Solutions at a Glance

Remote IT device management administration.

SECURE privileged systems administrator access to mission critical applications.

Who is ION Networks?

ION Networks… The most trusted name in remote device management and secure defense and commercial applications through controlled access technology. The ION solution enables service providers, equipment manufacturers, government and military agencies, and corporations to remotely manage, monitor, and secure critical voice and data network infrastructure.

ION solutions ensure the "privileged" system administrator can access systems without compromising security. Only trusted users can access these systems requiring a comprehensive solution that secures all privileged user connections; whether the user is a corporate IT employee, an equipment manufacturer or 3rd party consultant/service provider, contractor…

This is a solution that is flexible and can handle any type of connection or application needed to manage a device.

The ION solution is a purpose-built platform that enables secure remote device management with an integrated security architecture foundation. It uses similar security techniques as enterprise security platforms. This unique application enables access for both internal and external privileged users.

Meeting the most stringent security requirements, the ION solution has been vetted by the U.S. DoD and some of the world's largest financial institutions. ION technology has a security pedigree backed up by Federal Information Processing Standard (FIPS) and National Information Assurance Partnership (NIAP) certifications.

ION Networks is a part of API Technologies Corporation.

api technologies corp.

ION Networks
120 Corporate Blvd
South Plainfield, NJ 07080
Phone: +1 908.546.3900
Email: IONsales@apitech.com
www.apitech.com

ION Solutions
Overview

Who can benefit from the ION solution?

Equipment Manufactures / 3rd Party Service Providers

ION Networks provides solutions that allow service providers of any size to efficiently service their client's voice and data IT infrastructure requirements by utilizing multi-factor authentication, encryption, & access control. This provides end-users with protection against hacker threats and the assurance of visible transparent privileged access users via monitoring and recorded sessions.

The ION solution can be deployed to provide a primary, secure connection via the Internet or cellular connections. Service providers can depend on delivering services 24/7 with high availability and the highest standard of security. The benefit is a consistent method to rapidly and securely provide service delivery for infrastructures across all customers.

Don't have Internet access… the ION solution can also be used as an emergency out-of-band platform. You will reduce downtime and truck rolls when primary network access is no longer available and resolve systems issues via an alternative connection.

These "backdoors" into a network commonly have limited security. Typically there is incumbent weak security on the "backdoor" public connections via the PSTN or cellular network. The ION solution makes the "backdoor" security identical to the front door. You are still secure.

End-user Enterprise (Commercial / Defense):

Commercial – You can grant third party and internal users access for remote management of voice and data systems. Decrease downtime by not waiting for a service provider arrive at a location to the resolve issues. Utilize increased security measures by recording system activity and protecting against hacker threats to sensitive information with auto-lockout modem functionality.

About ION: *For over 25 years ION Networks has produced procures to secure "privileged user access" ensure systems administrative interfaces cannot be compromised. Over the past few decades systems and networks have changed but the need to secure these interfaces have not…ION's solution has evolved over this time to ensure our customer's systems are secured from both internal and external threats.*

Military & Government – Remotely access voice and data systems, local and abroad, with (DoD) Unified Capabilities Approved Products List (UC-APL) and Joint Interoperability Test Command (JITC) certified products. Utilize your DoD Public Key Infrastructure (PKI) to authenticate and secure your access points. Manage and record system activity and protect critical information against threats with multi-factor authentication and auto-lockout modem functionality. The systems management interface prevents security gaps, such as weak authentication, encryption, or systems changes/audit.

Products Overview

The ION solution is composed of an access gateway called Proactive Remote Integrated Intelligent Secure Management Solution (PRIISMS) and multi-function security appliances that enable local security and connectivity to remote devices.

ION Networks can be trusted. We have made significant investments into FIPS and Common Criteria certification to ensure the security foundation of our solution has been vetted by a third party testing organization. Additionally, ION Networks updates software regularly based on new software vulnerabilities and keeps up to date with updates to Open Source components.

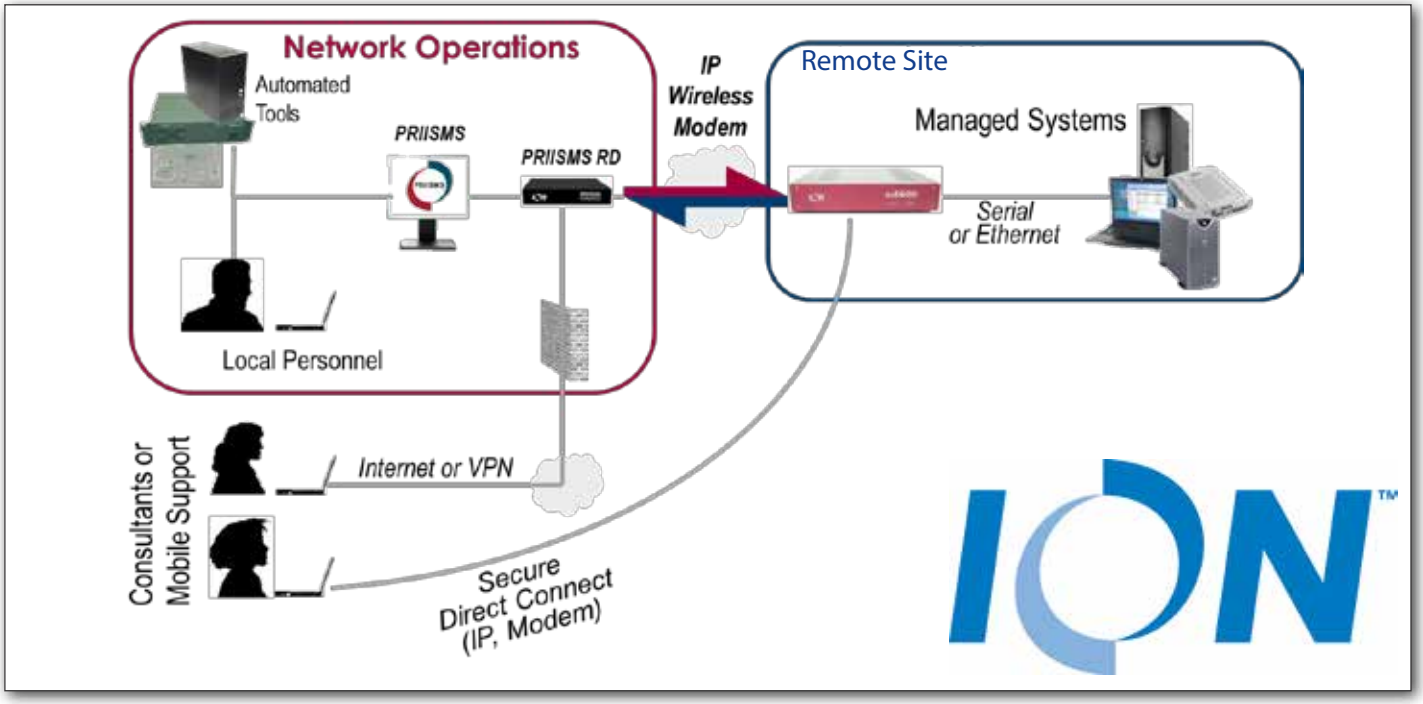
Scalability & High Availability

- The ION solution secures privileged user access from 25 managed devices to 10s of thousands of IT devices.
- It ensures High Availability deployments with system redundancy eliminating a single point of failure.

Flexible Platform Support

- You run all ION products on dedicated hardware/appliances or on virtual machines.
- It supports traditional enterprise deployments or in the cloud.
- It is compatible with ESXI servers or Hyper V.

ION Networks Complete Solution



What is PRIISMS…

ION PRIISMS (Proactive Remote Integrated Intelligent Secure Management Solution) is a secure web-based gateway application that provides centralized control over security and administrative access policies of distributed and complex network device environments. Service providers / network administrators can configure, troubleshoot, and manage consolidated or geographically dispersed critical network devices, in- or out-of-band, remotely or from a central Network Operations Center (NOC). The PRIISMS architecture provides a scalable solution ensuring the highest availability for an unlimited number of connections.

PRIISMS is a simple to use platform that provides a robust set of security features ensuring only trusted users can access the management interfaces of mission critical systems. In addition, PRIISMS provides the most comprehensive set of audit capabilities documenting what device(s) a privileged user has accessed, and what changes they made by recording sessions. PRIISMS provides the ability to control who can get access to specific devices and deliver confidence with visible transparent knowledge of what was done be it device access via SSH, Web, RDP or propriety client.

ION™ PRIISMS

- Single-sign-on technician access for remote endpoint management
- M2M automatic connectivity
- ION devices central manager
- Software, virtual machine or hardware appliance

ION Products

Service Access Point

What are the appliances… ION has a range of hardware and virtual machine (VM) security appliances to meet the unique needs of both VoIP and IT deployments. Secure appliances provide flexible and adaptable connectivity solutions via diverse networks or physical connectivity to devices via console ports or networks such as the PSTN, Cellular, or broadband networks. Utilizing the ION VM security appliance enables secure remote access to systems in cloud network environments.

ION™ Secure Virtual Machine

- Eliminates the cost of physical appliances
- Ensures privileged administrators access only permitted Cloud based systems utilizing VPN tunneling technology
- Cost-effective and scalable solution for small and large deployments
- Compatible with VMware, ESXI Server and Microsoft Hypervisor

ION™ SA600 Service Access Point

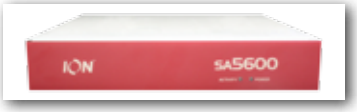
- Console terminal server, modem and wireless
- Ideal solution for legacy PBX monitoring and access

ION™ SA500 Service Access Point

- Ideal device for SME deployments for IP Office, BCM, or Suretel
- Low cost Internet service delivery platform

ION™ SA5600 Secure Appliance

- High-performance, Enterprise-secure appliance
- Easy connectivity, highly scalable solution
- Modem, Internet, or wireless connectivity device



ION™ SA5600-IA2 DoD/Gov Edition

- JITC/IA approved
- Dial-up, IP and console access
- Built-in two factor authentication
- Encrypted link
- CAC/PIV/SIPR card authentication

JITC/IA Certified

ION™ SA5610-SAL Avaya SAL Edition

- Plug-and-play SAL Gateway appliance
- Installs in under 10 minutes*
- Complete SAL Gateway installation without the headache of building from scratch
- Supports SAL Gateway and SLAMON

ION™ SM110 Secure Modem

- Eliminate weak passwords securing critical network elements
- Ideal for mission critical router console for OOB access

Appliance Overview	Secure VM	SA500	SA600	SA5600	SA5600-SAL
Internet	√	√	√	√	√
Out of band			Modem/Cellular	Modem	Modem
Console Server (Router/ PBX)			√	√	√
IP Endpoints	6-400+	6-24	6-24	64-400	64-400
	SME/Enterprise	*SME*	*SME*	*Enterprise*	*Enterprise (AVAYA)*

** In the majority of instances.*