Securing the Internet of Things

A Comprehensive Guide

2023

info@utahtechlabs.com

www.utahtechlabs.com

Agenda

→ Introduction

→ Who We Are

→ IoT Solutions - What Is It?

→ Why IoT Security Is Important?

→ Numbers

→ Crucial IoT Cyberattacks

→ What Contributes to the Challenges of IoT Security?

→ IoT Security Guidelines and Best Practices

→ Case studies

→ Resources for Cybersecurity

Embracing Secure Connections: **Empowering End-to-End Protection for Connected Devices**

In the age of digital transformation, the industrial landscape is experiencing an exponential rise of unmanaged devices, driving the demand for a strong IoT security strategy. By shedding light on the importance of proactive measures and collaborative initiatives, this paper aims to equip organizations with the knowledge and tools needed to navigate the complexities of IoT security and fortify their defenses against cyber threats.

Who We Are ?

UTL has unmatched expertise in digital transformations. By providing technology services, we can make your business autonomous and help you build your digital vision. Our solutions turn IT into a strategic asset, helping you overcome challenges in automation, service management, and operations.

Utah Tech Labs offers secure connections, end-to-end protections, and IoT security strategies for connected devices. Our expertise in IoT cybersecurity and big data analytics ensures a resilient IoT ecosystem. Partner with us to unlock the full potential of your business.

150

Experienced engineers

$1.8B

In customer revenue

5.6%

Attrition rate, the industry's lowest

6+

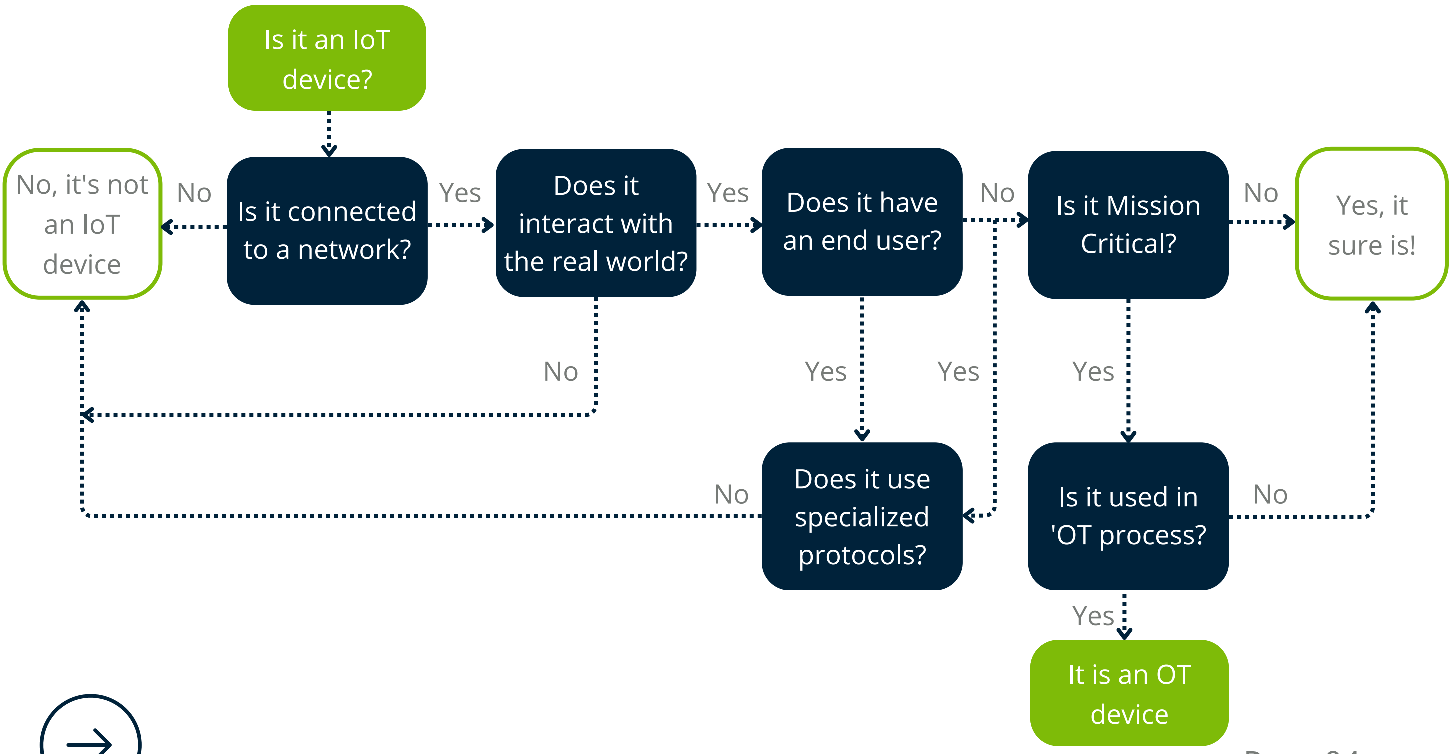
Diverse domains we serve

IoT Solutions
What Is It?

IoT security encompasses the measures and technologies employed to safeguard mechanical systems, software-enabled items, and networked computing devices within the Internet of Things (IoT) ecosystem. These safety measures, including secure connections and end-to-end protections, are designed to mitigate or eliminate cyber dangers associated with these devices.

The term "Internet of Things device" encompasses a wide range of items, from biological implants to sensors on machinery and electrical equipment. In industrial settings, smart devices collect, transmit, and respond to data from their surroundings. Some devices even engage in communication and decision-making based on the provided information.

Typically, a gateway or edge device acts as an intermediary, receiving data from these devices and transmitting it for local or cloud-based analysis. Regardless of whether a device belongs to the IoT, OT (Operational Technology), or IT (Information Technology) category, it requires protection to ensure operational resilience. The accompanying graphic helps illustrate the distinctions between these device types.

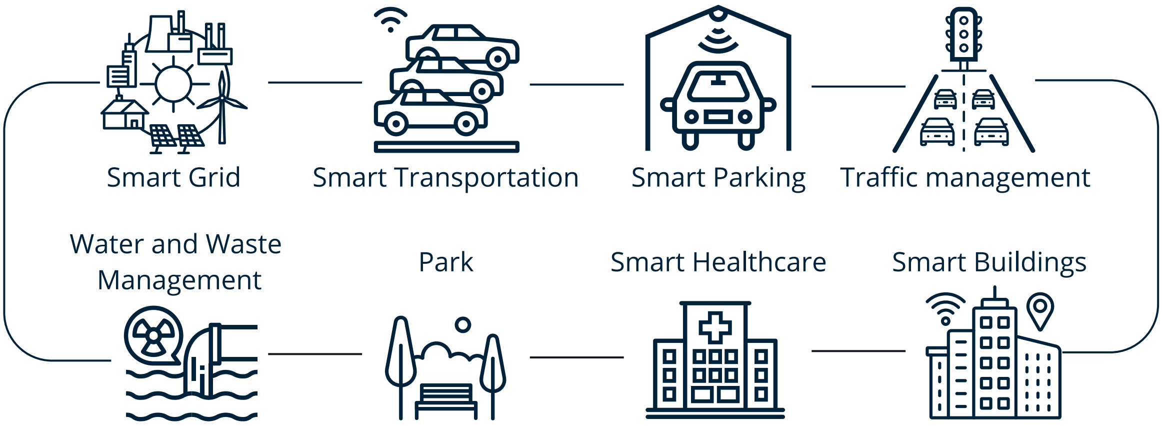


Is it an IoT device?
Is it connected to a network?
No
No, it's not an IoT device
Yes
Does it interact with the real world?
Yes
Does it have an end user?
No
Is it Mission Critical?
No
Yes, it sure is!
No
Yes
Yes
Yes
Does it use specialized protocols?
No
Is it used in 'OT process?
No
Yes
It is an OT device

Why Is IoT Security Important?

Operators of critical and industrial infrastructure are quickly deploying billions of devices to improve their automated processes by utilizing the data produced by these devices. However, this increasing trend poses new cybersecurity vulnerabilities as these gadgets connect to both public and private networks. Unfortunately, cyberattackers view these endpoints as easy targets for executing IoT cyberattacks, exploiting operational procedures, and seeking financial gain. At Utah Tech Labs (UTL), we prioritize IoT network security, offering robust measures to safeguard your infrastructure from such threats.

The illustration provided below shows the different uses for these gadgets in our day-to-day activities. Despite the fact that businesses use these technologies for a variety of objectives, improving their resilience against cyber threats should always be a top concern. Imagine the possible effects of a damaged electric grid or interference with life-saving equipment in a hospital. These situations are examples of critical infrastructure locations where disastrous consequences might occur.



Numbers

Since the beginning of this industry, the Internet of Things market has been on an exciting journey. The sector reached $100 billion in market revenue in 2017, and if it follows forecasts, that figure should grow to around $1.6 trillion by 2025.

It's estimated that the number of active IoT devices will surpass

25.4 bn

in 2030.

IoT solutions have the potential to generate

$4-11 tn

in economic value by 2025.

83%

of organizations have improved their efficiency by introducing IoT technology.

By 2025, there will be

152,200

devices connecting to the internet per minute.

Numbers

Hardware currently accounts for around 30% of the market's value.

The most-notable changes in this dynamic industry will emerge around new software that allows for IoT connection between devices.
Hardware still accounts for 30% of the total value of IoT technology, although trends suggest its global market value is decreasing.
(McKinsey Digital)

The amount of data generated by IoT devices is expected to reach 73.1 ZB (zettabytes) by 2025.

IoT big data statistics show that, with increased adoption, devices will globally generate exponentially more data in the following years. The numbers will reach 73.1 ZB by 2025, which equals 422% of the 2019 output, when 17.3 ZB of data was produced. To put that in perspective – one zettabyte is 1021 bytes, i.e. one billion terabytes (TB) or one trillion gigabytes (GB).
(IDC)

Companies could invest a total of up to $15 trillion in IoT by 2025.

It's no news that many companies have already taken note of IoT devices' vast potential to add value to their business operations. IoT statistics show that many clothing manufacturers, healthcare providers, and municipalities have already chosen to invest in this technology.
(Gigabit)

Our Mission

Crucial IoT **Cyberattacks**

IoT security issues are widespread and affect many gadgets, including thermostats, sensors, cameras, and process controllers. The potential danger posed by these weaknesses has already manifested itself in several notable events. One such case was the still-largest DDoS attack in history, the Mirai Botnet Attack in October 2016. Along the US East Coast, this attack severely disrupted internet service. The attackers gained access to several routers and CCTV cameras using unsecured Telnet ports and default passwords, turning them into a potent botnet army.

Different iterations of this malware are still around today, and the Nozomi Networks Labs team continues to keep a close eye on them.

In 2017, ten terabytes of data were stolen from a North American casino shortly after it was installed by hackers using a Wi-Fi-enabled fish tank thermometer. Through exploiting the thermometer's connectivity, threat actors gained access to the casino's network and extracted data on high-value customers. This event shows how a gadget can act as a doorway to a datacenter hosting sensitive apps and personal and financial data.

What Contributes to the **Challenges of IoT Security?**

01
Phase

Inherent Lack of IoT Security in Devices

IoT devices are often designed without adequate security measures and often remain unmanaged and lack suitable security safeguards. As a result, software updates are irregular or nonexistent, particularly for firmware where vulnerabilities are frequently present.

02
Phase

Ineffective Identity and Access Control Techniques

Hostile actors can break into IoT devices easier than well-managed IT equipment due to default passwords and insufficient authentication protocols.

03
Phase

Exposure of Connected IoT Devices as Entry Points

IoT devices are interconnected within an ecosystem that includes business applications, data centers, IT infrastructure, and the cloud. Due to their default lack of robust cybersecurity controls, they become attractive targets for hackers seeking entry into the broader network.

What Contributes to the **Challenges of IoT Security?**

04
Phase

Poor network segmentation

Large-scale industrial IoT implementations lack network segmentation needed to mitigate cyber threats or stop malware spread.

05
Phase

Limited Capability for Agent-Based Security Software Installation

The majority of IoT devices that are available on the market cannot host software security agents. IoT devices don't have full-featured operating systems like Windows, Mac, or Linux; instead, they have functionally constrained operating systems with constrained processing and communication power.

06
Phase

Unauthorized IoT Device Deployment

IoT devices usually omit IT and cybersecurity teams. Due to the lack of extra cybersecurity layers, this might result in devices being placed in vulnerable or sensitive parts of the network. This makes them easy targets for compromise.

IoT Security Guidelines and Best Practices

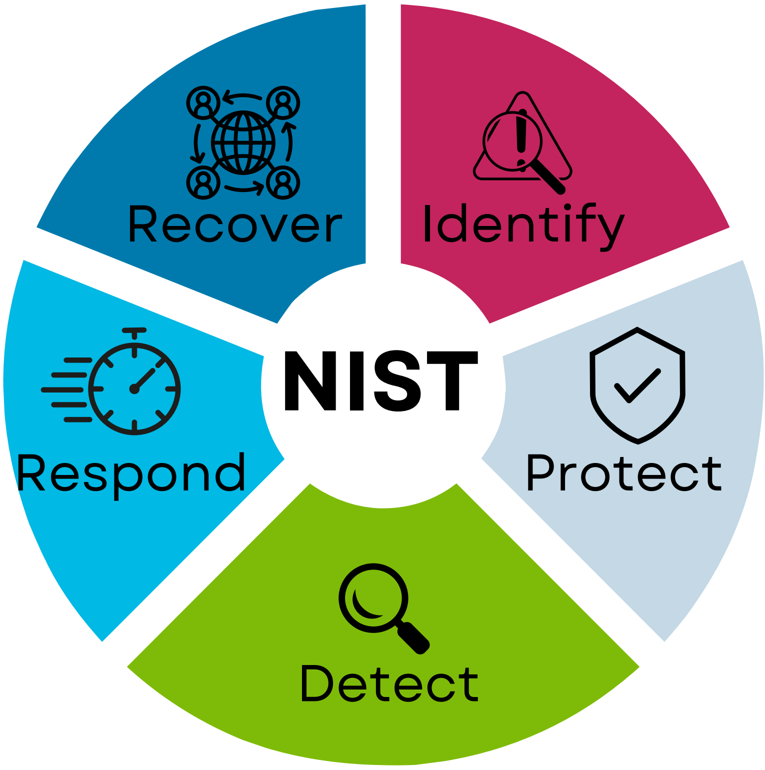
Although there isn't a single regulatory authority monitoring IoT cybersecurity, various federal efforts have been made to improve security procedures. NIST's (National Institute of Standards and Technology) Cybersecurity for IoT Program was launched in 2020. This program aims to create an environment that encourages global innovation and fosters IoT trust. This is done through the creation of standards, guidelines, and tools.

The NIST Cybersecurity Framework (CSF), a risk-based framework created to help enterprises protect their vital infrastructure and data, is one of NIST's useful resources. The CSF offers vocabulary and rules for understanding, controlling, and discussing cybersecurity threats.

We'll discuss some best practices for IoT security strategy using the NIST Cybersecurity Framework.

NIST Cybersecurity framework

The transfer of information on cybersecurity threats that affect IoT devices with industry partners and government organizations is another best practice. Yet another is to continuously review and enhance your cybersecurity protocols to make sure they are efficient and in line with the changing threat landscape.



Best Practices

1. Identify

Gain a comprehensive understanding about the IoT devices used in your company and the threats they bring. This entails determining the information that is gathered and transferred by these devices and estimating the possible outcomes of a cybersecurity breach. At this point, it is necessary to implement an asset management system that can deliver real-time data, such as zone and network location specifics, lifecycle data, and patch status.

2. Protect

Implement the necessary security measures to protect your network. This includes a firewall that can isolate, or end connections linked to malware or questionable activities. Network segmentation, multifactor authentication (MFA), and encryption are possible extra security measures. Create a system where network security engineers can apply patches to the assets that are most at risk and susceptible first, reducing overall cyber threat risk and boosting resilience.

3. Detect

To find possible cybersecurity threats and vulnerabilities, implement monitoring and detection techniques. This could entail using security incident and event management (SIEM) systems, network monitoring, and log analysis. Use a network monitoring system for industrial networks that may identify important threats in real time and integrate with network access control (NAC) solutions. For instance, in a DMZ configuration, it can instruct NAC to assign reserved VLANs for essential or sensitive assets.

Best Practices

4. Respond

To effectively respond to cybersecurity problems, develop and implement an incident response plan. Procedures for locating and isolating affected devices and systems, as well as for informing the appropriate parties about the occurrence, should be outlined in this strategy. The response procedure can be accelerated and streamlined by using thorough incident response playbooks and forensic analysis tools.

5. Recover

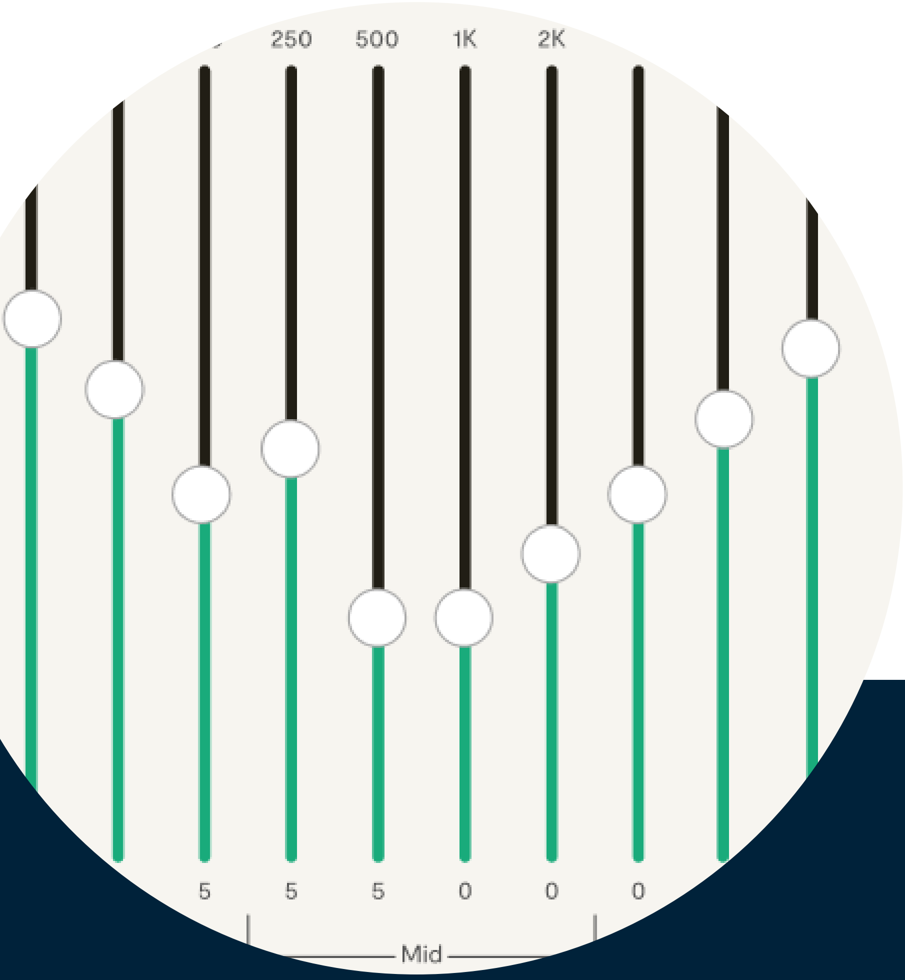
Prepare for business continuity situations and put recovery plans into operation. Establish restoration methods for the impacted systems and processes and come up with ways to lessen any potential effects. Review and adjust these methods frequently to make sure they remain effective and are in line with new risks.

Other best practices include exchanging information on cybersecurity dangers related to the Internet of Things with industry partners and governmental organizations. Additionally, in order to effectively respond to the shifting threat landscape, cybersecurity practices must be continuously evaluated and improved.

Case study Marley

House of Marley unveiled its latest app for seamless Bluetooth speaker connectivity and personalized music customization.

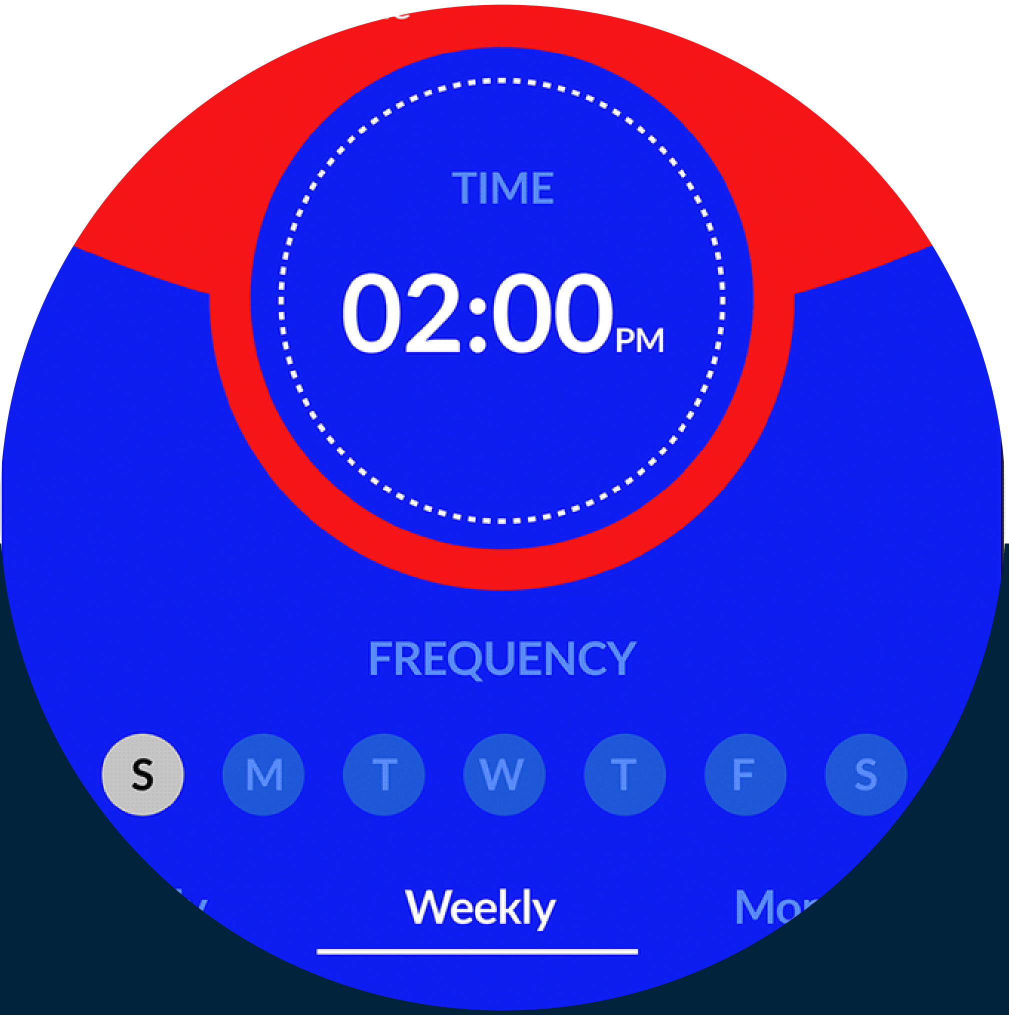
House of Marley's new app will allow you to connect all of your speakers via Bluetooth and customize your music experience. In this new feature, one will be able to control equalizers, ANC, and ambience to enhance the music experience.



Case study
Basu

BASU® Magic™ Launches EAlarmGPS™ - World's First Smart Emergency Alarm with Mobile App and Configuration Settings.

B A S U® Magic™, we were asked to create a configuration setting for their eAlarm device and a mobile application alternative. EAlarmGPS™ is the World's First (and standalone) Smart Emergency Alarm.



Case study
Drift

Experience Serenity Anytime, Anywhere with Drift - The Revolutionary ASMR Device for Mindfulness and Stress Relief.

Drift is our groundbreaking ASMR device designed to help you find tranquility and balance. If you're feeling stressed or seeking a way to enhance your mindfulness practice, Drift is the perfect solution.

drift
by HOMEDICS®

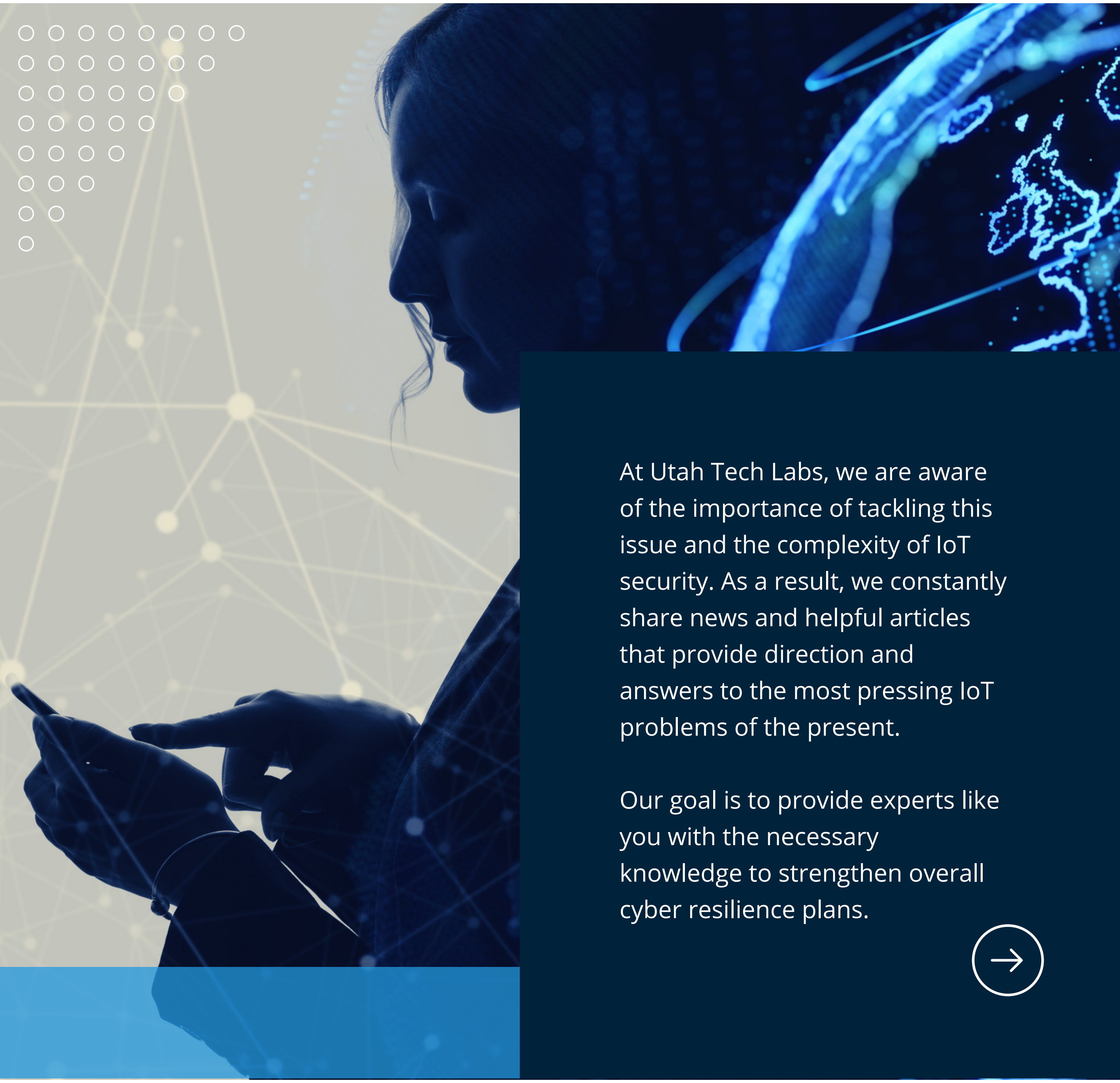
Case study
Nurvv

Revolutionize Your Running Experience with NURVV - The UK-Based Company's Innovative Running Devices and Companion Mobile App.

NURVV, a UK-based company, that we helped create a mobile application for runners and connected it to their innovative running (

NURVV | RUN™

Resources for Cybersecurity



At Utah Tech Labs, we are aware of the importance of tackling this issue and the complexity of IoT security. As a result, we constantly share news and helpful articles that provide direction and answers to the most pressing IoT problems of the present.

Our goal is to provide experts like you with the necessary knowledge to strengthen overall cyber resilience plans.

Let's Work Together

Whether you are doing product research, evaluating competitive solutions, or just scope planning to begin a project, we are ready to help you. We can assure you that you have all the right information.

UTL has helped many of the world's largest businesses with automated insights and optimized IT solutions. Let's put that experience in your business and growth.

Utah Tech Labs

☎ +1-801-633-9526

✉ info@utahtechlabs.com

🌐 www.utahtechlabs.com