



IoT Today: Building a Secure, Scalable Wireless WAN for Devices

Reduce security risks across every WAN connection with a zero trust network designed for enterprise IoT

'Things' are getting serious

Data collection, customer service, and remote monitoring and control are just a few factors driving the growth of the Internet of Things (IoT). The rapid pace of IoT device deployment is increasing network sprawl and expanding an organization's attack surface. From sales and customer service to the heart of the factory or warehouse and even into customer locations, many "things" are positioned far outside any reasonable network perimeter. And these things often must be managed and monitored remotely by third-party contractors and service technicians, which increases security risks.

"Things" are not the same as users and require an updated security approach. The growth in IoT hacks, security intrusions, and data breaches has spawned many overly complex security offerings. But most current security models require the device to run a browser or an agent, which doesn't translate well to IoT devices. An up-to-date security foundation is needed — one that enhances, not degrades, IoT performance and potential based on zero trust.

Starting from zero (trust)

“Trust no one” is more than just a movie cliché. As security becomes the top priority for IoT deployments, zero trust networking steps in as the ideal approach, removing any implicit trust and continuously monitoring and validating connections explicitly allowed through policy.

Many IoT intrusions begin with a hacker identifying and penetrating vulnerable devices. From there, they can move laterally throughout the network and either install malware or exfiltrate valuable data. A zero trust security architecture takes the lead role in reducing these risks by hiding IP addresses, making devices undiscoverable on the network. Cloaking the devices and hiding their IP addresses makes them undiscoverable on the network and significantly shrinks the attack surface.



An effective zero trust network evaluates network traffic on a per-session basis using adaptive verification policies. This takes different variables into account, including a device’s physical location, session source and destination, user identity (if any), and established usage patterns. By creating a secure tunnel between the source device and target application, zero trust restricts lateral movement and precludes bad actors from hijacking the session, while intrusion detection and prevention systems (IDS/IPS) continuously verify the connection.

Smart buildings have hundreds or thousands of IoT devices, monitoring and controlling lights, HVAC, energy usage, and security. Many of these systems provide different levels of access to building managers, tenants, and third-party maintenance or service contractors. By restricting network access to valid sources and destinations and continuously validating the packets, zero trust IoT routers ensure authorized users have access only to the things they need to do their jobs and nothing else.

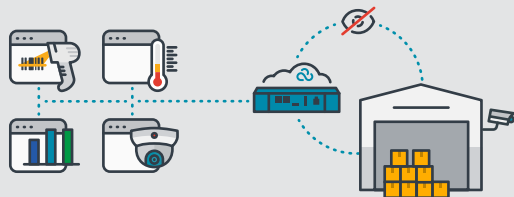
Adding security functions to every IoT router increases costs and makes managing the network more complex. The solution? A hybrid mesh firewall, which utilizes on-premises, cloud-based, and on-router capabilities to deliver optimal performance, along with enhanced security. Service gateway functions offload security processing so that small IoT routers can deliver extensive security. Integrated IDS/IPS continuously compares the zero trust connections against a dynamic set of signatures, watching for any signs of malicious activity and ensuring authorized zero trust connections are not hijacked.

With centralized dashboards, enterprises can deploy and manage multiple security functions, including hidden micronetworks, segmentation, encryption, and web filters across numerous locations and device types. Similarly, a single policy engine supporting fine-grained policies enforces security across the entire network. Integrating these functions into a single pane of glass provides a streamlined experience from the edge to the core, simplifying operations and accelerating time-to-service.

Flexible protection at the gateway

Many modern security methods, such as biometrics, two-factor authentication, and awareness training, are designed for users, not IoT devices. Too many of these devices still have their default passwords, are not fully managed by IT staff, and are regularly accessed by outside suppliers or customers. So, security for “things” falls on the next node in the network: the IoT router or gateway.

Advanced IoT networking endpoints offer a wide range of purpose-built hardware for various applications and locations. Multiple connectivity options, including 5G and 4G LTE cellular, Wi-Fi, Bluetooth®, and Gigabit Ethernet, enable placement of the router as close to the IoT devices as possible, limiting the area of physical vulnerability. Ruggedized models provide options for harsher environments, including ingress protection ratings for extreme temperatures and vibration, so IoT networks can be protected no matter where they reside.



IoT devices are being used in warehouses and manufacturing facilities to monitor equipment status, production rates, temperature and humidity, video surveillance, and a host of other important inputs. By connecting these devices to a semi-ruggedized IoT router, they are immediately hidden on micronetworks and protected from discovery. Zero trust networking limits communication to and from specified resources and applications, and controlled authorization provides specific, limited access for legitimate third parties.

Additional features and external integration points on these models support almost any use case:

- Active GNSS/GPS capabilities enable location information and asset tracking.
- Locking USB adapters provide connections to serial-based assets.
- External general-purpose input/output (GPIO) pins enable monitoring and control of external sensors and actuators for local and physical security awareness and alerting, such as door open or closed, water leak detected, or temperature limit exceeded.

Advanced IoT routers provide software and hardware security and flexibility. Available APIs provide access to alerts, device health, cellular strength and connection quality, and location information for integration with third-party management tools.

SDKs enable lightweight Python or Docker container-based applications to run securely at the edge. Container orchestration facilitates large-scale deployments with a single pane of glass for monitoring and management. Third-party integrations and technology partnerships, such as Amazon AWS IoT Greengrass and Microsoft Azure IoT Central, bring additional functionality to IoT devices, including cloud processing to reduce hardware requirements at the edge. Even IoT devices connected to a small router can have access to full modern security services.

Reliable protection with cellular

Cellular and wide-area networks (WANs) form another vital security layer for IoT devices, which are often deployed far from wires and traditional networks. Connection issues are a common networking concern — even more so for security-related IoT devices, such as building entry systems or video surveillance. Routers explicitly designed for IoT and cellular or wireless WAN networks include intelligent software and management features to deliver predictable and sustained connectivity. Features include:

- Software-driven and remotely upgradeable modems ensure that IoT routers stay up-to-date with patches and enhancements.
- Centralized dashboards and comprehensive visual representations of cellular health and security are critical to maintaining visibility over these widely distributed network assets.
- Advanced systems translate complex signal strength and quality values into intuitive graphical representations.
- Efficient cellular-aware management protocols, adaptive compression, and real-time event triggers keep administrative traffic to a minimum.



Delivering acceptable quality of service (QoS) and quality of experience (QoE) are just as important for devices as they are for people. Auto-connection and broad carrier certifications help routers establish faster and more persistent connections. Additionally, continuous integrity testing from source to destination enables the router to dynamically adjust operating parameters to ensure optimal performance. By monitoring higher-level network issues, the router can trigger a graceful link failover before the remote things are even aware of a problem, thus improving uptime.


Video surveillance, building entry, and other security systems are dependent on their upstream link. Traffic optimization and application-aware networking capabilities keep these data streams flowing. For example, security teams may want to shift to live video feeds during a suspected security event. Less critical data can then be dropped or steered to alternative links, and forward error correction can mitigate the impact of a lost cellular connection. Two links can also be bonded into one to aggregate bandwidth for on-site video.

Traffic optimization is another potential job for an IoT network. Application-aware settings help the router steer traffic to the most appropriate link and maintain the best possible connection. Load balancing spreads traffic across multiple links, or intelligent bonding brings two links together for better reliability, control, and aggregate bandwidth for high-value IoT applications.

Scalable protection for lean IT

Network security is only as good as the team configuring and managing it. Supporting thousands or tens of thousands of remote things is a security challenge for any organization. With many adopting a lean IT model of technology operations that emphasizes efficient processes and accelerating workflows, the challenge only grows. Zero-touch deployment, scalable management tools, and location services help lean IT teams efficiently and securely deploy and manage large IoT deployments without overextending resources.

Zero-touch deployment provides a solid foundation for zero trust IoT networks. The ability to send IoT routers to remote locations with pre-provisioned firmware and preconfigured settings reduces both the deployment time and the risk of configuration errors. Bulk maintenance and operational functions keep remote routers up-to-date with both software and configuration parameters. This means that lean IT teams can add endpoints with minimal touchpoints and without travel or truck rolls.



Zero trust networks are ideal for kiosks, digital signage, and self-service systems deployed at the network edge and require secure and scalable connectivity. Zero-touch deployment gets these devices into the field quickly with consistent configurations and continuous software updates. Centralized cloud management allows the IT team keep an eye on everything, troubleshoot issues in real-time, and even track router locations via GPS/GNSS.



Cloud-based management is another essential tool to maintain visibility and control over these widely distributed network assets. This enables companies to:

- Monitor and manage any number of wireless WAN devices from a single pane of glass
- Enforce consistent and fine-grained security policies from a single policy engine
- Provide filters and drill-down capabilities to make it easier to diagnose localized issues

Combining cellular coverage maps with device locations and live views of signal strength is another helpful feature that improves router placement and facilitates network planning. Details about remote router locations boosts confidence knowing they are installed where they should be and have not been stolen or hijacked. Full-stack analytics optimize application traffic and facilitate diagnostics and troubleshooting.

Learn more at [cradlepoint.com](https://www.cradlepoint.com)