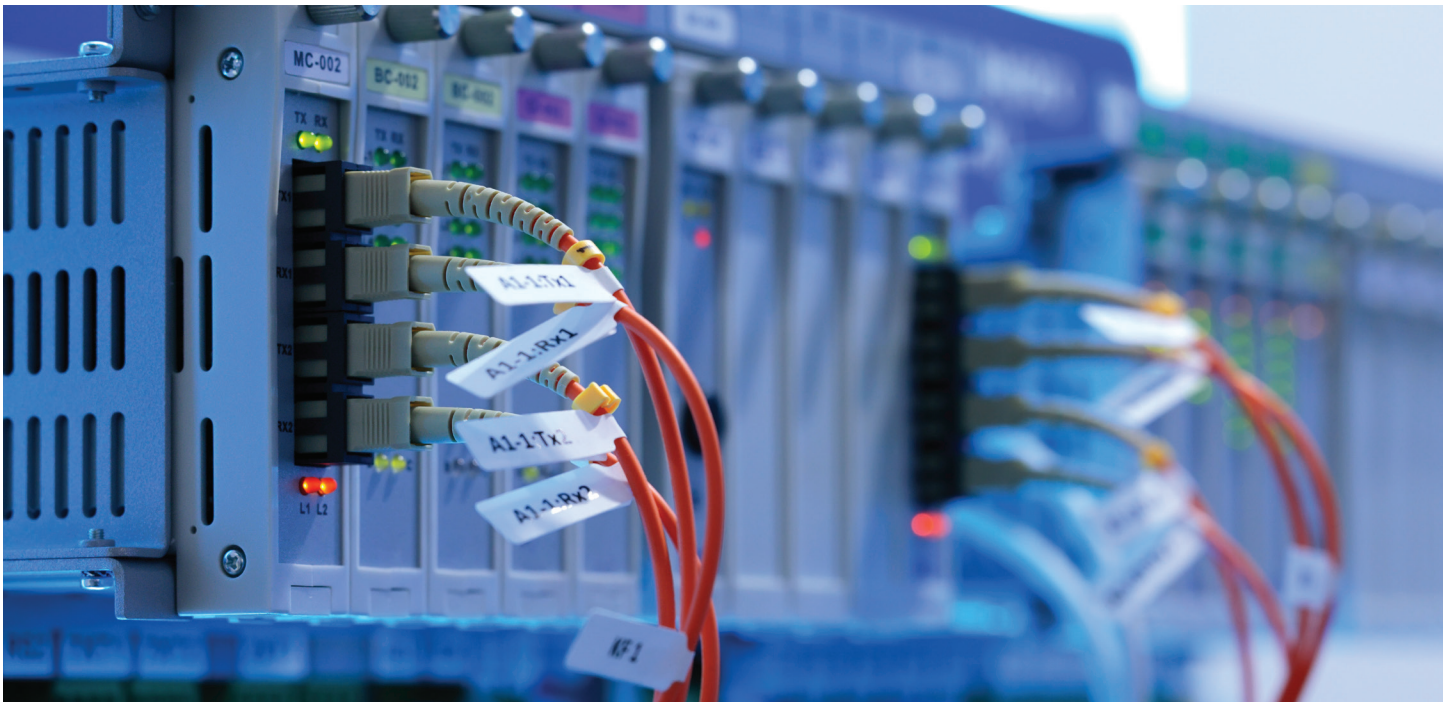


CLAROTY

Game Over for Consumer Tech Risk in Critical Infrastructure

Claroty found a consequential number of consumer devices on production OT, healthcare, and commercial networks. Each of these assets presents attackers with a viable pathway onto the network.



Introduction

A programmable logic controller (PLC) is the hub of an industrial network. It communicates with sensors, actuators, and other smart instruments that ensure production lines remain reliable and available. PLCs also sync with human-machine interfaces (HMI) and supervisory control and data acquisition (SCADA) systems that connect humans to physical processes. It's also possible for PLCs to interact with other PLCs to coordinate production line actions, edge gateways in order to send field data to the cloud for processing, or enterprise systems for inventory tracking and scheduling.

Nowhere in that chain should there also be a Nintendo Switch or a Tesla Model 3.

New Claroty research analyzing more than 45 million devices, however, has uncovered a consequential number of gaming consoles, entertainment devices, and connected cars on industrial and healthcare networks. While there are legitimate use cases where a gaming console could be found on a network (for example, a children's hospital where patients may request to play video games), time after time we discovered these types of assets right alongside PLCs, patient monitors, and other devices on company networks.

Nintendo is the canary. Production and healthcare networks are the coal mine.

Despite decades of caution from researchers and security companies, and millions of dollars invested in technology to protect these critical networks, there remain critical failures in virtual network segmentation, continuous threat detection, remote access, and overall governance that still allow for consumer devices to co-exist inside critical operational environments.

Our research enumerates the devices we discovered in our dataset, and how they can provide a pathway for an attacker to compromise industrial devices and cause intolerable disruptions and negatively impact businesses across industries.

©Copyright Claroty. All rights reserved

Key Findings

The dataset for this report includes:

45 million+
assets in our dataset for this research

30,000+
critical infrastructure locations

25%
of the dataset is made up of OT and medical devices (with IT making up the rest)

This research focuses on devices that should never be networked with mission critical devices. Critical infrastructure will be more secure when these networks are free from superfluous and needless equipment. In the study, Claroty found:

16,745
gaming consoles on OT and healthcare networks

44,059
smart home and entertainment devices on OT networks

4,915
connected vehicles on OT networks

Methodology

Claroty analyzed device inventories across critical infrastructure networks to identify the presence of inappropriate devices—those that have no legitimate operational purpose in industrial, healthcare, or commercial environments. The presence of consumer electronics, personal vehicles, and entertainment devices serves as a proxy for network health and segmentation effectiveness.

©Copyright Claroty. All rights reserved

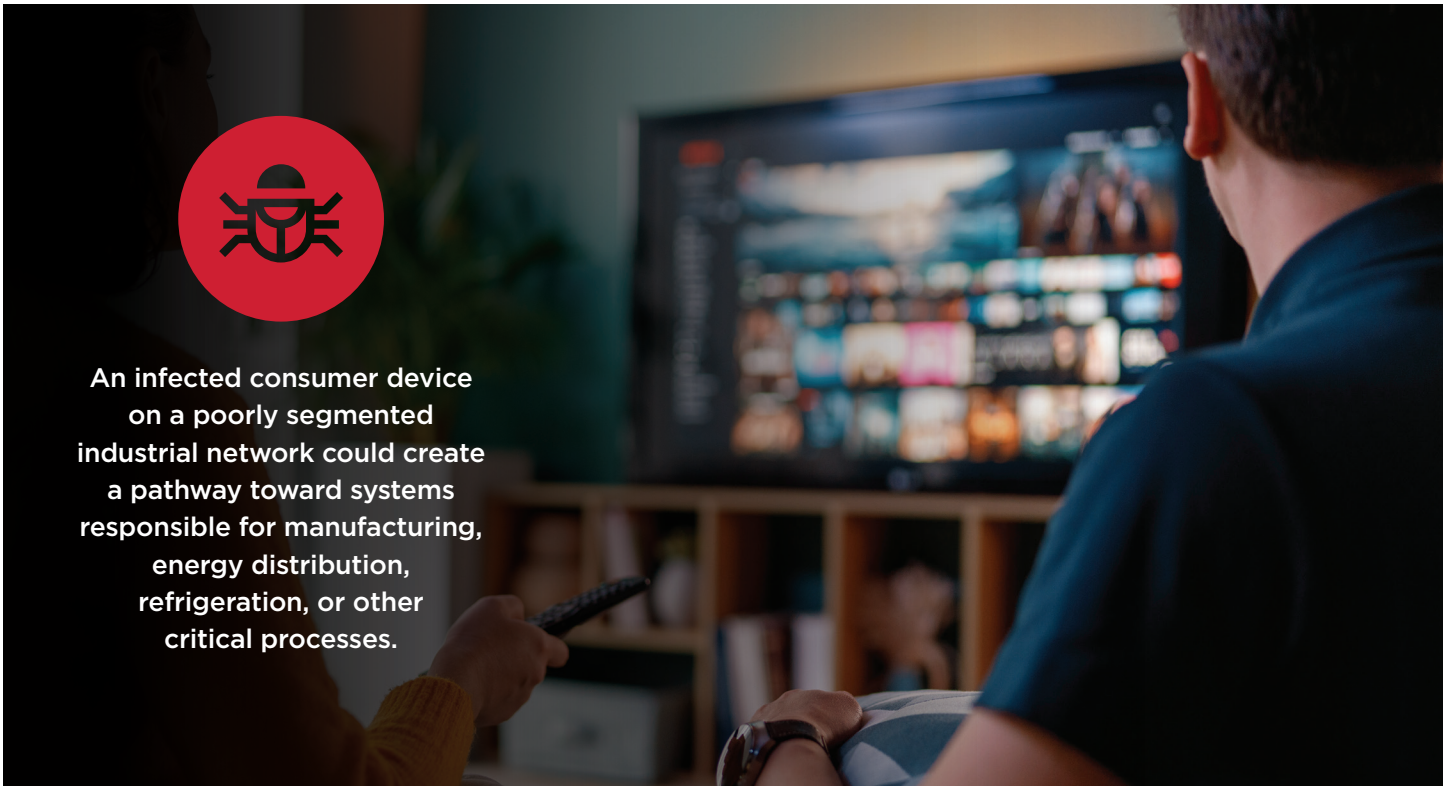
Critical Risk Devices: A Legacy Problem

Industrial, healthcare, and commercial networks were designed around predictability. Operators, engineers, and medical staff operate under an umbrella of safety and availability with the goal of keeping production lines and patient care moving forward uninterrupted. Connectivity has blurred some lines between operations and IT, and non-industrial or non-healthcare devices can introduce unexpected cybersecurity risks that threaten the expected reliability of these sensitive networks.

Claroty's research has uncovered a consequential number of consumer technology devices such as smart home and entertainment systems, gaming consoles, and cars connected to sensitive operations networks. These devices may appear harmless, but when they share network infrastructure with industrial control systems, building management systems, and medical devices, they can become an entry point for attackers seeking to disrupt production, compromise critical processes, or threaten operational resilience.

Consumer devices are rarely designed to meet the security, reliability, and lifecycle requirements of operational environments. Software and firmware vulnerabilities are present on these devices, many of which are not secure by design or default. Many have insecure communications or must reach out to the public internet to a cloud service that is outside a factory's or hospital's control. Most organizations will not have visibility into these rogue third parties' security posture and the risks they may introduce to production and medical networks.

The fundamental problem is these devices introduce unmanaged assets, unexpected communications, and potential vulnerabilities into an environment where a compromise can have physical consequences.



©Copyright Claroty. All rights reserved

Top 10 Vendors by Critical Risk Device Count:

Of the more than 45 million devices analyzed, over 450,000 (approximately 3.5%) are classified as having a "critical risk" due to known vulnerabilities, outdated firmware, or lack of security updates.

Vendor	Critical Risk Devices
Apple	155,972
Rockwell Automation	132,868
Axis Communications	40,706
Schneider Electric	28,568
Zebra Technologies	19,068
Siemens	13,420
Hanwha Techwin	12,775
Fanuc Robotics	7,332
Honeywell	4,335
GE	4,326

This dataset for this report spans:



PCs and tablets



Automation equipment (PLCs, controllers, HMIs)



Industrial printers



IP cameras and surveillance systems



Robotics and manufacturing systems

©Copyright Claroty. All rights reserved

Risk Scores

Device risk is not only determined by a CVE or CVSS score; multiple factors make up scoring criteria, including:

1. **Vulnerabilities:** Presence of confirmed or potentially relevant CVEs, especially those with high CVSS scores, known exploits (CISA's Known Exploited Vulnerabilities database), or high Exploit Prediction Scoring System (EPSS) scores

2. **Internet Exposure:** Whether the device communicates with the internet, especially inbound/server communication

3. **Operating System Risk:** Outdated, unsupported, or end-of-life operating systems

4. **Security Controls:** Lack of endpoint security, unmanaged devices, or missing security updates

5. **Device Criticality:** The operational importance and potential impact of compromise

These represent the entire OT stack—from cloud services to keyboards, IoT sensors to PLCs. Our research reveals further issues:

Attackers Thrive on Unmanaged Assets, Connections

As we've seen with recent attacks on supermarkets in Europe, for example, attackers are accessing networks via unsecured internet-facing assets. In the supermarket attacks, attackers were able to manipulate temperature controls and defrost food, causing millions in lost stock and revenue. Once a device is compromised, its position on the network becomes important.

If it can communicate freely with other systems, an attacker may attempt to discover reachable assets, abuse improperly configured access permissions, steal credentials, or exploit vulnerabilities in adjacent computers and servers. A compromised device can also provide a foothold for further reconnaissance and lateral movement.

The greatest danger emerges when connectivity between IT and OT networks is insufficiently controlled. Determined attackers looking to manipulate or disrupt operations can expose weak or non-existent segmentation, excessive permissions, shared credentials, or unmonitored connections to move deeper onto the network. An innocuous connection from a connected automobile on the same network as OT, IoT, and BMS assets can provide a pathway to access those sensitive devices. If the pathway is unknown, the risk is substantial.

©Copyright Claroty. All rights reserved

In an age where artificial intelligence is lowering the barrier to entry even further for threat actors to not only carry out reconnaissance, but also to scan internet-facing assets for known vulnerabilities, this is a real problem for environments steeped in legacy systems that cannot be taken off the network without fear of further disruption.

The problem for OT, commercial, and healthcare networks is that they may operate outside IT's control, with individual sites maintaining autonomy over their operations. This decentralized approach has created an architecture characterized by:

- **Perimeter-focused security:** One large boundary firewall with minimal internal controls
- **Limited network segmentation:** Few guest networks or isolated VLANs for non-critical devices
- **Minimal access controls:** Low barriers to connecting devices to corporate OT networks
- **Mixed-use infrastructure:** Consumer devices sharing network space with HMIs, PLCs, MRIs, and cooling systems

We not only found tens of thousands of consumer devices on OT networks, but also exploitable CVEs on the consoles, entertainment devices, and cars that could provide determined attackers with a foothold on the network.

Let's look at some of the numbers per device category:



3.5% of critical infrastructure carries critical risk vulnerabilities

Cars, watches, and gaming consoles operate on neighboring VLANs to turbine controls, MRI machines, and physical security systems

The distance between normal operations and catastrophic failure is often just a VLAN misconfiguration

©Copyright Claroty. All rights reserved



Gaming Consoles

The presence of gaming consoles in hospitals has to be evaluated differently than from a strict industrial setting because there is a legitimate (and humane) use for them in care clinics, although they should be architected to be on the correct guest or internet-of-things (IoT) networks.

In healthcare, gaming consoles were largely concentrated in children's hospitals where they serve legitimate patient needs.

Healthcare

14,624
gaming consoles discovered

13,939 (95.3%)
connected to production networks instead of guest or IoT networks or VLANs

691 (4.7%)
categorized as high risk

In industrial and commercial applications, the presence of gaming systems is considerably smaller, but with zero viable business use, their presence is often more troubling.

Industrial

963
gaming consoles discovered on production OT networks

862 (89.5%)
connected to production networks instead of guest or IoT networks or VLANs

30 (3.1%)
categorized as high risk

©Copyright Claroty. All rights reserved

Smart Home and Entertainment Devices

Our research uncovered thousands of consumer IoT devices operating on production OT networks—none of which serve legitimate business cases in critical infrastructure settings.

2,670
Sonos media players

23,424
Roku streaming sticks

37,314
Smart watches

In contrast to gaming systems, these devices are more often on the guest network.

Device	Total Devices	Total on Guest Network	% on Guest Network
Roku	23,424	17,454	70.5%
Smart watches	37,314	27,111	72.7%
Sonos	2,670	173	6.5%

This contrast represents an interesting behavior bias. When connecting a device with limited business justification, they are more likely to use the guest network.



©Copyright Claroty. All rights reserved



Connected Vehicles

Modern vehicles require Wi-Fi connectivity for software updates and patches, leading employees to connect personal vehicles to corporate networks after their commute.

Vendor	Device Count
Tesla	3,425
Ford Motor Company	984
Texas Instruments	775
Honda	390
Hyundai Motor	79

Six critical CVEs on Tesla Model 3s were discovered, including dangerous remote code execution and buffer overflow vulnerabilities

121 security issues were linked to Ford F-150 trucks, the highest number linked to connected vehicles in our data set.

Almost none of the vehicles were properly isolated onto guest networks.

©Copyright Claroty. All rights reserved

Root Causes Enabling This Security Gap

Segmentation is the go-to control for OT, healthcare, and commercial networks where downtime is intolerable and organizations have long windows of exposure to security issues. Those issues include KEVs, weak system or network configurations, poorly secure remote access, or unsupported legacy technology still vital to core production lines or patient care.

Remediation for each of these problem areas requires scheduled downtime, in addition to regression testing of firmware and software updates, and close monitoring of updates in production in case of disruptive faults caused by new software or firmware.

Critical factors enabling this security gap include:

Decentralized Management

Individual site autonomy prevents consistent security policy enforcement because it allows separate locations to create, modify, or ignore security rules independently.

When local branches or departments have the authority to manage their own networks, systems, and access controls, this negates the advantages that uniform security postures across the entire organization present.

The after-effect includes inconsistent exposure management where some updates are delayed, creating excessive windows of time where organizations are susceptible to exploits of known vulnerabilities or weak configurations. It also can manifest in diverse security tools that add complexity to overall exposure management, and further fragment security policies around access controls, for example.

Autonomous sites may also lead to blind spots that impact threat detection in a centralized security operations center. OT, healthcare, and commercial entities are then particularly at risk because these autonomously managed sites may be the easiest to compromise and provide attackers the foothold they seek on a network.



©Copyright Claroty. All rights reserved

Legacy Architectures

Networks designed decades ago with perimeter-only security models fail in today's connected architectures. Industrial networks, for example, are no longer flat architectures where every device can see and communicate with each other. This enables rapid lateral movement and threatens the integrity of production lines and overall uptime and availability.

Digital transformation fundamentally changed data flows within industrial environments. Where hierarchical communications between layers once dominated, hyper-convergence now rules. Systems communicate across layers to enterprise and cloud environments as easily as to global supply chain partners. This lateral communication directly contradicts the Purdue Model's vertical, hierarchical structure.

Unlike IT systems, which prioritize data confidentiality and tolerate planned downtime, OT systems prioritize availability and safety, running continuously for months without interruption. This operational divide creates friction when applying traditional security frameworks across converged environments. The same applies to healthcare networks where patient safety is paramount, and commercial organizations where supply chains and production must avoid disruption at all costs.

Slow Modernization

Legacy technical debt is a big impediment to modernizing today's production networks. Not only are these assets no longer supported by their respective vendors, but often they're also still a critical part of process success and patient care. Ripping and replacing this technology is slow and expensive.

Organizations must first consider not only the technical debt at play but also the dependencies between these assets and the rest of the production or patient networks. Critical traffic cannot be blocked or disrupted because of a change. In addition to dependencies, there are other considerations such as custom software and configurations in place that could also be as disruptive as a cyberattack if changes are not made carefully.

Modernization also requires expensive hardware and software upgrades and specialized expertise that doesn't come cheaply. Consultants and engineers will be needed to architect and implement modern upgrades to networks, and undoubtedly, new investments will be required to protect OT, healthcare, and commercial networks from current threats.

Recommendations

Our critical infrastructure will only be as secure as the number of Nintendo Switches we allow on the network.

The security posture of hospitals, power plants, manufacturing facilities, and water treatment systems is directly correlated to the discipline with which we enforce network segmentation.

Every Nintendo console, Tesla, and Apple Watch connected to production networks represents:

- An expanded attack surface
- A potential pivot point for lateral movement
- A blind spot in security monitoring
- A failure of segmentation policy

©Copyright Claroty. All rights reserved

Path Forward: Achieving Nintendo = Zero

To secure critical infrastructure, organizations must:

- Implement strict network segmentation: Separate guest, IoT, and production networks with enforced policies
- Deploy continuous asset discovery: Maintain real-time visibility into all connected devices
- Enforce secure access requirements: Prevent unauthorized devices from accessing production networks
- Accelerate modernization efforts: Replace legacy systems and redesign network architectures
- Establish governance frameworks: Centralize security policy while respecting operational autonomy

The goal is clear: Nintendo = Zero.

When gaming consoles, smart watches, and personal vehicles no longer share networks with critical operational technology, we will have achieved much of the segmentation necessary to protect our most vital systems. Until then, the chaos is just one misconfigured VLAN away.

About Claroty

Claroty empowers organizations to protect the mission-critical infrastructure that underpins modern life. The AI-powered Claroty Platform serves as the single source of operational truth, providing the deepest visibility and broadest protection across cyber-physical systems (CPS), leveraging five core solutions: asset inventory, exposure management, network protection, secure access, and threat detection. Claroty helps organizations operationalize CPS protection through a programmatic approach designed to reduce risk, maintain operational integrity, and meet compliance–whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.

©Copyright Claroty. All rights reserved