ION™ A DIVISION OF apitech™

Whitepaper

Solving the Top 3 Privileged User Access Problems

NetGard™
Privileged Gateway Solution

Solving the Top 3 Privileged User Access Problems

NetGard™ Privileged Gateway Solution

Cyber security is top of everyone's mind in today's hyper-connected world. The traditional security perimeters used by organizations are vulnerable, and fast-growing technologies like cloud, mobile and virtualization are blurring the security boundaries of an organization. Data are the most precious commodity and its integrity is vitally important to any organisation. Indeed, information and its underlying infrastructure are the lifeblood of any business. Data are only increasing in both volume and velocity, and the most valuable and confidential information, such as customer identities, financial information, and personal data are the things that cyber criminals want.

Businesses continue to globalize and are more likely to have a growing number of internal and external access points. Where, at one time, all of the IT department was in-house, this is decreasingly the case. Worldwide collaboration and the upswing of using independent contractors, managed service providers and freelancers for targeted work brings to light the safety and security of IT systems. This is where secure remote access, in particular, Privileged Access Management comes into play.

Managed Service Providers (MSPs) and enterprises face many challenges dealing with remote access to critical network devices and systems. They are often managing a diverse set of tools in order to deliver a robust set of services and maintain systems inside the enterprise network or in the Cloud. These include the typical IT Data Centers or VoIP systems but also mission critical systems such as HVAC, Security Monitoring Applications, and core systems such as medical or lab equipment. In order to manage these systems, enterprises and MSP's need to manage access to a group of users with elevated rights. These types of users give access to both internal and vendor managed users.

The access provided and privileges assigned to these users should be managed from a centralized location and work on the principle of least privilege, providing the minimum access required for these users to do their job. However, it is often multiple tools and access points that control who gets in and what they can do. This results in 3 major problems facing organizations needing to ensure security and compliance.

#1. Remote Access and Management

The network is open to risk as remote access and management of systems and privileged accounts is required in today's world. This needs to be managed with consistent controls to avoid hacking and compromise.

#2. Time to service

How quickly connected devices and networks can be serviced when user rights and access are managed through multiple systems.

#3. Ensuring compliance

How varied compliance needs such as SOX, NIST, IRS, PCI or HIPAA can be met when there are no proper auditing capabilities across all systems.

#1. Remote Access and Management

The Problem

The sharp rise in remote working means that agencies and employees have become more geographically disparate and may be working from their home rather than the office, so secure remote management of IT and voice systems has become a necessity. Every day internal technicians, contractors, and outside vendors remotely access all types of equipment over their home wifi networks, so it's even more important that the right security is in place for privileged user access. Traditional network security falls short in meeting the demands of privileged session management for remote users, vendors and systems. MSPs, the enterprise CISO, CTO, CFO, and other vendors managing networks must enable a broad range of privileged users to securely access a complex network of distributed IT assets.

The Solution

Netgard™ Privileged Gateway from ION Networks, a universal, secure, remote access gateway that allows MSPs and enterprises to manage privileged user access to critical voice and data services. It enables both internal and external users to access only authorized parts of the network, reducing the threat of a security breach without compromising productivity.

Netgard Privileged Gateway:

- Is a cost-effective, secure remote access platform for internal and external privileged users
- Reduces risk of privileged user breach
- Is built around the concept of a Federated Connection, enabling a trust relationship to be built with vendors
- Provides a scalable pay as you grow system that meets future business needs
- Has the flexibility to enable access and monitoring to virtually any trusted platform that is FIPS certified
- Is a highly configurable solution to meet the zero trust requirements of both parties
- Is a trusted FIPS 140-2 certified solution
- Meets stringent compliance requirements with the most robust auditing
- Delivers granular controls, visibility and reporting of technician activity
- Offers the most robust audit to meet stringent compliance requirements
- Reports on technician activities, providing additional visibility on performance

#2. Time to Service

The Problem

Connecting to your customers' networks through multiple remote access tools is hugely time-consuming, so your technicians aren't as productive as they could be. The excessive time to provide delivery of services affects schedules and revenue and not only do time-consuming processes affect productivity and revenue, it also leads to a poor work-life balance for technicians managing 24/7 delivery.

The Solution

Netgard Privileged Gateway securely links to the endpoint through a Federated Connection. A Federated Connection is a digital handshake, defined by a Service Contract and agreed by both parties, that determines access rights and controls, and creates a secure, compliant link to solve the time and cost issues of typical connections. It meets the need for quick, but secure, access without limiting the level of service that can be delivered, and prevents excessive delivery time for these services by offering an easy way to set up specific access for privileged internal and external users.

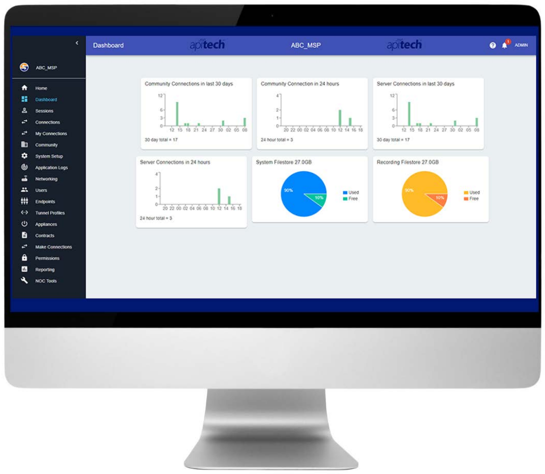
Once approved, the session activities are logged and session recording can be activated. The Federated Connection builds a trust relationship to ensure all parties' technical and security needs are met, with one party (from either side) controlling and managing the connectivity. It forms an agreement about the baseline security methodologies (for example encryption, key strength, and hashing) and then defines access rights and controls, including:

- Who is allowed access
- When access is permitted
- What devices each individual is allowed to access
- Whether per connection authorization is required

Changes and adjustments to the connection are quick and simple. If new technicians need access, or existing technicians need permission changes, the contract can easily be adjusted.

With Netgard Privileged Gateway accessing your customers' systems is quick and simple so you can go in and out with ease using your customer-agreed rules. It meets the needs of vendors and enterprises to provide robust service delivery techniques with an elevated set of security technologies. In addition it:

- Removes additional costs to vet and approve a one-off access method for each MSP
- Simplifies access paths, limits vectors of attack
- Improves work life balance of technicians providing 24/7 support against stringent SLA's



Netgard Privileged Gateway dashboard view

#3. Compliance

The Problem

Solutions managing privileged access need to meet stringent compliance and auditing guidelines with comprehensive audit trails and session recording required to ensure full accountability. System logs and session recordings need to paint a complete picture when forensics are required to understand who did what to the system, and when.

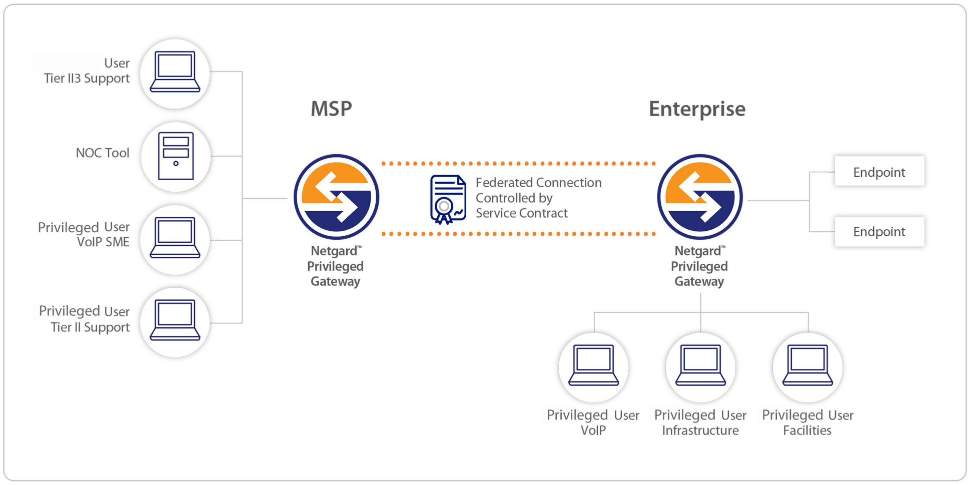
The Solution

ION Networks has a 30-year security pedigree backed up by FIPS and NIAP certifications. Netgard Privileged Gateway meets the most stringent security requirements, and has been vetted by the U.S. DoD and some of the world's largest financial institutions. It complies with stringent industry recognized standards such as FIPS, HIPPA, SOX, PCI, and meets the needs of both private enterprises and government entities.

Summary

Netgard Privileged Gateway solves all your remote access, time to service and compliance needs as it:

- Saves time and resources, and reduces complexity by allowing you to manage all customers, technicians, or vendors using just one tool
- Tailors custom security roles and rules at the security perimeter gateway
- Provides access to complete forensics of internal and external technician activity, capturing all actions
- Complies with security and industry regulations
- Uses a Federated Connection to build a trust relationship with customers or vendors
- Allows you to scale services to suit business growth



A Privileged User Gateway (PUG) service contract controls the connection between federated privileged user gateways

ION A DIVISION OF apitech

Solving the Top 3 Privileged User Access Problems

About ION Networks

A trusted name in remote device management and secure access, ION Networks provides remote access solutions that enable customers to securely manage, monitor, and maintain high quality of service for critical voice and data network infrastructures. Customers include MSPs, enterprises, equipment manufacturers, and government and military agencies. ION Network's solutions include:

- Netgard Privileged Gateway for Managed Service Providers
  Netgard Privileged Gateway for Enterprise
- ION PRIISMS
- ION Service Access Point
- ION Secure Appliance
- Avaya Secure Access Link Appliance
- ION Secure Modem
- Netgard MFD Follow-Me Print Solutions
- Netgard MFD – CAC/PIV security appliance
- ION ST530 Two-Factor Authentication Token

ION Networks is a division of APITech with a 30+ year pedigree in security, access and connectivity solutions, and global reach.

Contact Us

USA
Tel: +1 908-546-3900

Canada
Tel: +1 613-270-9009

UK & Europe
Tel: +44 (0) 1452 557 237

Email: sales.ion@apitech.com