Secure, ZeroTrust™ Networks for Enterprise Workforces

Join's perimeterless infrastructure securely connects your people to their work—in the office and in the cloud.

From Perimeter Thinking to ZeroTrust™ Security by Join.

Today's networks are no longer confined to an office – your workers can be anywhere, using multiple devices – making it impossible to maintain security and performance in traditional IT infrastructures. With Join's ZeroTrust™ Platform, no individual or device gains access to the network unless they are authorized and authenticated.

Define. Define the users and devices who can access network resources.

Control. Only authorized users and devices are allowed on networks you define.

Monitor. Join ensures network traffic is segmented to guarantee total network security.

join™

SECURE PRIVATE NETWORK

Join's Secure Private Network is independent and separate from the public internet, enabling you to safely share data directly between access points. Data traversing across the public internet is still vulnerable to attacks and outages – even when using a VPN. Our purpose-built private network keeps your data safe, and can be scaled to handle variable amounts of traffic or configured to give priority to certain types of traffic.

PERIMETERLESS ARCHITECTURE

With Join's Perimeterless Architecture, there is no concept of "inside" or "outside" the network – your users and devices can be anywhere, making it impossible to maintain a clearly defined network perimeter to keep the bad actors out. Your sensitive resources are kept secure in the Join network.

ZERO TRUST ACCESS MANAGEMENT

A key feature in our perimeterless architecture is in our proactive approach to security and identity. Join protects against a variety of causes of data breaches, including attacks that compromise privileged users on the network. Because we verify a user's identity each time a request is made, we ensure only authorized users access allowed network resources.

CONTEXT BASED ACCESS

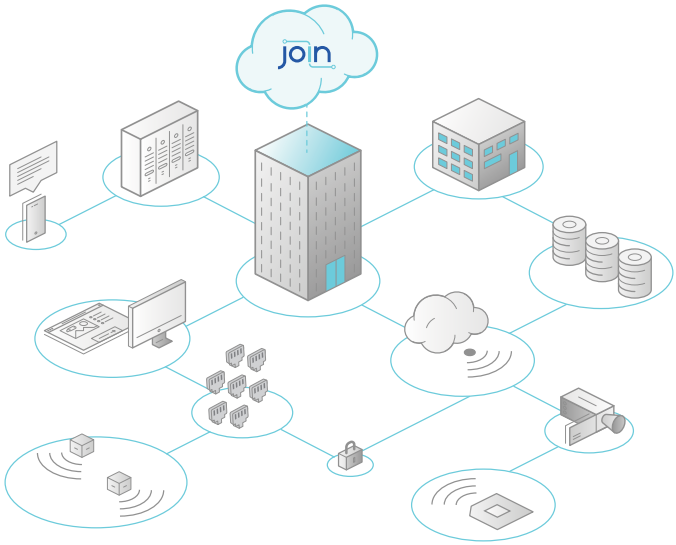
Join makes the decision of what to trust easy by evaluating the context of the user and device each time a request is made. Access to our network is granted based on a device, its state, location, and the associated user. The system continuously evaluates the entire context of each request to deliver secure, verified access throughout the network.

SOFTWARE DEFINED POLICIES

More devices and more users mean more risk. Through our Software Defined Policies, we help you determine who should have access, and how you can protect your data without impacting user experience for your employees. By collecting detailed information about the context of the user and device making the request, our platform can evaluate in real-time whether to accept or deny a specific request. Individual multi-factor authentication ensures that users and their devices are verified.

SEGMENTED IoT NETWORKS

Secure your operational technology with Segmented IoT Networks. Less advanced devices have no inherent security capabilities and only the most basic network functions, making them vulnerable to attack. Join separates the traffic of these devices through our Segmented IoT Network. By partitioning your network into secure segments, these IoT devices are isolated, allowing them to be managed without putting other more traditional devices at risk, and because some regulations mandate segmentation, such as PCI DSS, with Segmented IoT Networks, you remain compliant while staying secure.



join™

Join Digital Inc.
77 Geary Street, Suite 630
San Francisco, CA 94108

www.joindigital.com
sales@joindigital.com
415.366.5638