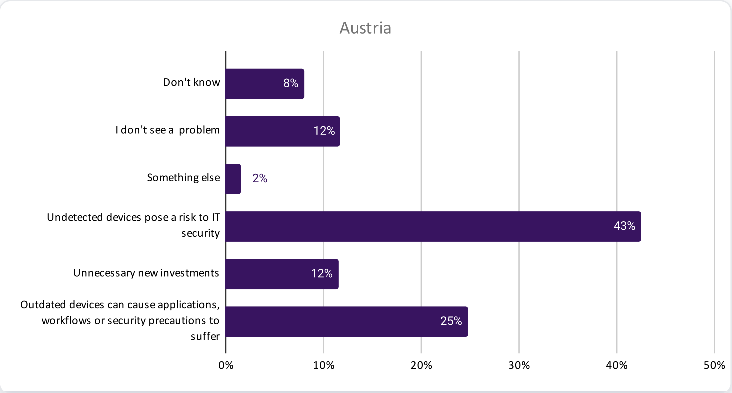
# QUESTION **NO. 7** – RISK OF UNDETECTED DEVICES

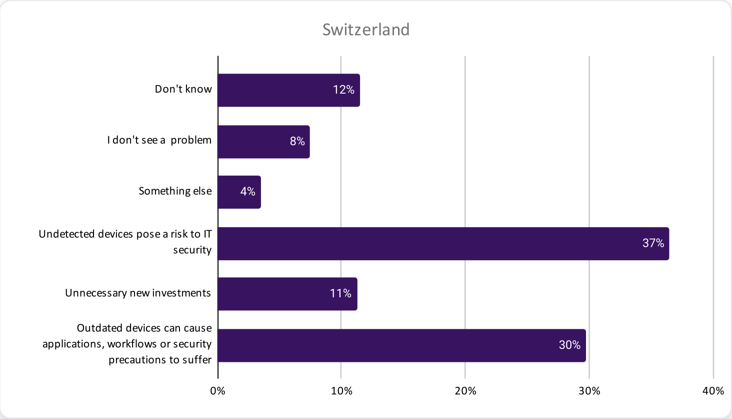
**Which problem associated with undetected and unaccounted for smart devices in the enterprise do you think is most serious?**

Evaluation (DACH region, total):

- Approximately **41 percent** say that they regard undetected devices as a **risk to IT security**
- Approximately **40 percent** say that they associate **other risks** with undetected IoT devices
- Approximately **20 percent** say that they are **unable to make any statement** in this regard or that they **cannot see any problems**





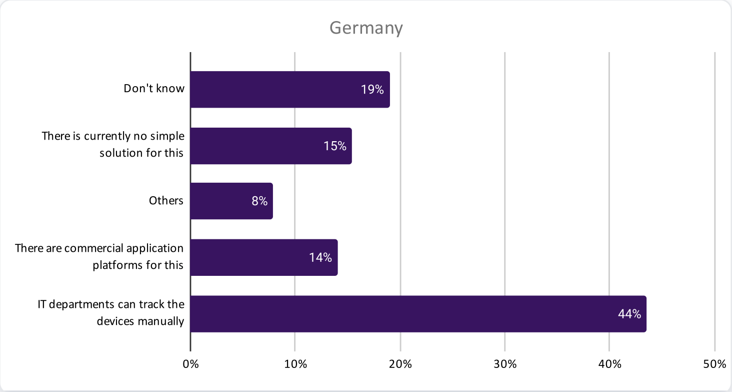


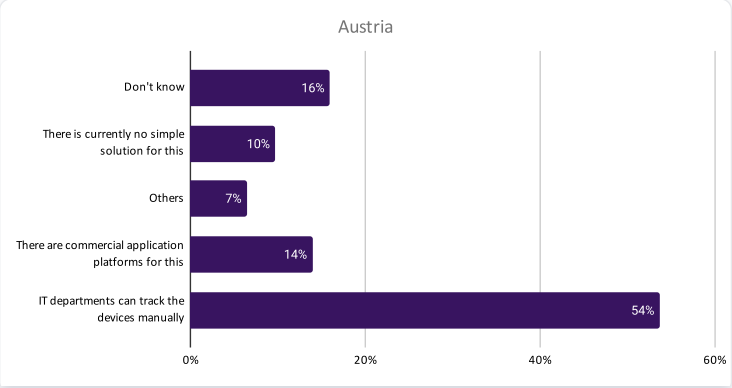
# QUESTION **NO. 8** – THE SOLUTION

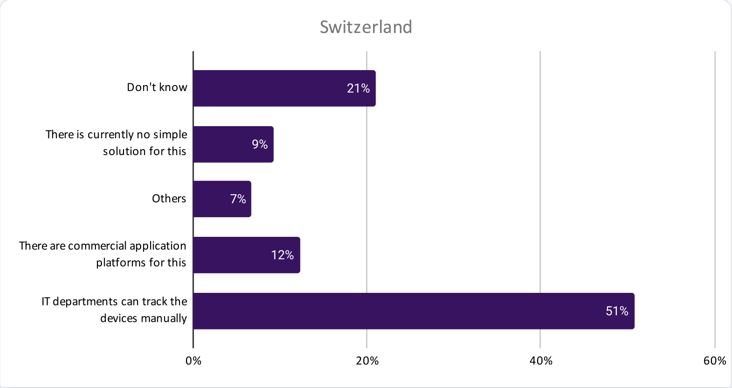
## How do you think undetected and/or unaccounted for smart devices can be tracked down in the enterprise?

Evaluation (DACH region, total):

- Approximately **50 percent** say that **IT departments** can track down the devices manually
- Approximately **19 percent** say that they are **unable to make any statement** in this regard
- Approximately **13 percent** say that **commercial platform solutions** are available for this purpose
- Approximately **11 percent** say that **no simple solution currently exists**
- Approximately **7 percent** say that they are currently using a **different solution**







# **EVALUATION** – DACH IT DECISION-MAKERS ARE NOT CONFIDENT ABOUT IOT SECURITY

The number of IoT devices used in DACH companies is growing. Around 2/3 of the DACH respondents confirm that their company uses more IoT devices today than it used five years ago. However, they generally lack a complete overview of all connected IoT devices. Only slightly less than half believe they are aware of all IoT devices connected to their corporate network.

The disquieting thing about this is that only 1/3 believe there is an increased security risk associated with the use of IoT devices. And they believe this despite the fact that approximately 2/3 say they are aware that IoT devices can transmit data to the outside world and from the outside world back into the corporate network without them noticing.

Uncertainty surrounds the question of how this risk could be contained. Only about half would be willing to reduce the number of their IoT devices in order to increase their network's security because the added economic value of these devices is simply too preponderant. About half believe that manual research by the IT department offers a viable path. And, 11% go so far as to say that adequate solutions do not exist at all. This is a widespread misconception, as will be shown below.

Only one in every ten survey participants says that **commercial platform solutions** that currently exist could help.

**The Armis survey shows** that only very few DACH companies know how to reconcile value creation and security when it comes to the use of IoT devices. However, the DACH region is not alone with this result.

# **INADEQUATE MONITORING** OF IOT DEVICES EXACERBATES VULNERABILITY

The number of attacks on IoT devices has been escalating for years. The global increase exceeds 100 percent annually. In the first half of 2021, Kaspersky alone recorded 1.5 billion attacks on IoT honeypots that it had deployed worldwide. [5] Again, this was an increase of more than 100 percent compared to the previous year. This comes as no surprise, as companies across the board continue to face significant difficulties in coming to grips with the security of their IoT devices. More than 50 percent of devices are vulnerable to medium and severe cyberattacks, [6] and 98 percent of their data is transmitted over the network in unencrypted form. [7]

The number of attacks on IoT devices also increased significantly in the DACH region again last year. The DACH healthcare industry was hit particularly hard. Approximately 69 percent of the IT decision-makers in this industry assume that their IoT infrastructure is insufficiently secured. In Germany alone last year, 21.3 percent reported an increase in attacks on the IoT systems they are responsible for securing. Nevertheless, only 23.3 percent have resolved to heighten the security of their IoT devices this year. Only slightly under 1/3 conduct regular audits at all. [8] These alarming figures are frighteningly similar to those discovered in the Armis survey.

One thing above all is needed to counteract this: investments in the automated monitoring and management of the entire network landscape. Contrary to popular belief, effective technical solutions are now available.

# **TRADITIONAL SOLUTIONS** DON'T HAVE A GRIP ON IOT DEVICES

For a long time, IT decision-makers had to rely on traditional endpoint and network security solutions. But when it comes to identifying and managing IoT devices, these solutions have not been very effective – and they continue to be insufficiently effective. It is accordingly not surprising that nine out of ten IT decision-makers in the Armis survey do not regard commercial platform solutions as a suitable answer to their IoT security challenges. IoT devices are not agent-compatible. They also operate from the access layer of a network, rather than from its distribution or core layer. Network security solutions that use choke points and parameters to locate and identify IoT devices lack key starting points to effectively detect and manage these devices. But new, modern solutions that can circumvent this very problem do indeed exist. One such solution is the **Armis Agentless Device Security Platform**.

# **ARMIS** – AN EFFECTIVE PLATFORM SOLUTION FOR THE ENTIRE NETWORK ENVIRONMENT

Armis is currently the world's leading security platform for detecting and managing all types of endpoints – whether they are managed or unmanaged, IoT, or OT devices.

The platform can detect, identify, and secure every connected device in real time and without degrading the network's performance. To accomplish this, all traffic on the company's LAN and WLAN is passively monitored. The results are then analyzed and evaluated based on the data stored in the Armis Device Knowledgebase, which contains over 2 billion devices. This enables the platform to identify and classify each device. Anomalies can thus be assessed, threats can be detected, and countermeasures can be taken in a timely manner. The Armis platform tracks all connections and data histories in real time, compares them with known reference values, and automatically detects policy violations, misconfigurations or unusual behavior. If a threat is suspected, the IT department is automatically notified. The personnel in the IT department can then sever the connection between the network and the IoT device in time and quarantine the infiltrated device.

### Managed IoT devices

Managed IoT devices are completely controlled by the service provider. The user has no overview or possibility of influencing them.

### Unmanaged IoT devices

Unmanaged IoT devices are completely controlled by the user. The service provider has no overview or possibility of influencing them.

The Armis platform is not only suitable for IoT devices. It can also be used to discover, identify and monitor all devices connected to a network, thus securing the network against unauthorized access – whether they are managed or unmanaged devices, operational technology or even industrial control systems. With the Armis platform, enterprises can finally take comprehensive control of their entire network environment.

**Book a demo and discover how the Armis platform can enable your organization to see and secure all your devices.**

# SOURCES

1. Statista, Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025 (in billions), 2021.
2. IDC, Worldwide Semiannual Internet of Things Spending Guide, 2021.
3. IDG, Studie Internet of Things 2021, 2021.
4. Tara Seals, IoT Attacks Skyrocket, Doubling in 6 Months, in: threatpost.com, September 6, 2021.
5. PYMNTS.com, Kaspersky Detects 1.5B IoT Cyberattacks This Year, 2021.
6. Unit 42, 2020 Unit 42 IoT Threat Report, 2020.
7. Unit 42, 2020 Unit 42 IoT Threat Report, 2020.
8. Kaspersky, Patient Krankenhaus – Studie zur IT-Sicherheitslage im Gesundheitswesen in Deutschland, Österreich und der Schweiz, 2021.

## About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

info@armis.com

20211223-1

ARMIS®