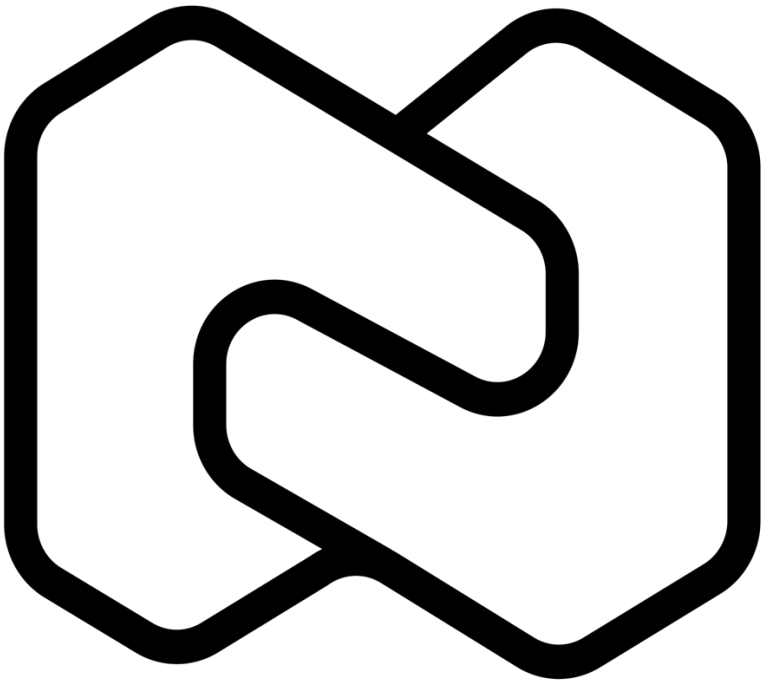
VIN – Product Brief



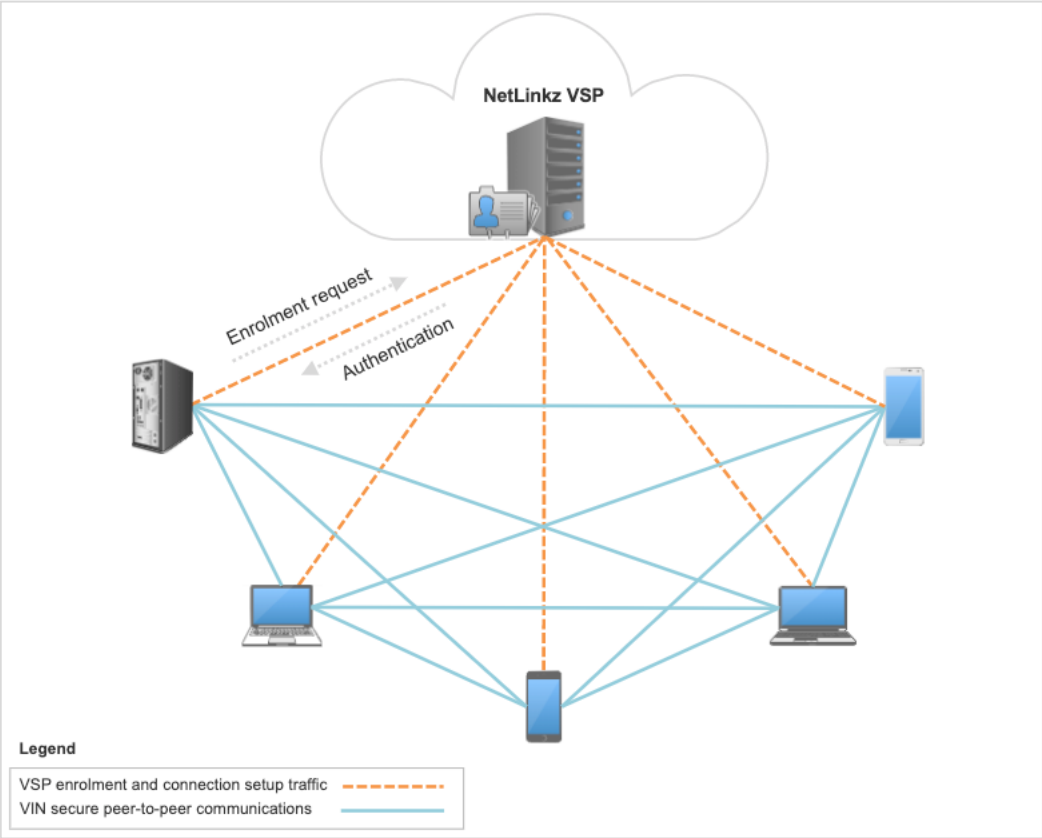
Netlinkz

Table of Contents

Product Overview

The NetLinkz VSP platform lets people securely connect their devices and cloud computing resources using an encrypted mesh network known as the VIN. The VSP provides authentication services for devices and facilitates the establishment of secure connections between devices that have been authenticated.

VIN client software running on the devices provides VIN-enrolment and encrypted communications capabilities. After a device or cloud computing instance joins the VIN, it communicates directly with other devices in a peer-to-peer mode.



All applications on a device can utilize the VIN for secure communications. The VIN can transmit any kind of data and there is no limitation on the size of file transfers.

The VIN is a virtual network. Administrators can deploy a VIN in any public or private network. An administrator can also segment physical networks using the VIN, creating private networks under their control.

Problems Addressed

The VIN allows customers to securely connect devices distributed across any network topography without deploying expensive network access servers and specialised network infrastructure (like VPN concentrators). Typical usage scenarios:

- Remote access into a device behind a firewall
- Secure cloud, data centre or IoT network access

The VIN also allows customers to spit communications within a LAN into isolated virtual networks (micro-segmentation).

How are Problems Solved

The VIN is a virtual network that is network agnostic. This means that the VIN can span multiple physical networks and automatically traverse firewalls. As such, it provides a convenient and efficient means of providing remote access and cloud/data centre/IoT network access.

When used in conjunction with firewall rules, the VIN's encryption and enrolment-based network model allows for LANs to be securely segmented into private networks with limited access.

Features & Benefits

Security

- The VIN security has proven to be un-hackable (winner of multiple security awards, officially pen-tested 2x & recipient of an ASAE 3150 Assurance Report)
- The VSP is typically deployed outside a customer's core network, making it difficult for attacks to find.
- Communications in the VIN are protected by strong AES 128-bit encryption that only authenticated devices can decrypt.
- The VSP is a network controller. It does not participate in the VIN, so it cannot be used to intercept VIN communications.
- VIN network administrators can monitor VIN authentication requests sent from devices and disconnect devices, if required.

Single-vendor, turnkey solution

- The NetLinkz platform does not rely on expensive hardware.
- No third-party software is required.
- Minimal configuration (if any) is required to allow VIN traffic though the customer firewall.

Easy to deploy

- The VSP platform can be deployed on premises or in the cloud.
- The VSP platform features a single-command install from a secure repository. The installation only takes a few minutes an no pre-installation configuration is required.

- The VIN client software is available for desktops and servers (Windows, Mac and Linux) and phones and tables (iOS and Android). Users can install the software without assistance.
- Administrators distribute VIN enrolment invitations to their users. Users accept the invitation via the VIN client interface.

Highly efficient networking

- The VIN Client software runs as a network service that provides a continuous "nailed-up" connection, so the VIN is always available for applications on the user's device.
- Devices in a VIN exchange data directly using peer-to-peer communications, so VIN traffic utilizes the shortest path available in the underlying network infrastructure when traveling from sender to receiver.
- The VIN does not rely on a central switch (such as a proxy or VPN gateway) to relay traffic, so there are no inherent communication bottlenecks.

Numerous applications

- The VIN provides secure networking and network segmentation.
- The VIN can be used in conjunction with firewalls to protect cloud infrastructure from unauthorized access.
- Hybrid clouds can be formed using the VIN to join clouds belonging to multiple cloud service providers and clouds in different geographic regions.
- Third-party software vendors and system integrators can add VIN security to their products by bundling the core component of the VIN Client with their software and communicating with the VIN Client through an API.

Competitive Analysis

The VIN has three classes of competitors:

- Secure peer-to-peer virtual networking software (i.e. software that works in a similar fashion to the VIN) – such as Net Foundry, Zero Tier & Tempered Networks
- Remote access software – such as LogMeIn, TeamViewer, GoToMyPC, VNC Connect, Zoho
- VPN software – such as Cisco VPN & OpenVPN

The VIN is a better alternative to all of the above, because solutions in the above classes have numerous disadvantages when compared to the VIN:

Solution	Key Disadvantages Compared to VIN
Secure P2P software	• Setup is not easy and management consoles are complicated / hard to navigate

	• Network performance is poor (none could match the VIN in speed tests) • Relies on public multi-tenanted infrastructure or requires hardware (Tempered Networks) – likely the source of poor performance encountered in testing and potentially a security issue • Client software has no network directory – making the secure networking less user friendly
Remote Access Software	• Relies on public infrastructure to broker connection with target device – potentially a security issue • Most vendors only support PC and Mac targets • Most vendors provide a thin-client virtual desktop experience • Number of concurrent connections is limited to a couple of sessions – whereas there is no target limit on the VIN • Some vendors require authorisation of access on the target machine – making the software cumbersome to use from a logistical perspective
VPN	• Requires network access server (usually expensive hardware) • Exposes the base network to attack – security issue • Network access server is a potential a bottleneck (performance and reliability-issue prone) • Cannot protect traffic end-to-end – potentially a security issue