imprivata®

CUSTOMER STORY

NISC eliminates security risks with SecureLink

"The ability for our support reps to locally run our third-party application that is located on the customers' networks was a major success for us. We are also taking full advantage of the auditing capabilities that come with SecureLink."
– Scott Kaylor, Team Lead Network Install & Support, NISC

SUMMARY

NISC had limited visibility into who was connecting to what on their customer networks, no alerting system, and a lack of reporting capability. Now that the IT company has turned to SecureLink, they are able to enforce policy around remote access, giving their customers the power to review connections, and the capability to allow or deny them. It's a win-win for both sides – their customers are pleased because they have more control over third-party access from NISC, and NISC removed security vulnerabilities.

CHALLENGES

NISC provides an array of IT solutions to more than 750 companies. Being able to see and monitor remote access connections on their customer networks was a huge challenge for the IT company. They were using business-to-business (B2B) virtual private network (VPN) tunnels to support their customers, but this option offered limited alerting and reporting capabilities, and the related security risks were a major concern.

SECURELINK KEY BENEFITS

- Reduce security risks by eliminating B2B VPN
- Provide fully secured, world-class customer support
- Monitor and audit access to more than 750 networks

ABOUT

NISC®

National Information Solutions Cooperative (NISC) is an IT company that develops, implements and supports software and hardware solutions for telephone companies, electric cooperatives, and other public power entities. NISC has offices in North Dakota, Iowa and Wisconsin, with its headquarters in Lake St. Louis, Missouri. The company has more than 900 employees across its four locations.

www.nisc.coop

SOLUTION

They began searching for a solution that was easy to use, provided control over connections, and replaced their B2B VPN tunnel access. After looking for a solution for about five years that would work well for the company, their technical staff discovered Securelink's platform and determined that it provided NISC with the best method to support their customers. Other solutions they examined only allowed connections for applications like RDP, SSH, or Telnet. However, NISC needed the ability to add customer applications and launch these from their own desktops – and SecureLink's flexible technology provided that feature.

NISC's main objective was to find a security solution that allowed their support representatives to seamlessly integrate their existing support techniques. But they also needed to secure that process by gaining visibility into who was connecting to a customer, and what support they may be providing. Choosing SecureLink meant they were able to mimic B2B VPNs and allow access for the software application that they provided to customers.

NISC was impressed with the setup and implementation assistance SecureLink provided the company, which exceeded their turnaround expectations – and saved the company around 1,000-plus man-hours of configuration time. Within just a couple of months, gatekeepers were installed at all 750-plus NISC customer sites. After that, all they had to do was train their support groups on how to utilize SecureLink to connect to and support customers.

RESULTS

SecureLink was a change for the employees, but they've embraced it. Previously, they had only used VPNs. SecureLink provided support personnel with an efficient way to utilize familiar tools, such as WebEx, while increasing NISC's control over access. In fact, they reduced 1,500 endpoints having access to VPN tunnels, down to just a handful of business servers needing direct B2B VPN tunnel access to their customer servers.

The ability to open up a range or group of ports to a customer server and locally run their third-party application was perhaps the most valuable feature of the SecureLink platform for NISC. Other technologies they explored were not able to run their third-party application locally.

> "I think the ability to open up a range or group of ports to a customer server is the most important feature of SecureLink." – Scott Kaylor, Team Lead Network Install & Support, NISC

Before SecureLink, there was no alternative way for the company to remotely access security-conscious customers who refused to have an open VPN from their network to NISC. After putting SecureLink in place, they are able to put existing customers' security concerns at ease. They are also finding it easier to acquire new customers, due to the robust IT environment SecureLink provides the company.

NISC has also taken full advantage of the auditing capabilities that SecureLink offers them. With security the IT company's main focus, having wide open, unmonitored access to their customers' networks posed liability issues. Now that they have eliminated VPN access, the company has fast, audited access to their customers' networks – with limited security and liability risks.

NISC can now show their customers that they are looking out for their best interests. SecureLink enables them to provide world-class customer support, while keeping security top of mind.

About Imprivata

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com