Pulse Secure®

Entegrus strengthens security posture with Pulse Secure's Secure Access Solutions, enabling seamless, transparent user access for energy distribution

Summary

Company: Entegrus

Industry: Energy Distribution

Technology Challenges:

Strengthen security posture whilst reducing complexity of managing a growing number of mobile users and remote infrastructure

Solution:

- Pulse Secure 5000 series appliances
- Pulse Policy Secure
- Pulse Connect Secure

Results:

- Seamless integration between SSL VPN and NAC for reliability and easy deployment
- In line with best practice guidance from leading industry governance bodies
- Host checking and integrated sign-on makes upgrade transparent to user base

ENTEGRUS™

Ensuring the right balance of security while maintaining flexible access to network and application resources is an essential requirement for utility providers. Within such a highly regulated and nationally critical environment, best practices dictate a constant cycle of security review and strengthening to meet an increasingly potent threat posed by cyber criminals. For stretched IT departments, Pulse Secure's Secure Access Solutions are designed to solve the challenges of access control, SSL VPN, mobile device management, and IoT security, using a unified and highly integrated policy driven platform.

Challenge

Entegrus brings electricity, renewable energy and water services to 60,000 customers in Canada's southwestern Ontario region, while keeping safety, reliability and efficiency top-of-mind.

The company's subsidiary highly focused on electrical distribution, Entegrus Powerlines, provides safe, sustainable and reliable power to Entegrus customers in the communities of Chatham-Kent, St Thomas, Strathroy, Mount Brydges, Parkhill, Dutton and Newbury. The company provides billing services, meter reading, customer service support for billing and account queries, and a 24/7 automated and online service to access account balances and payment history.

Reliable and secure IT is a critical component in the delivery of its energy and data services but can become a challenge for the 5-person IT team charged with covering **three primary sites**, several large customer sites that have embedded IT systems plus an increasingly mobile workforce – across an area spanning 2300 Sq miles. As Dave Cullen, Manager of Information Systems for Entegrus explains, "Getting to some of our sites is often a three-hour round trip drive which means security and connectivity are a vital requirement for our staff and teams. As a critical utility, we need to ensure that our systems are protected to the highest levels at all times."

Solution

Entegrus has always maintained philosophy to adhere to best practice security guidance as defined by standards such as NERC and NIST. As a result, Cullen and his team have regular review sessions that evaluate current security posture along with assessing potential process changes and new technologies that can further strengthen its position.

"The threat landscape is continually evolving, forcing us to always consider how we can go one step further," says Cullen. "With a widely distributed IT infrastructure, we considered Network Access Control as an effective way to improve our security posture without dramatically altering how we operate."

The 2018 merger of Entegrus and St. Thomas Energy also highlights a wave of consolidation within the sector which also has security implications. "We needed to make sure that our secure access technologies could adapt to both new regulatory requirements as well as business drivers like the recent merger which grew our customer base by around a third plus adding 28 more staff members."

Entegrus has a long-standing relationship with Pulse Secure. The level of integration between the SSL and NAC and the extended feature set made it a straightforward choice for us," says Cullen.

Results

The upgrade uses high-performance Pulse Secure appliance series running Pulse Policy Secure. Each purpose-built appliance provides Entegrus with a single point of convergence for managing the secure network connectivity and access challenges across its fixed and mobile workforce. In conjunction with the Pulse Secure Client, the Pulse Secure Appliances lower OPEX and CAPEX by reducing the number of appliances and servers needed to deliver and control secure network access regardless of a user's location or device.

Cullen and his team use Pulse Policy Secure to automate the device validation and access rights as part of an integrated connectivity process deployed to all users and remotely managed devices.

Cullen highlights a number of benefits including a simplified method of managing complex policies and user access rights plus an enforceable method of checking end-point devices to ensure that only properly patched operating systems are able to connect to the network. In addition, the tight integration with its existing Juniper estate makes provisioning of SSL based VLANs a simple and scalable policy driven process.

"Perhaps the two most important things is that we have increased our security posture and for the most part, there has been zero impact on our end users," explains Cullen.

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net

VERSION CS 032918