Network security device USB

AI Overview

USB security devices protect networks by controlling access, monitoring activity, and preventing malware or data theft through physical and software-based measures.Physical USB SecurityUSB port blockers and cable locks are simple yet effective hardware solutions. Port blockers physically prevent unauthorized USB devices from being connected, while cable locks secure active devices like keyboards or docking stations to prevent tampering or accidental disconnection . High-security environments may use epoxy sealing or locked computer cases to permanently disable or restrict USB access . These measures are particularly useful in public-facing systems, healthcare, retail, and industrial environments.Software-Based USB SecurityUSB security software monitors, restricts, or blocks USB port usage to prevent unauthorized file transfers and malware infections. Features often include:Device whitelisting to allow only trusted USB devicesEncryption and access controls for sensitive dataActivity logging and real-time alerts for suspicious USB activityCentralized policy enforcement across endpoints Examples include AccessPatrol, which provides centralized management, auditable records of file transfers, and enforcement of USB policies even for remote devices . Other platforms, like DriveLock, implement a zero-trust approach, ensuring only verified users and devices can access critical data .Networked USB ManagementUSB-over-IP devices, such as Digi AnywhereUSB Plus, allow USB peripherals to be connected and managed over a network. These devices provide:Secure, encrypted connections using TLS and compliance with standards like FIPS-140-2, PCI-DSS, and HIPAACentralized control to assign ports to specific users or groupsSupport for multiple USB hubs daisy-chained to manage up to 127 devicesFlexibility for desktop, panel, or rack mounting, with options for Gigabit Ethernet and Wi-Fi connectivity This approach enables organizations to protect host PCs by relocating them to secure areas while still prov...

Article Content

Chinese hackers develop LONGLEASH malware to expand ORB network

Chinese hackers tracked as ''UAT-7810'' are actively evolving their malware to expand their Operational Relay Box (ORB) network by compromising internet-facing networking devices,

USB-Over-IP | AnywhereUSB Plus | Connect USB

These USB hubs provide secure, robust connectivity between peripheral devices and a PC without the physical proximity constraints typically associated with USB

Computer Network Tutorial

A computer network is a system of interconnected devices, such as computers, servers, smartphones, and printers, that communicate to exchange

Attackers Exploit Three Fortinet FortiSandbox Flaws, One Patched

Attackers are exploiting three Fortinet FortiSandbox flaws, including one patched last week, risking auth bypass and command execution.

Healthcare IoT Network Security: How to Protect Connected Medical ...

Harden medical devices with a practical healthcare IoT network security guide to segmentation, encryption, patching, device inventory and vendor controls.

CISA Urges Hardening Fortinet Devices After Reports of Credential ...

This activity, referred to as FortiBleed, involves the exposure of leaked credentials associated with approximately 74,000 Fortinet devices, including firewalls and virtual private network

Cable Locking Systems for Network & USB Security

Cable locking systems offer a simple but powerful way to secure USB and network connections, prevent downtime, and maintain control over critical infrastructure.

The Best Hardware Security Keys for 2026

These are the top security keys we''ve tested for keeping your information private and secure.

Home Network VLANs: Isolate IoT Devices for Security | State of ...

Segment your home network with VLANs to protect computers from compromised IoT devices. Complete guide to creating trusted, IoT, and guest networks with firewall rules.

Record-Breaking 15 Tbps DDoS Attack From 500,000

Microsoft Azure thwarted what may be the largest distributed denial-of-service (DDoS) attack ever recorded in the cloud on October 24.

Free Apps on Samsung and LG Smart TVs Secretly Turning Your Devices ...

Free apps available on Samsung, LG, Roku, and other major smart TV platforms have been quietly enrolling millions of living room devices into a commercial residential proxy network

SP 1800-36, Trusted Internet of Things (IoT) Device Network-Layer ...

This guide shows how to provide network credentials to IoT devices in a trusted manner and maintain a secure device posture throughout the device lifecycle, thereby enhancing IoT security in alignment

11 Best Practices for Securing USB Devices on a Network

However, with the wide availability of USB devices comes the need for more secure practices when using them. To ensure your network is secure against malicious attacks, here are 11

USB Blocking Techniques and Tools: Protecting Your Network from ...

Learn about effective USB blocking techniques and tools to prevent data breaches and malware infections from unauthorized removable media devices in your organization.

Using peripherals securely | National Cyber Security

Beyond removeable media, USB devices can provide additional capabilities that could be abused for malicious purposes. A good example of this is the USB

Secure Media Exchange (SMX) | USB Protection

Designed to prevent unchecked USB devices from accessing USB ports while keeping the port active for authorized devices. Honeywell SMX is capable of

Device Connectivity Accessories & Port Security

Secure your devices with premium connectivity accessories and port security products. Explore USB locks, HDMI locks, network locks, and Smart Keeper

Defense-in-Depth: Top 5 Layers of Security Against

In the fight against USB-related threats, IT security professionals are increasingly adopting a defense-in-depth approach. This strategy involves

REDUCING THE CYBERSECURITY RISKS OF PORTABLE

Organizations can reduce the cybersecurity risks of USB device use with secure physical and logical controls on the access, storage, and usage of USB devices, and training on how to utilize USB

Transforming secure access with Zscaler Private

Zscaler Private Access (ZPA) offers a modern approach by providing secure access to private applications without exposing networks to the public Internet.

FBI Seizes NetNut Proxy Platform, Popa Botnet – Krebs on Security

On June 19, three different security firms issued similar findings: That NetNut is a residential proxy network which populates a botnet called Popa, and distributes software for devices

Network Security in Schools 2026: The Definitive Guide for K–12 ...

As security risks intensify, districts can take these steps to secure networks, devices and data without overextending resources.

What is Cyber Security? A Complete Beginner''s Guide

Cyber security is the protection of internet-connected devices and services from various attacks. It is the practice of safeguarding systems,

Free Virtual USB: Share & Access USB Devices over Network

Unleash your USB devices with our free USB over Network software! Access any USB peripheral – from printers and webcams to specialized hardware and security dongles – from

Overview of Microsoft Defender for Endpoint Plan 1

Get started using the Microsoft Defender portal, where you can view incidents and alerts, manage devices, and use reports about detected threats

Contact Us

For more information, pricing, or custom solutions, please contact us:

Website: https://www.mr-security.co.za
Email: info@mr-security.co.za
Phone: +33 1 45 23 67 81
Address: 10 Rue de la Paix, 75002 Paris, France

This document is for informational purposes only. Specifications subject to change without notice.