Strategies to Improve Security Posture and Agility at the Edge

THIS EBOOK EXPLORES THE SINGLE MOST DANGEROUS SECURITY RISK TODAY

ATTACKS CAN HAPPEN ANYWHERE, AT ANY TIME

Ripple20, SolarWinds, SACK and Amnesia are strong evidence that security threats are always present.

This ebook explores the single most dangerous edge security risk today and provides guidance on improving security posture and agility to manage and mitigate future attacks.

WHAT IS THE SINGLE MOST DANGEROUS EDGE SECURITY RISK TODAY? COMPLACENCY OR INACTION.

Complacency or inaction arises from numerous and varied factors, like insufficient resources, lack of expertise and competing priorities.

Here are some common circumstances:

- Deployment of seemingly innocuous connectivity solutions in vast and mission critical networks that are vulnerable to attack
- Irregular security software updates of decentralization hardware, especially those that require remote updates
- Deployment of a variety of connected devices with complex architecture and no common toolset to easily manage them
- Limited physical controls to protect vital network components, especially those outside the security of the data center
- Insufficient security protocols for license dongles and other critical devices

FIVE PROACTIVE STRATEGIES

IMPROVE SECURITY POSTURE AND AGILITY AT THE EDGE

1

Assume the next attack will happen, because it will.

a. Treat the edge of the edge as public.

b. Apply a layering tactic using different independent methods of protection.

c. Design security redundancy into the system in the event a security control fails, or a vulnerability is exploited.

d. Enhance physical security measures at the edge with access controls and surveillance, to reduce chances of theft or unauthorized access. When this is not feasible, use hardened and secure encrypted devices.

2

Don't just design for today, design for the future.

a. Only deploy infrastructure management components with local encryption and other security features.

b. Plan for future cryptographic algorithms that will require increases in memory and CPU capacity.

c. Configure for auto updates of firmware to address future security requirements.

d. Design systems with security that can scale.

3

Continually evaluate every connectivity component, and plan for periodic updates.

a. Every component of a network, no matter how small or seemingly insignificant, introduces risk. Replace connectivity hardware at the edge that does not promote security, only offers an outdated or unsupported security tool, or has limited memory and disk space to run the latest security updates.

b. Only deploy the latest industry leading network components, with security measures enabled and configured to the most secure settings possible, right out of the box.

FIVE PROACTIVE STRATEGIES

IMPROVE SECURITY POSTURE AND AGILITY AT THE EDGE

4

Proactively increase agility to react to security threats.

a. Use an enterprise management system (EMS) like Digi Remote Manager® to centrally configure, monitor, log and audit connected hardware, and to easily adapt and deploy security updates without creating new vulnerabilities.

b. Deploy containerization technologies to ensure applications run smoothly from one computing environment to another to facilitate simple, rapid deployment, increased productivity and improved security.

5

Proactively build security into all connectivity solutions.

a. Simplify building secure, connected products with a security framework, such as Digi TrustFence®.

b. Incorporate security controls at every point of access, from secure boot to secure ports, encryption and authentication by user level.

A USB-OVER-IP PLATFORM THAT MEETS ALL FIVE PROACTIVE STRATEGIES

Digi AnywhereUSB® Plus — Industry Leading USB Connectivity More Speed, More Power and More Security

Digi AnywhereUSB Plus, with Digi TrustFence built-in and combined with Digi Remote Manager, meets all five proactive strategies to improve security posture and agility at the edge.

DIGI ANYWHEREUSB PLUS PROVIDES RELIABLE DATA TRANSFER AND USB DEVICE CHARGING

Maximum USB Speed with AnywhereUSB Plus

Digi AnywhereUSB Plus uses USB 3.1 gen 1 Type A ports. While in direct connection environments, these ports can achieve theoretical speeds of up to 5 Gbps performance on AnywhereUSB Plus but will be slower due to the nature of the AnywhereUSB protocol and the effect of the network.

To maximize transfer speeds, your USB cables should all be rated for USB 3.1 or higher, you should connect devices directly to the AnywhereUSB Plus and not add an additional hub downstream of the AnywhereUSB Plus. Also monitor the network connection between the AnywhereUSB Plus and the Computer that will access the devices to be aware of any capacity constraints on the network side.

Digi AnywhereUSB Plus is backwards-compatible with USB 2.0.

Many USB Configuration Options and Benefits

Digi offers the flexibility of 2, 8 or 24 USB ports for small, medium and high-density device management.

Control access and assign specific ports or groups of ports at an individual or group level. Different users can only access the equipment they are approved to work with, as they need it, without affecting access to any other devices being managed.

Digi AnywhereUSB 2 Plus

2 USB 3.1 Gen 1 Ports
Single 10M / 100M / 1G Ethernet
5 VDC

Digi AnywhereUSB 8 Plus

8 USB 3.1 Gen 1 Ports
Single 10M / 100M / 1G / 10G Ethernet
12 VDC
Single SFP+

Digi AnywhereUSB 24 Plus

24 USB 3.1 Gen 1 Ports
Dual 10M / 100M / 1G / 10G Ethernet
Dual Power 100-240 VAC
Dual SFP+

DIGI ANYWHERE USB PLUS INCREASES YOUR SECURITY POSTURE AND AGILITY

USB Hub with Industry Leading Security

The TLS certificate-based security of Digi AnywhereUSB Plus is uniquely encrypted to protect sensitive financial, personal and technical data across a network. Digi TrustFence is built in. Designed for mission-critical applications, Digi TrustFence serves as a foundation that enables you to easily integrate device security, device identity, and data privacy capabilities into your network of USB devices. Digi TrustFence designs security into IoT devices that can grow and adapt with new and evolving threats.

The following features are built into every Digi AnywhereUSB Plus device:

- Unique password for each hub
- Configurable network service port numbers
- Secure access and authentication to the web UI and CLI
- One password, one permission level

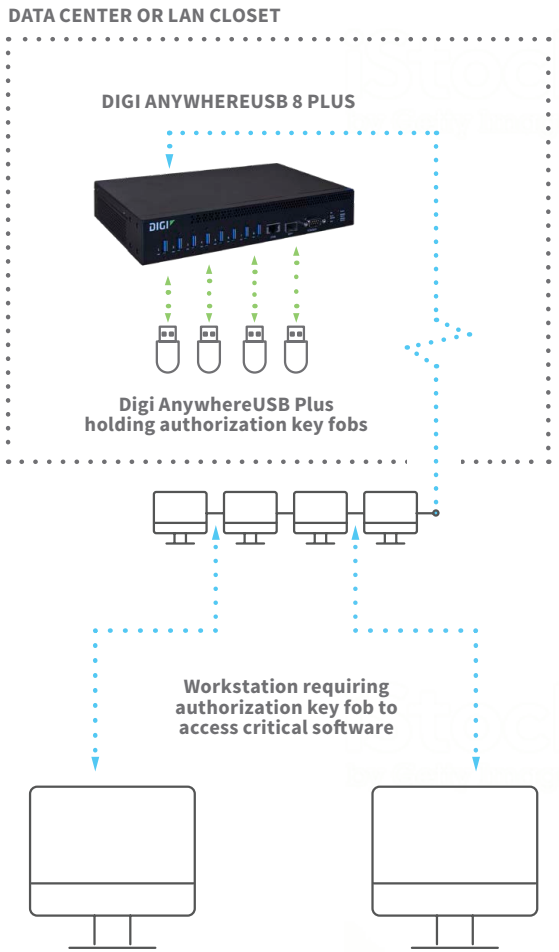
- Ability to selectively enable and disable network services such as mDNS, HTTP/HTTPS, and SSH
- Encrypted access to AnywhereUSB Plus traffic: Access to the USB-over-IP traffic is encrypted and authenticated by default and cannot be disabled
- Comprehensive management capabilities with Digi Remote Manager, which enables you to manage Digi AnywhereUSB Plus remotely and securely
- Protected by the Digi TrustFence® framework

LICENSE DONGLES CAN POSE A SECURITY RISK

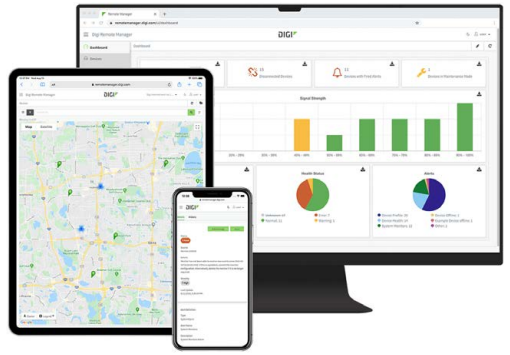
Control Access to Dongles

Digi AnywhereUSB Plus protects dongles from being stolen, lost or damaged while allowing employees to connect to and interact with equipment or computers.

Digi AnywhereUSB Plus hubs can be daisy chained together to accommodate 127 dongles at one time.



CONFIGURE, DEPLOY AND MANAGE REMOTE USB-OVER-IP ASSETS SECURELY



ADD DIGI REMOTE MANAGER TO DIGI ANYWHEREUSB PLUS

- Industry-leading cloud and edge tools for rapid device deployment, and easier asset management
- Monitor IoT devices, asset performance and security with bi-directional communications
- Automate mass firmware and software updates to enhance functionality, stay in compliance and scale your deployment
- Access data from edge devices that were previously out of reach
- Integrate device data through open APIs to gain deeper insights and control with third-party applications
- Receive real-time alerts and detailed reports on network health and device conditions

LET'S CONNECT

United States	Matt.Propes@digi.com
Canada	Chris.DeHoog@digi.com
EMEA	Jean-Marie.Dubois@digi.com
Other	Businessdevelopment@digi.com

Digi is a complete IoT solutions provider, supporting every aspect of your project, from mission critical communications equipment, to professional services, to getting your application designed, installed, tested and functioning securely, reliably and at peak performance.

Digi has 35+ years of experience connecting the “things” in the “Internet of Things” — devices, vehicles, equipment and assets. Digi has been issued more than 160 patents and we have connected over 100 million devices.