

OpenBlue



A revolution in secure networking

OpenBlue Airwall

Protection you can trust

OpenBlue Airwall makes things on a network invisible and protects against cyber-attacks. This comprehensive solution is exceptionally effective at protecting critical physical infrastructure, while still allowing secure remote access.

Overview

Securing a company's distributed network is incredibly expensive and difficult to scale. Attacks and breaches present massive risks to your company's reputation. Managing your company's IoT deployments and network access demands is only getting more complex as time goes on.

Solution providers tell you:

1. Visibility is security
2. Attacks are inevitable
3. Connect first, secure later

Providers will say you need more firewalls, VPNs, VLANs, ACLs and SSH keys. But how can you be sure you're truly protected?

There's a lot of information to absorb, but critical infrastructure and data are at risk if you don't make the right decision.

A better way to secure your network

OpenBlue Airwall enables secure access and total invisibility at any scale, across any network.

OpenBlue Airwall secures every endpoint in your network, with true micro-segmentation and secure remote access. You can secure your local data center and your global infrastructure.

OpenBlue Airwall works with your existing network investments, so no need for rip-and-replace or forklift upgrades. Network-based attacks are a thing of the past and managing your network is no longer complex or costly.

OpenBlue Airwall delivers defense-in-depth

1. Zero trust network access (ZTNA)
2. Software-defined perimeter (SDP)
3. Micro-segmentation for every endpoint
4. Software-defined network (SDN)
5. Multi-factor authentication (MFA)
6. Lateral movement eliminated

What is OpenBlue Airwall?

OpenBlue Airwall is a virtual air-gap solution that ensures your devices are completely invisible. It eliminates lateral movement from bad actors across your network. OpenBlue Airwall uses Host Identity Protocol (HIP)² to secure network communication between devices, enabling micro-segmentation and remote access at scale on any network.

Most networks are configured to use IP addresses to identify and locate devices in the network.

The security policies and access controls for this type of networking are IP-based.

When you network with OpenBlue Airwall, in contrast, devices are assigned a cryptographic identity as the sole criteria for network communications. By default, devices only communicate through the encrypted identity framework. This means devices don't even show up on a pen test.



Rather than finding a metaphorical locked door, there is no door to even knock on. From the perspective of a pen tester or bad actor, the network is essentially invisible. The architecture also makes OpenBlue Airwall incredibly easy to deploy and install because it uses the existing network. We simply deliver a different type of message.

Your network with OpenBlue Airwall

OpenBlue Airwall enables your organization to create a secure, private, easy-to-manage, mobile internet. You can define one or more overlays, with each overlay made up of virtual trust segments, and each Edge Service possessing its own unique 2048-bit cryptographic ID following the HIP RFCs. The result is a solution with military-grade encryption that can span nearly any device, network or environment.

OpenBlue Airwall is set up using an intuitive, visual and point-and-click management and orchestration engine. Unlike traditional IP networking and SDN approaches, OpenBlue Airwall requires little to no modification of the underlying network or security infrastructure. It provides a simple, policy-based configuration of devices or groups of devices that are explicitly trusted based on whitelisting. This trust, based on unique cryptographic IDs³, determines what systems or machines can initiate and establish communication before any data is exchanged.

OSI Model	Gateway	Agents
Physical – Layer 1	✓	✓
Data link – Layer 2	✓	✓
Network – Layer 3	✓	✓
Transport – Layer 4	✓	✓
Application – Layer 7	✓	✓



A secure networking architecture

An OpenBlue Airwall solution can span multiple existing VLANs, subnets and cross-networking boundaries – across data centers, public clouds, campus networks, remote locations and even unmanaged networks. You can connect or disconnect in seconds without disturbing the existing networking and security infrastructure.

OpenBlue Airwall enables a unified secure networking architecture that reduces complexity

and creates consistent application of policy across all connected systems and devices. This trust-based enforcement model is easily verified for compliance purposes.

By creating operational efficiencies, OpenBlue Airwall significantly reduces configuration errors and the resulting lateral attack vectors. Network and resource provisioning are simplified and can now be done in minutes.⁴

Devices are natively invisible to hacker reconnaissance, and protected against DDOS, MiTM attacks, IP spoofing and other types of network and transport layer attacks

Set policies across hundreds or even thousands of devices with a few clicks
– reduces complexity and overheads as you manage your network

Secure connection with devices in remote field locations with limited connectivity, to factories, offices, data centers and mobile devices

Deploy with any major cloud service and across any mainstream server, desktop or mobile operating system; as well as in front of any networked device

No need to replace existing infrastructure or add more staff; far less expensive to manage and maintain than either firewalls or VPNs

OpenBlue Airwall components

Building an OpenBlue Airwall Overlay requires that you deploy two or more OpenBlue Airwall Edge Services in a hub-and-spoke topology, mesh or both. Every endpoint in an OpenBlue Airwall Overlay knows the IP-layer state of its peers, and every peer maintains identity-based routing tables. OpenBlue Airwall's policy-based approach⁵ helps any edge service establish the most direct route to a resource within an overlay.

OpenBlue Airwall Edge Services (Gateways and Agents) provide invisibility, secure connectivity, identity-based routing and IP mobility.⁶ They enforce the Conductor's provisioning, deprovisioning and revocation of trust for any managed IP resource. Using cryptographic identity, OpenBlue Airwall Edge Services enable the mobility and migration of an IP resource anywhere within the OpenBlue Airwall Overlay, without requiring changes to the existing networking or security infrastructure. This decoupling overcomes many of the addressing, routing, mobility and failover challenges associated with traditional IP networking and SDN technologies.⁷

Our approach makes it easy to deploy and extend a unified, trust-based and encrypted network. This ease of deployment enables micro, macro and cross-region segmentation, as well as global IP mobility. Deploying and maintaining intra-cloud (region to region), cloud-to-cloud, and cloud-to-data center cryptographic, trust-based communications becomes simple, verifiable and secure.

1

Protect your things



Agent



Gateway

2

Connect your things



Relay

3

Manage your things



Conductor

Protect your things



Agents

Agents are applications installed on devices (Windows and macOS) that enable zero-trust network access (ZTNA) from anywhere in the world. By default, all communications are encrypted end-to-end and multi-factor authenticated (MFA), enforcing a software-defined perimeter (SDP) at the distributed edge.

Easily integrate user authentication with device-based authentication, overcoming much of the complexity associated with extending directory services to include device-based trust. Explicitly allow or deny any device to securely connect to a network, and also easily segment access by defining resources that a device or group of devices can access. Devices no longer have the session constraints of legacy VPNs and are not restricted by the number of concurrent client-to-resource encrypted sessions.

Deployment options:	Windows	Ubuntu
	10 and 11	20.04 LTS and 22.04 LTS
	macOS	
	13 and above	

Agent can be deployed on Windows or Linux servers.

They enable invisible server deployments. Configure server OS and/or cloud security group to disallow connections except those secured through the Agent.



Gateways

Gateways protect things downstream. They are deployed in front of devices or hosts that cannot protect themselves. Examples include legacy systems and machines, or when customers are unable to install the Agent.

Physical OpenBlue Airwall Gateways have built-in Ethernet, Wi-Fi, and Cellular (3G, 4G and 5G modems), as well as serial-over IP for the most flexible link connectivity options found in the industry. These devices can connect via fiber, wired, Wi-Fi or cellular. Configure physical devices for high availability depending on customer needs. Replace existing cellular modems, access points, VPNs and internal firewalls for significant CapEx or OpEx savings.

Virtual and cloud Gateways function in the same manner as physical Gateways. Instantly connect, protect, segment, move, failover and disconnect any private or public cloud-based workloads anywhere in the world. There is no longer a need to deploy and maintain separate networking and security policies for on-premises and cloud-based resources.

Deployment options:	Cloud	Connectivity
	Amazon Web Services	Wired
	Microsoft Azure	Cellular
		Wi-Fi
		Fiber
	Virtual	Physical
	VMWare ESXi	Airwall 75
	Microsoft HyperV	Airwall 175
		Airwall 3200
		Airwall 3033

Connect your things



Relay

Relay routes encrypt communications between all your things across all networks. Reduce network complexity and enable complete connectivity between every endpoint, without modifying the underlying network. Wherever that endpoint is and however that endpoint is online, it can be connected.

Available in cloud, virtual or hardware form factors, Relay allows the WAN and internet to behave like one network, making WAN micro-segmentation a reality. It provides a private identity namespace that eliminates the need for expensive public IP addresses and inbound firewall rules to connect devices.

Relay is the only routing technology that doesn't rely on Layer 3 rules, network addresses or traditional routing protocols to securely connect and route privately addressed systems across networks. Relay verifies cryptographic identities and only forwards authenticated and encrypted traffic to authorized endpoints. Reduce network complexity by eliminating connection barriers like NAT, different addressing realms, IP conflicts and complex firewall rules.

Deployment options:

Cloud

Amazon Web Services
Microsoft Azure

Virtual

VMWare ESXi
Microsoft HyperV

Physical

AV3033 – 1U Platform



Manage your things



Conductor

Conductor enforces visibility and access policy for all your things with point-and-click simplicity. Make your things invisible by creating a software-defined network (SDN) that's micro-segmented, encrypted end-to-end and multi-factor authenticated (MFA). Define the overlay network segments and systems that protected machines are allowed to access, as well as how they connect on the LAN, WAN and public internet. Policy creation and management is simple and requires no advanced training.

Available in cloud, virtual and hardware form factors, Conductor enables fast network provisioning, micro-segmentation and secure connectivity. All of this is based on unchanging cryptographic machine identities, not network addresses that change and can be spoofed.

Intuitive network orchestration eliminates the complex, disruptive and time-consuming provisioning steps associated with traditional IT solutions like firewalls and VPNs. Our customers deploy and revoke secure overlay network access in seconds, with little to no change to their existing network infrastructure.

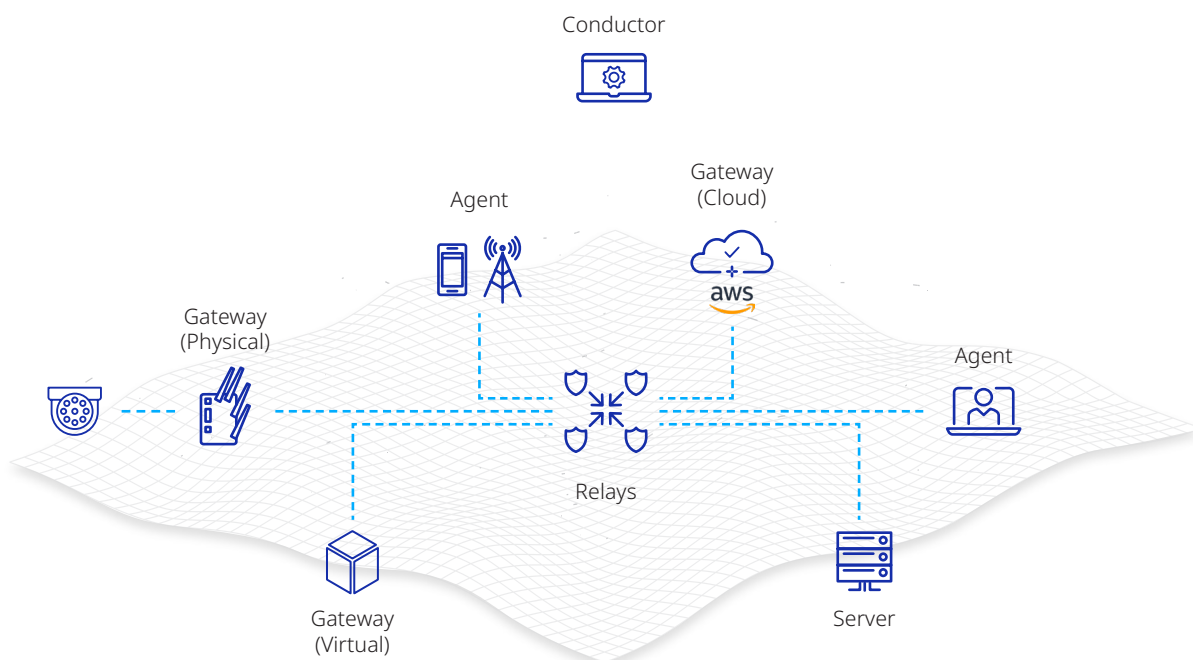
Deployment options:

Cloud

Amazon Web Services
Microsoft Azure

Virtual

VMWare ESXi
Microsoft HyperV

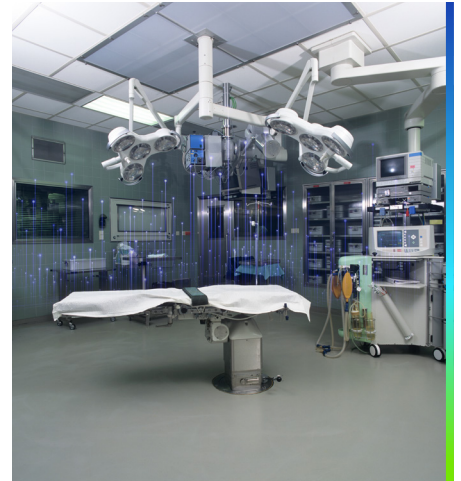


OpenBlue Airwall use cases

Suitable for a variety of uses

Critical infrastructure protection, rapid provisioning and cost-effective remote support

Automatically network, cloak, secure and manage critical infrastructure, such as oil and gas pipelines, electrical substations, smart meter systems and healthcare devices from anywhere in the world. Implement this solution without the cost and complexity of attempting to deploy and maintain separate routers, firewalls and VPNs. Because access is based on cryptographically signed, authenticated and authorized devices, the risk resulting from the common practice of using shared administrator credentials is eliminated. Organizations can significantly reduce their cyber-risk and the productivity loss of having to send field technicians to remote locations for maintenance.



Instantly provision or revoke vendor, third-party or supply chain access

Some of the most common attack vectors today are third-party systems that are either permanently or temporarily connected to a corporate network. HVAC systems, building automation, web services, vendor technicians, PoS systems, and even guest Wi-Fi all increase an organization's attack surface. Pinholes are opened in firewalls and then frequently forgotten. Configuring temporary VPN access is laborious, slow and cannot be easily segmented down to a specific resource. Permanent connections for things like building automation are difficult to maintain over time. Using VLANs or ACLs cannot prevent lateral movement from a bad actor. With OpenBlue Airwall, you can provision temporary or permanent access instantly that cannot be traversed, is immediately verifiable, and can be instantly revoked regardless of user credentials.

On-demand secure network provisioning and PCI compliance

Provision Point of Sale (PoS) systems, kiosks or pop-up stores in seconds, then cloak, segment and move out of scope for PCI compliance over any network. Shared and unmanaged networks become a non-issue, because OpenBlue Airwall prevents hackers from using temporarily or permanently connected systems on a corporate network as an attack vector. All communication has 256-bit-AES encryption.



MPLS replacement, remote office security and instant failover

Replace costly MPLS networks with OpenBlue Airwall and commercial broadband for distributed remote sites. This approach provides better security, faster provisioning and simpler management. At each site, you can deploy an inexpensive Gateway, creating a cloaked, secure and private corporate WAN. Adding a new link to an OpenBlue Airwall Overlay requires just a few clicks in Conductor. Remote office exposure to Man in the Middle (MiTM) attacks is prevented because hackers are unable to find and fingerprint devices in order to execute attacks. And if a link fails, the Gateway immediately fails over between links, ensuring high availability.



Secure and segmented user, vendor and application access control

Unlike traditional VPN technologies, an Agent or Server can now have many concurrently encrypted virtual trust segments (VTS) or tunnels to specific applications and services, without requiring an appliance. Building automation vendors can deploy OT systems at customer locations and provide encrypted and verifiably segmented access to those systems for faster and less expensive maintenance. They can do this without their customers fearing those systems as a potential attack vector.

Vendor systems can be verifiably segmented and cannot communicate with any other system on the corporate network. You can cloak all other systems on the corporate network, so they will not respond to any communication with those systems unless it is explicitly allowed. Securing internal and remote access for employees anywhere in the world becomes far more practical and cost-effective than traditional VPN and firewall technologies by eliminating failover, key management and networking problems associated with client appliance access and mobility. Agents and Servers can now connect directly or through Gateways without opaque and complex legacy network constraints.

Secure and segmented machine-to-machine communication

Servers running an Agent can bind a unique ID that is only known and available to other Agents. This unique ID frees the application server from the constraints of the hosted network, allowing it to freely move from network segment to network segment and even to a public cloud within an OpenBlue Airwall Overlay, without losing its IP address. Only whitelisted devices can locate the Agent's enabled service by its Cryptographic ID and its unique IP address.



OpenBlue Airwall delivers



Device invisibility and automatic AES encrypted tunnels



Network transparency, resiliency and instant failover



Secured VLAN isolation and micro, macro and cross-boundary segmentation



Transparent mobility of secured devices and services within OpenBlue Airwall



Connectivity for secure Layer 2 or Layer 3 networks across any link



Default zero trust model with one-click trust establishment (cryptographic ID)



Rapid provisioning, revocation and instantly verifiable quarantine



Visual Trust Map to assist with proving PCI and other compliance



Flexible deployments supporting physical, virtual and cloud appliances



Extensibility down to clients, servers, applications and embedded hardware

Appendix endnotes

1. Billions of devices without built-in cybersecurity are connecting to IT networks and are creating a massive and rapidly growing attack surface. Enabling the remote control of critical and physical infrastructure has created attack vectors that didn't exist when today's security solutions were being designed. The result is rapidly rising costs and complexity, with a measurable decline in protection. The original inventors of the networking technologies that became the Internet never imagined the billions of devices we use today. They introduced something that turned out to be a huge, critical assumption. The fatal flaw is that your IP address is used as both your location and identity. Every device gets an IP address, which is used as its identity. And that address can be found. If it can be found, it can be hacked. Moreover, every device hacked can be used to hack other devices.

2. Host Identity Protocol (HIP) was conceived as a solution to overcome the fatal flaw in TCP/IP networking, which has made networking security the complex Rubik's Cube it is today. The Host Identity Protocol standard (HIP RFCs 5201, 5202, 7401, 7402, and VPLS RFC 4665) was first proposed by Robert Moskowitz in 1999, as an individual IETF submission. It has been used in production since 2006 for everything from secure field communications by the military to accelerating manufacturing operations at Boeing by securing and enabling network mobility of their tooling infrastructure. The cornerstone of HIP "is the idea of separating a host's identity from its present topological location in the internet" for the sole purpose of "enabling a secure and mobile internet." One of the most important principles is that HIP is backward and forward compatible with any IP-based network, application or resource. HIP is an open standard, but to realize the vision of "a secure and mobile internet," a new management paradigm was needed. It required scale, policy-based orchestration, and the compatibility of HIP-based services across any operating system, hypervisor, container or hardware platform.

3. Using unique cryptographic IDs makes OpenBlue Airwall extremely resilient. Decoupling the identifier and locator functions of an IP address restores its original purpose as a resource locator. Unlike other technologies, networking and security policy orchestration is so simple that authorized business teams could easily make their own policy changes without involving other teams or risk exposing corporate networks and other connected resources.

4. Network and resource provisioning are much simpler with OpenBlue Airwall. Failover is faster, predictable and easily verifiable. Dependence on complex firewall

rules, VPN policies and key management overhead, ACLs and VLAN configuration is greatly reduced. Managing a simple IP address change, migration, addition of a new network, office or kiosk, or providing temporary or controlled third-party access no longer requires significant time and expertise.

5. OpenBlue Airwall uses a policy-based approach, enforced at the device level. This approach enables all endpoints to know and maintain knowledge of where resources within and across networks are located, and what OpenBlue Airwall Edge Service is in front of a single resource or many resources. Every Edge Service has the equivalent of a policy-based table that is instantly updated via the Conductor any time an administrator or a secure API call makes a change. The policies maintain state across Edge Services via Conductor, but do not require persistence, ensuring only authorized resources are in fact communicating with others that have been explicitly allowed.

6. OpenBlue Airwall Edge Services follow the Host Identity Protocol standard. This standard initiates trust before transport communication is established and before any data is exchanged between authorized Edge Services. Conductor orchestrates policies across Edge Services that are distributed throughout an OpenBlue Airwall Overlay, where the Conductor maintains state but does not require persistence for edge services to function.

7. OpenBlue Airwall Edge Services adapt to your network deployment. They effectively function as a switch, eliminating or reducing the need to maintain VPNs, complex firewall rule sets, VLAN segmentation, routing convergence and DNS for failover, and ACLs to accomplish secure connectivity, access, availability and segmentation. This functionality allows for a flexible deployment model that can span nearly any type of resource, location or environment. This capability of easily extending a secure networking overlay as broadly or deeply as an organization chooses across any environment cannot be matched by any other SDN, SDWAN, traditional networking or security vendor.

Additional resources

- tools.ietf.org/html/rfc7401
- tools.ietf.org/html/rfc7402
- www.pnr.iki.fi/publications/hip_survey.pdf
- <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

About Johnson Controls

At Johnson Controls (NYSE:JCI), we transform the environments where people live, work, learn and play. As the global leader in smart, healthy and sustainable buildings, our mission is to reimagine the performance of buildings to serve people, places and the planet.

Building on a proud history of 140 years of innovation, we deliver the blueprint of the future for industries such as healthcare, schools, data centers, airports, stadiums, manufacturing and beyond through OpenBlue, our comprehensive digital offering.

Today, Johnson Controls offers the world's largest portfolio of building technology and software as well as service solutions from some of the most trusted names in the industry.

