insight.tech POWERING IoT AND EMBEDDED INNOVATION

Avoid VPNs with Global Access Networks for IoT Control

The underlying network is fundamental to a secure remote device management solution, and the digital safety of any IoT device deployment for that matter.

Here, enterprises have traditionally selected one of two options:

- **Virtual Private Networks (VPNs)**, which create secure, encrypted tunnels through less secure public networks—reducing the chance of hacking or data leaks.
- **On-Premises Networks** that offer robust security by completely isolating systems and their data from less-trusted connections.

But both VPNs and on-premises networks have some notable disadvantages—starting with complexity.

Depending on the environment and use case, each implementation can require a number of different protocols, types of equipment, and service providers, leading to interoperability challenges **(Figure 1)**. Performance and latency can also be issues, especially for VPNs.

Cost is another drawback. The hardware, software, and services of VPNs or on-premises networks can have a high price tag. And then there's the IT personnel time and resources to manage this network infrastructure that includes:

- Installing certificates
- Configuring routers and firewalls
- Setting up fixed IP addresses
- Working with corporate databases

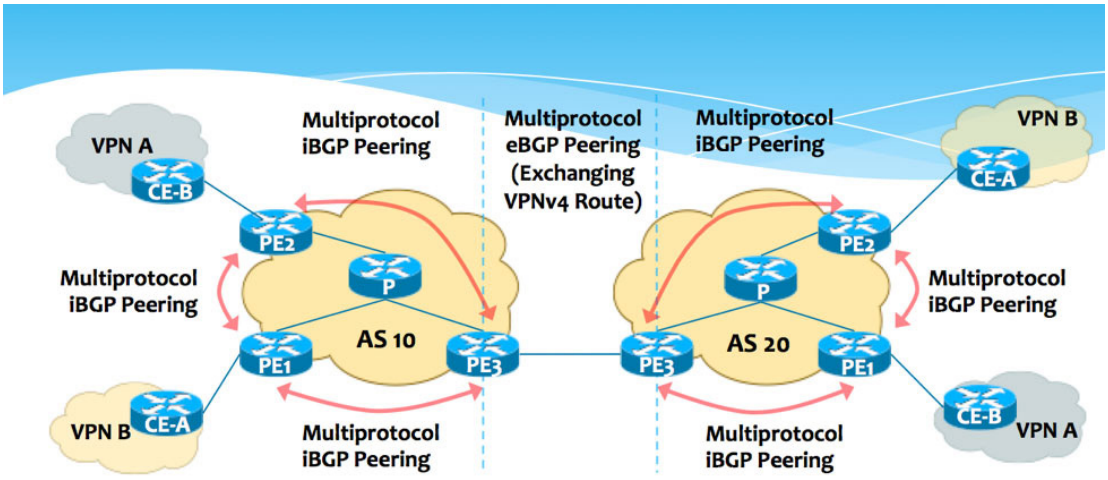

Figure 1. VPNs can increase deployment cost and complexity. (Source: OrhanErgun).

An effective remote device management solution must be compatible with standard network infrastructures, and also needs to account for security gaps between people, processes, and systems.

For commercial use cases like retail digital signage, this translates into a platform that is device agnostic, built from a foundation of robust security, and operates in real time.

Offloading Cost and Complexity

As deployments grow, VPNs and on-premises networks can quickly become too complex or too expensive. To support secure remote device management, it's clear that the industry needs an alternative solution.

TeamViewer GmbH is one company that uniquely addresses this need. It owns, manages, and operates a Global Access Network of more than 100 worldwide networking hubs.

This infrastructure allows companies to connect systems quickly and scale deployments efficiently.It also enables secure device, application, service, and data access from virtually anywhere.

The TeamViewer IoT secure remote monitoring and management solution is designed to reduce the cost and complexity of large-scale IoT systems **(Figure 2)**.

Real-Time Monitoring, Management, and Control that Puts Security First

The TeamViewer IoT platform is deployed over the company's Global Access Network, and supports features such as comprehensive activity logging, thresholding, and automated alerts in a user-friendly cloud dashboard.

But the multilayered security architecture sets the solution apart from other device monitoring and management

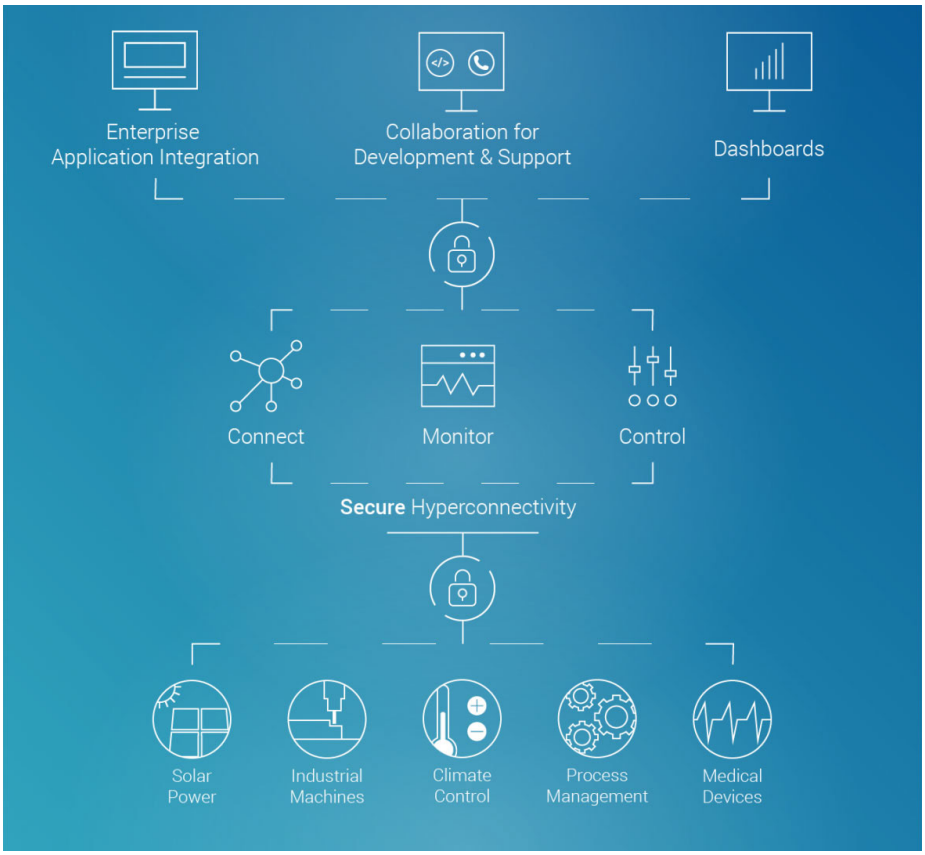

Figure 2. The TeamViewer IoT platform remotely monitors and manages IoT devices. (Source: TeamViewer GmbH)

platforms. This starts with an ISO 27001-certified data center backbone, which includes account and management console-level protections—preventing unauthorized access and tampering **(Figure 3)**.

From there, all data transmissions are secured using a 2048-bit RSA public-private key exchange and 256-bit AES encryption. The digital identity of clients exchanging data on the network is verified using VeriSign certificates.

Beyond data traffic, the platform enables application-level security in the form of blacklisting and whitelisting, two-factor authentication, and access control for incoming/outgoing data.

This layered security architecture provides the foundation for security features unique to the TeamViewer IoT platform. For example, "Enforced Recording" automatically captures all remote session activity and cannot be paused or stopped.

Not only does this assist with troubleshooting and system analysis, it also helps identify suspicious activity occurring anywhere on the network.

These features integrate seamlessly with existing deployments through a capability called "Silent Rollout," which allows for software installation, updates, and functional support without interrupting system operation. As a result, operators can connect to and control IoT devices in seconds over an encrypted end-to-end connection **(Figure 4)**.

Secure Retail Device Management In Action: A Philips Case Study

The TeamViewer IoT platform is deployed in industries such as manufacturing, agriculture, building automation, and retail. In fact, Philips has installed the TeamViewer IoT application on its electronic displays to help improve the smart retail shopping experience for operators and consumers.

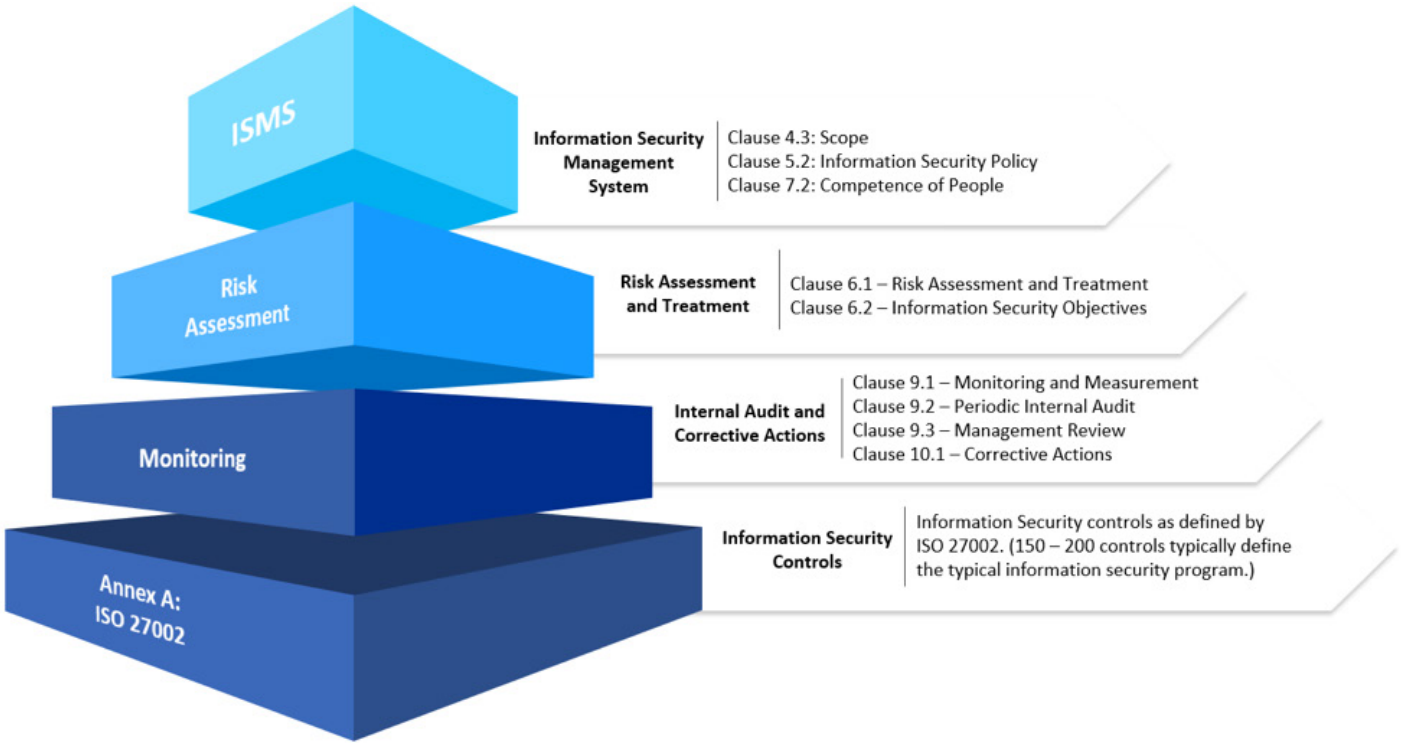

Figure 3. The TeamViewer IoT platform is ISO 27001-certified. (Source: risk3sixty)

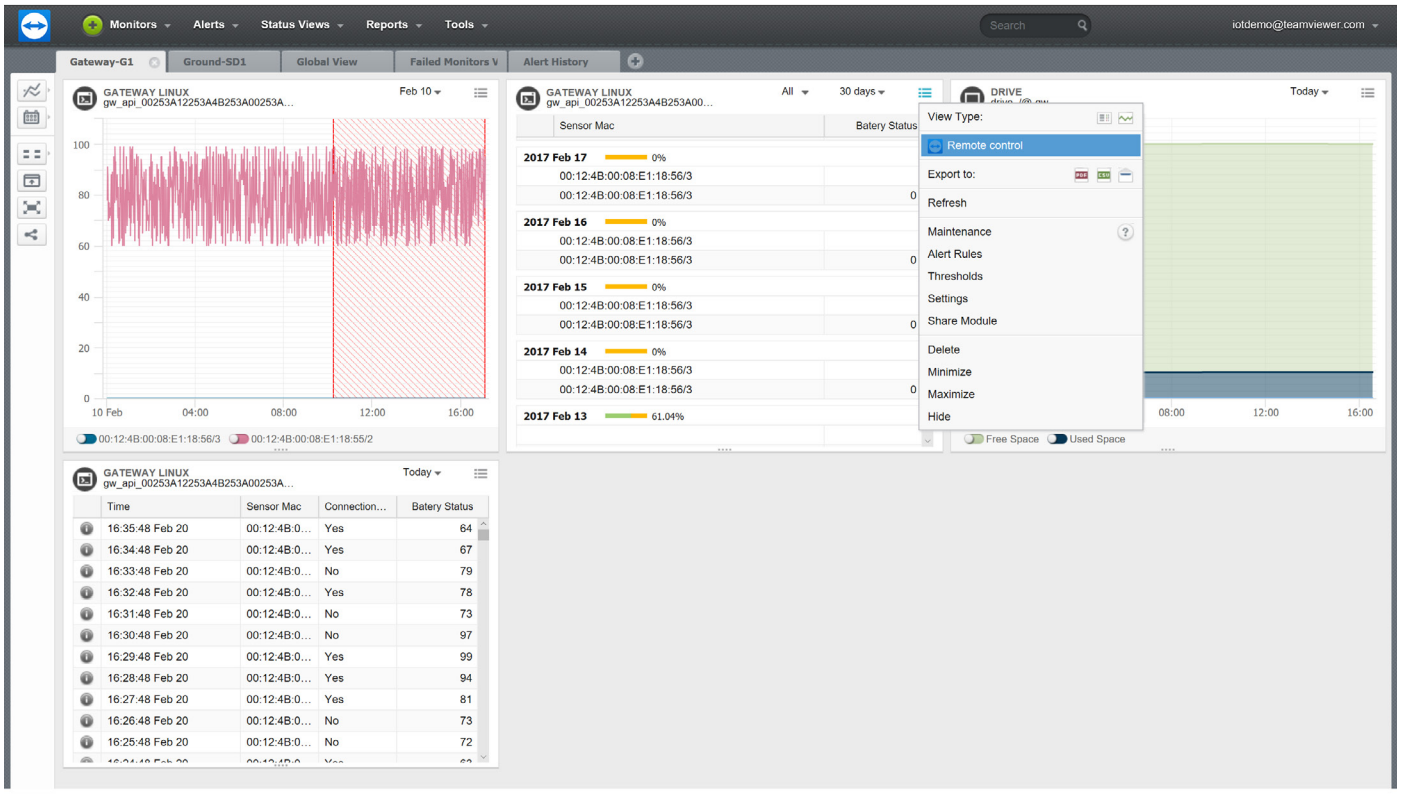

Figure 4. A cloud-based monitoring and management dashboard allows users to visualize device data, and connect to and control systems over an encrypted channel. (Source: TeamViewer GmbH)

As a major global OEM with multinational clientele, Philips needed a way for its commercial customers to monitor and manage Android-based digital displays at any time, from anywhere. The solution had to be granular enough so that operators could view the performance and activity of individual retail displays remotely, and also change their content and settings.

With the TeamViewer IoT platform, Philips' retail customers were able to turn shopping into a personalized customer experience.

On lighter-traffic days, consumer information can be combined with ad campaigns that target a specific demographic in a specific store or region. On busier days, multiple displays can be linked into large video walls that project the brand's image.

The platform's monitoring and control functionality also helps Philips digital signage operators to capitalize on intelligent sensors and big data analytics. Point of Sale (POS) device activity, product and store performance, as well as customer metrics can be collected and tracked-turning this remote monitoring and management into a competitive advantage.

Since much of the data captured and transported across the TeamViewer network is proprietary or sensitive, these analytics capabilities would be impossible without a robust multilayered security architecture.

Intel® Next Unit Of Computing (Intel® NUC) Onramps Scalable Remote Monitoring and Management

Another advantage of the TeamViewer IoT platform in retail deployments is that all digital signage media collateral is hosted in the data center, not on the endpoint. Therefore, companies looking to take advantage of the remote

monitoring, management, and insights can leverage low-cost endpoint infrastructure that's easy to scale.

For example, the Intel® Next Unit of Computing (Intel® NUC) is an entry-level digital signage platform that supports 4K resolution, multiple displays, encryption, and remote management via platforms like TeamViewer IoT **(Figure 5)**.

With a customizable board and chassis, the NUC platform can be configured to accept a variety of processor, memory, and operating system (OS) configurations. Combining it with TeamViewer IoT agent, which is both device agnostic and supports both Windows and Linux, makes for an extremely flexible solution.

Manage IoT Devices, Not Infrastructure

TeamViewer IoT illustrates the widespread need for IoT device management solutions that are scalable, reliable, and secure.

Because it is built on the secure foundation of the company's Global Access Network, operators in these industries can offload IT infrastructure headaches and focus on cutting product deployment times, analyzing system data, and developing new applications. The future of IoT devices is about managing devices and data, not the enterprise infrastructure.

Figure 5. The Intel® Next Unit of Computing (Intel® NUC) is a compact, customizable digital signage solution that supports multiple configurations. (Source: Intel®)