ION™

# How does your organization manage Privileged Users?

## A GOVERNMENT & MILITARY SOLUTION GUIDE

IONsales@apitech.com | www.apitech.com| Tel: +1 908-546-3900

api technologies corp.

## Who is ION Networks?

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

Ensuring the “privileged” system administrator can access systems without compromising security and only trusted users can access these systems requires a comprehensive solution that secures all privileged user connections; whether the user is an employee of a corporate enterprise IT organization, an equipment manufacturer or 3rd party consultant/ service provider.

## A Solution for Every Industry

A majority of IT security dollars are spent on securing the perimeter of the enterprise network and providing security to end-user applications. Unfortunately, this does not include protection against attacks by "trusted" insiders who are routinely given access to network administrative interfaces. With ION, industries such as banking, government, technology, telecommunications, and healthcare are able to use a cost-effective and leading privileged user access security solution.

## Secure Systems & Information Assurance

For years, ION Networks has provided a solution to manage Priviliged User Access. ION is the most trusted name in remote device management and secure access technology. ION appliances and software enable service providers, equipment manufacturers, government and military agencies, and corporations to remotely manage, monitor, and secure critical voice and data networks. ION is part of the Secure System & Assurance Division of **API Technologies** which designs security solutions for senstiive environemts where data, if compromised, could have severe financial, political, privacy and defense-related consequences.

IONsales@apitech.com | www.apitech.com | Tel: +1 908-546-3900

# ENABLE SECURE REMOTE DEVICE MANAGEMENT OVER ANY NETWORK

## Securing Remote Management for the World's Most Critical Information & Communication Assets

**The Challenge**

As agencies and employees become more geographically disparate, remote management of IT and voice systems becomes a necessity. Every day internal technicians, contractors, and outside vendors remotely access all types of equipment, including PBX and VoIP systems, IT devices, and storage systems. Remote access and management systems have changed from simple terminal emulation programs to web, remote desktop, and proprietary tools. Operations departments are overwhelmed by new and ever-changing security and compliance requirements, burdened with re-purposing and managing legacy remote access technology ill-equipped to meet today's remote management requirements. Finally, it is required that a solution is certified for U.S. Government use, eliminating procurement and deployment barriers.

**The Solution**

Ensuring the Privileged System Administrator can access systems without compromising security and only trusted users can access these systems requires a comprehensive solution that secures all privileged user connections.

### Secure all users including:

- Government enterprise IT organization employee
- Equipment manufacturer
- 3rd party consultant or service provider

### Flexibility

The ION solution is a purpose-built platform to enable secure remote device management with a security architecture foundation. Using similar security techniques as enterprise security platforms, this application enables access for both internal and external privileged users.

### Compliance, Listed On DISA APLITS

Meeting the most stringent security requirements, the ION solution has been JITC certified and vetted by the U.S. DoD and some of the world's largest financial institutions. ION technology has a security pedigree backed up by FIPS and NIAP certifications.

IONsales@apitech.com | www.apitech.com | Tel: +1 908-546-3900

## Product Overview

The ION solution is comprised of an access gateway called PRIISMS and multi-function security appliances that enable local security and connectivity to remote devices.

ION Networks is 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. Addiitonally, ION Networks updates software regularly based on new software vulneralbilities and keeps up to date with updates to Open Source components.

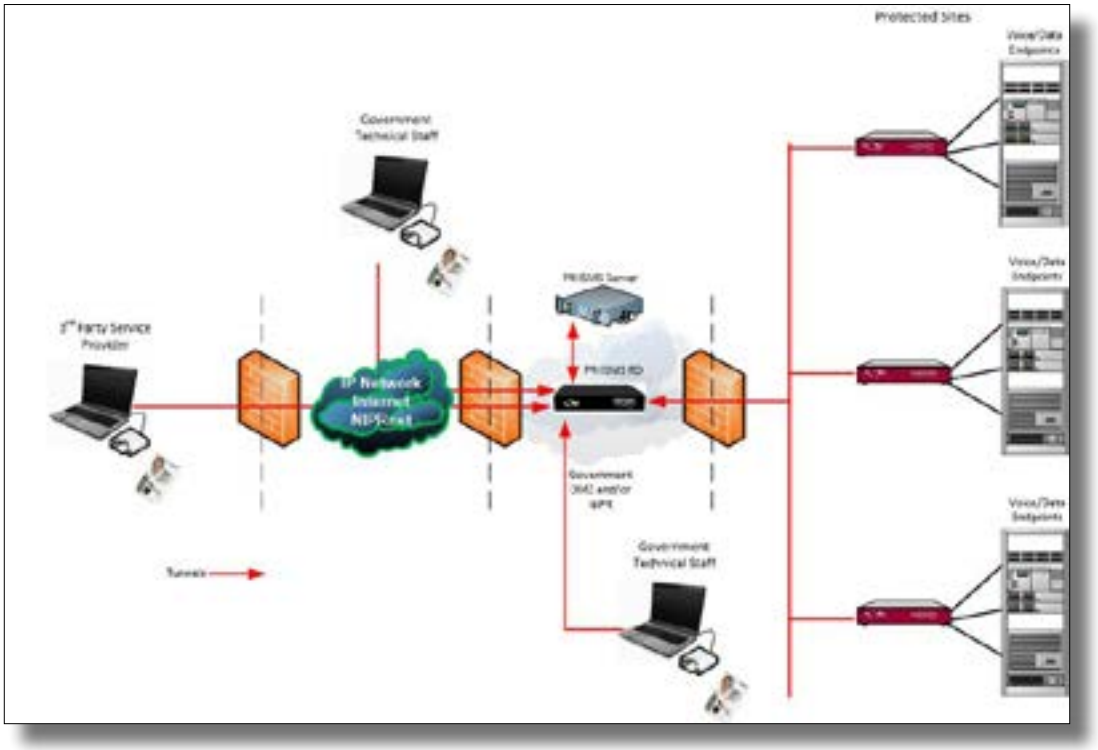
**Scalability & High Availability**

- Secure privileged user access from 25 managed devices to thousands of IT devices.
- Ensure high availability deployments with system redundancy eliminating a single point of failure.

**Flexible Platform Support**

- Run all ION products on dedicated hardware/appliances or on virtual machines
- Supported for traditional enterprise deployments or in the cloud.
- Compatible with ESXI server or Hyper V.

### Government & Military Deployment



## 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 confi gure, 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 of availability 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 accessed, and what changes they made with recorded sessions. PRIISMS provides the ability to control who can get access to specifi c devices and confi dence with transparent knowledge of what was done be it device access via SSH, Web, RDP or propriety client.

IONsales@apitech.com | www.apitech.com| Tel: +1 908-546-3900

# Service Access Point 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 broad band networks. Utilizing the ION VM security appliance enables secure remote access to systems in Cloud network environments.

## What are the recommended appliances...

### ION™ SA5600-IA2 DoD/Gov Edition

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


FIPS 140-2 VALIDATED

### ION™ Secure Virtual Machine

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

### 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

## Selected Use Cases

**US Department of Defense | US Marine Corps | Defense information Systems Agency | Defense Health Agency**

The US DoD required that all systems installed on IP or voice networks pass a system interoperability and information assurance test. The ION solution was one of the first systems that passed both sets of tests and received JITC approval. [The ION system was and certified with Avaya, Cisco, Nortel, Juniper & Lucent systems.] Use of the ION system was then expanded to secure all system administrative interfaces of critical communication systems located at US Marine Corps, Defense Information Systems Agency and The Defense Health Agency bases across the globe.

**NASA**

NASA needed a secure out-of-band (dial-up) access system to Cisco routers and switches that met their requirement for strong authentication. Since two-factor authentication and SSH encryption is embedded in ION solution NASA choose the SA5600 Secure Appliance for this application.

**White House Communications Office**

The White House Communications Office is responsible for managing and monitoring critical voice systems used by the President of the United States. Whether the President is in the White House or traveling in Air Force One his communications go through a special Avaya voice system. The White House Communications Team uses the ASG Guard II (Avaya OEM of ION's Secure 5500 appliance) to remotely access these Avaya switch and voice adjunct systems for remote diagnostics and management.

**United States Postal Service**

Sprint is the primary voice provider for the United States Postal Services. Sprint needs to remotely access the Nortel voice devices installed at US Post Office locations across the country. The US Post Office has a stringent security requirement that Sprint could only meet with the ION SA5600 Secure Appliance. With the SA5600 Secure Appliance, Sprint can now securely monitor voice systems installed at post office locations throughout the country.

IONsales@apitech.com | www.apitech.com| Tel: +1 908-546-3900

## Contact ION Today

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

## Visit Us

www.apitech.com

api technologies corp.