



Reap the Rewards of Managed Services with Vendor Solutions from ION

As you read this, vendors are likely accessing your company's network. Greater than 40% of companies outsource IT to Managed Service Providers (MSPs), and that number is expected to grow to 57% in the next two years. (Business Communications Review, September 2006)

New Vendors, New Challenges

Because vendors – such as telecommunication providers, equipment vendors, and service providers – share the responsibility for maintaining critical systems, they require remote access to a variety of network resources. Granting this necessary access often requires giving up a measure of control, and presents the following challenges:

No Accountability: Traditional remote access solutions provide little or no visibility into vendor activities on enterprise systems. As such, enterprises have no way to measure how well (or how poorly) a vendor performs and what value is actually delivered.

Compliance Challenges: Most compliance policies now require enterprises to produce a record of all actions taken on and within the network. However, most traditional remote access solutions do not produce a detailed audit trail.

Security Risks: Solutions such as traditional VPNs extend too much trust. Once a vendor is in the network, the vendor has unfettered access to privileged information and mission critical systems.

Productivity Loss and Redundancy: Different departments within an enterprise have unique vendor remote access requirements. As such, many more employees may spend time working through connectivity and security requirements than needed, rather than focusing on core responsibilities.

ION's Vendor Access & Control Solution

The Vendor Access & Control Solution from ION allows enterprises to reap the rewards of managed services and make the most of their vendor relationships, without surrendering control.

Featured Solution Benefits

- Speed problem resolution and reduce downtime
- Avoid "fire drills" during an outage
- Negotiate better contracts with vendors
- Significantly reduce the time and costs associated with granting vendor access to enterprise systems
- Gain visibility into vendor access and activities
- Eliminate finger pointing
- Meet or exceed security and compliance requirements

In addition to these organization-wide benefits, individual departments can improve efficiencies and overcome common challenges through implementation of ION's Vendor Access & Control Solutions. Read on to discover the positive impact ION's solutions have on four key functional areas: IT Operations, Security Management, Voice Management, and Vendor Management.

IT Operations

Responsible for the implementation and ongoing management of IT systems, this group often bears the operational pain of granting, denying, controlling, and managing vendor access in the face of ever-heightening security requirements.



Challenges

Given this team's growing list of responsibilities, vendor access presents a constant and time-consuming challenge.

This group typically offers two types of solutions for vendor access: VPN or token. However, both of these solutions are problematic. On one hand, VPNs require customization and extend too much trust to vendors. (Once in the network, vendors' administrative-level permissions offer few restrictions, allowing them to access any variety of systems and confidential data.) On the other hand, token access (typically used to grant remote access for internal employees) is limiting for vendors, who require administrative-level access to effectively manage IT systems.

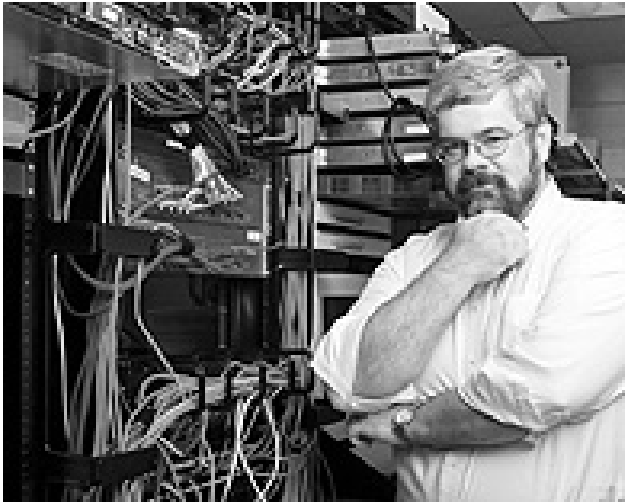
ION Solution Benefits for IT Operations

Purpose-built Technology Saves Time: Unlike VPNs and token solutions, ION's solution was designed specifically for remote vendor access. The centralized solution is easy to administer and provides a high degree of control. Vendors and/or individuals may be added or removed in minutes.

Maintains Consistent Security Practices: With ION's solution, vendor access is centrally controlled and administered. All departments may now use a single system for remote vendor access, eliminating redundancy. This also eliminates granting of unapproved, unmonitored access. The system keeps a detailed record of all vendors and access points available to each. At the click of a mouse, your IT operations team may identify which specific devices are available to each vendor.

Meets (or Exceeds) Compliance Requirements: ION's solution was designed with security in mind and is currently used by the US Department of Defense, Social Security Administration, and many Fortune 500 financial services firms. Built-in features, such as two-factor authentication and AES encryption provide unparalleled security, while reporting features, such as keystroke logging and audit trails offer a complete record of all vendor access and activities for every session. The visibility into vendor actions and reporting proves controls are in place to monitor activities on the network. These controls are key components of many compliance requirements.

Extends the Correct Amount of Trust Without Inhibiting Remote Service Delivery: Permission-setting features let the IT operations team and/or individual departments easily define which vendors may access which resources at any given time. Your team members also have the ability to permit or inhibit selected administrative activities on enterprise systems giving your vendors the permissions necessary to carry out their contracted assignments without putting your IT and voice assets at risk.



ION offers
the only
purpose-built
solution
for secure
vendor access
& control.

Security Management

Your Security Management team is tasked with implementing and enforcing consistent security practices throughout the organization to mitigate risk and ensure compliance with a variety of government and/or industry-mandated requirements.

Challenges

Maintaining consistent security policies across all departments is essential. However, the variety of vendors and the multitude of their remote access requirements makes consistency difficult (or impossible) to achieve. Your security team must therefore make decisions that may negatively impact remote service delivery (for example, a “no modem” policy) or treat every managed services engagement/vendor separately, investing time and energy negotiating access. Finally, security teams are limited by traditional remote access technologies designed to allow access by trusted parties (for example, branch offices and employees), rather than vendors whose requirements do not neatly fit into the traditional remote access mold.

ION Solution Benefits for Security Management

One Solution, Many Vendors: ION’s centralized, easy-to-manage solution allows enterprises to use a single platform to provide remote access to all vendors, regardless of required connectivity method. Vendor access granted by this solution provides your security team with complete control over access to, and activities on your enterprise systems.

Detailed Audit for Compliance: The ION solution offers a real-time audit trail of all actions (including individual keystrokes) taken on enterprise systems, often an essential compliance requirement.

Purpose-built for Vendor Access: Unlike traditional VPN solutions, which are not built to accommodate vendor access, ION’s purpose-built solution is configured right out of the box, saving your security team hours typically spent configuring VPNs.

Voice Management

Voice Management is tasked with ensuring corporate telecommunication systems are up and running. This typically includes the management of VoIP systems, PBX systems, routers, etc. The Voice Management group typically outsources some or all management of voice systems to various telecom companies and equipment vendors, who typically deliver services managed under a Service Level Agreement (SLA).

Challenges

In the age of convergence, this group must manage a wide array of devices, ranging from VoIP to legacy telephony systems. Most vendors require remote access to the systems in order to maintain uptimes dictated by the SLA. This presents a challenge for voice management teams who may be unfamiliar with new, complex IP security requirements. Also, due to the wide array of systems this group must support, granting and managing vendor remote access becomes time consuming and complicated.

IT Solution Benefits for Voice Management

One Solution Meets All Access Requirements: ION's Vendor Access & Control solution provides secure vendor access to virtually any device, any application, using any type of connectivity. This flexibility is essential for the voice group that deals with systems ranging from legacy voice to state-of-the-art VoIP systems.

Reduced Downtime via Secure Modem Access:

In many cases, an Internet or VoIP outage may be corrected by rebooting a router using a dial-up connection. However, many companies have phased out modems, citing security reasons. If a vendor cannot remotely access a router, a field technician must be dispatched to the site, often extending the length of an outage for hours, or even days. ION's solution provides emergency dial-up access in a highly secure way, without incurring the risks associated with traditional, password-protected modems.

ION the leader
in remote
management of
voice systems,
used by more
than half the
world's largest
telecoms.





ION helps
you get
maximum
value from
your vendor
relationships.

www.ion-networks.com

Vendor Management

Vendor Management is a relatively new department for many organizations. Tasked with managing an enterprise's vendor relationships, it is typically this group's responsibility to negotiate contracts and ensure the company is receiving the best possible service from a vast network of vendor partners.

Challenges

With most traditional remote access solutions, enterprises are unable to collect data on vendor activities. Vendor Management professionals must therefore rely on vendor-supplied performance data. Given the subjective nature of the data and the lack of visibility into vendor activities on enterprise systems, Vendor Management teams are at a disadvantage when re-negotiating vendor contracts. Often, one of the more complex items in negotiation with vendors revolves around the conditions for granting remote access. Small changes, made by either the vendor or the enterprise, have ripple effects and cause both parties to make adjustments in security and/or connectivity, contributing to frustrations on both sides and their associated productivity loss.

IT Solution Benefits for Vendor Management

Visibility into Vendor Activities: ION's solution provides a detailed record of vendor access and activities, giving Vendor Management teams a clear record of the actions taken by vendors on enterprise systems, which can then be measured against vendor agreements to better determine overall value.

Service Provider-Friendly Platform Simplifies Negotiations: The ION solution was designed with both enterprises and service providers in mind. The flexible architecture ensures that services and connectivity methods may be easily added or changed without the need to involve all the organizations using the service providers. Also, many of the world's largest telecom companies and equipment manufacturers, already rely on ION products to deliver secure remote services.