SB Energy

Powering Up Secure Solar Energy Networks with Versa Unified SASE: An Inside Look with SB Energy

INDUSTRY

Energy

CHALLENGES

- Solar plants require an upload of detailed power generation data to the cloud
- Off-takers monitor solar plant operations and provide curtailment orders to increase or reduce energy production
- All of this requires secure real-time communications with the plants' SCADA systems
- Staff and third-party contractors needed to remotely monitor operations of each plant from headquarters or from remote work sites around the world

RESULTS

- **A more secure way to connect** SB Energy's power plants to cloud applications, headquarters, and external contractors
- **Secure internet access** for employees and contractors working at head offices or working remotely
- **An integrated platform and a unified set of policies** from the combined network and security capabilities delivered by Secure SD-WAN, Zero Trust Network Access (ZTNA), and Internet Security
- **Minimized risk around third-party contractors** connecting to plant systems
- **An improved security posture, simplified administration,** and the opportunity to explore unified SASE for IoT plans

Background

SB Energy is building a better future now. Founded in in 2019 and backed by SoftBank Group and Ares Management Corporation, the company is a leading utility-scale solar, energy storage, and technology platform. SB Energy currently owns and operates 2 GW of solar energy generation capacity and is experiencing rapid growth. Cybersecurity and networking are critical components to ensure maximum energy production, and SB Energy underwent a transformative journey by implementing a unified Secure Access Service Edge (SASE) solution.

Security and Connectivity Challenges for SB Energy

Secure Communications Between Plants and Azure Cloud

To monitor power plant performance, SB Energy's solar plants upload detailed power generation data to their Cloud. Additionally, off-takers also monitor solar plant operations and provide curtailment orders for SB Energy to increase or reduce energy production. All of this requires secure real-time communications with the plants' SCADA (Supervisory Control and Data Acquisition) systems.

Securing reliable connectivity to SB Energy's plants posed a challenge, given that employees operate from remote locations where VPN access to project sites is often problematic. The company had designed a dual-circuit architecture that leveraged a broad set of connectivity options, including:

- Direct internet access (where available)
- Wireless (LTE, including the FirstNet first responder network)
- Point-to-point cell towers
- Satellites

Even with this robust architecture, there were still risks. Moreover, visibility into network availability was not trivial as it increased the complexity and time to troubleshoot connectivity problems. Lastly, while plant data was encrypted before it was sent to Azure, the company sought additional steps that would further secure communications.

Secure Communications Between Users and Plants

SB Energy staff and third-party contractors needed to remotely monitor plant operations of each plant from headquarters or from remote work sites around the world. While the company had implemented a VPN solution to provide remote access to each plant, the complexity of using different certificates along with a

non-unified architecture increased complexity for SB Energy staff and third parties. Often, users had to reinstall their entire VPN software each time they wanted to connect to a different solar plant. This led to diminished productivity for SB Energy's end users.

Furthermore, the company sought to minimize risk around third-party contractors connecting to their plant systems, given SB Energy does not have full control over the security hygiene of these organizations or the device security of the individuals who were connecting. If a contractor with a compromised device connected to one of their plants, it could compromise the entire plant network.

Secure Communications Between SB Energy Staff and the Internet

SB Energy staff needed to access the internet while working at the company's headquarters or working remotely. Recently discovered cyber-attacks against U.S. critical infrastructure and military installations made it imperative to secure SB Energy staff when they accessed the internet.

Transforming SB Energy's Networking and Security with Unified SASE

SB Energy sought a better, more secure way to connect the company's power plants to their cloud applications, headquarters, and external contractors. While SB Energy initially looked at a Zero Trust Network Access solution from a well-known provider, the company felt that this solution would not help address the network reliability issues they were facing and would be challenging given the vendor's lack of support for securing IoT devices.

SB Energy, working with Versa, realized that the combined network and security capabilities delivered by a unified SASE solution from Versa Networks could address multiple requirements. The Versa Unified SASE platform offered a portfolio of capabilities, including Secure SD-WAN, Zero Trust Network Access (ZTNA), and Internet Security, all delivered from an integrated platform managed via a single pane of glass and a unified set of policies.

"The potential of these measures to accurately identify communication protocols and promptly mitigate unauthorized or harmful communications enhances IoT security within SB Energy's solar projects."

Syed Abidi
SB Energy's manager of cybersecurity and network operations

Versa SD-WAN: Secure and Reliable Network Connectivity from Solar Plants to Azure Cloud

SB Energy has deployed Versa Secure SD-WAN to provide secure and reliable network connectivity between their solar plants and their applications in the Azure Cloud. Benefits include:

- Resiliency: The SD-WAN solution provides dual circuit resiliency across multiple types of internet transports at different sites, including cellular LTE and satellite. Circuit failures, brownouts, and link flaps are seamlessly dealt with by the SD-WAN overlay providing transparent failover and dynamic connection optimization.
- Less Troubleshooting: With intelligent network optimization and automation, as well as support for remote monitoring and administration, the SD-WAN solution has significantly reduced the troubleshooting burden on the network team.
- Enhanced Security: Communications security between plants and the Azure Cloud has been improved by utilizing the SD-WAN's secure, encrypted tunnel capabilities to augment the data encryption already in place.

Versa Secure Private Access: Zero Trust Network Access for User-to-Plant Connectivity

SB Energy has deployed Versa Secure Private Access (VSPA) to provide Zero Trust Network Access to SB Energy plant networks for employees who need to remotely manage the plant, as well as third party contractors that need to monitor the plants on behalf of off-takers. This capability is used by employees working onsite at SB Energy headquarters, as well as remote or travelling team members. With employees travelling around the world, SB Energy has set up gateways in North America, Europe, and Asia. So now anywhere employees travel, they can connect to those gateways and be able to log into these plants in the U.S. seamlessly. Benefits include:

- **Seamless Zero Trust Network Access:** By replacing their legacy VPN solution with Versa's ZTNA solution, employees and contractors can now quickly and seamlessly access SB Energy plants from HQ or remote locations.
- **Reduced Troubleshooting:** Elimination of client certificate problems and overall reduced administrative burden to provision and troubleshoot legacy VPN secure access.
- **Improved Security Posture:** Implementing a Zero Trust approach to plant access improves overall security by enforcing granular access policies and continuously monitoring device security posture.

Versa Secure Internet Access – Cloud Security for SB Energy Staff

Versa Secure Internet Access (VSIA) provides cloud-delivered security for SB Energy's employees when they access the internet, whether they are working in the office or remotely. Specific security components deployed by the company include:

- **Secure Web Gateway (SWG) and Cloud Firewall as a Service (FWaaS)**, used for internet filtering and malware protection.
- **Cloud Access Service Broker (CASB),** used for access control and data protection for SaaS applications used by SB Energy.
- **Data Loss Prevention (DLP),** used for inspection and control of sensitive data leaving the organization, including data going sent to Generative AI tools like ChatGPT.

Benefits include:

- **Unified Security:** Versa's integrated SSE solution delivers comprehensive internet security for SB Energy employees, no matter where they are working.
- **Simplified Administration:** The administration burden for SB Energy's IT staff is significantly reduced with a solution that consolidates multiple point products into a single platform. Versa's solution provides visibility and control through a single pane of glass, and unified security policies for every session for every user, on any device, accessing any application.

According to Hemen Mehta, VP, North America Partner Sales for Versa, "We want to congratulate SB Energy on their successful implementation of a comprehensive SASE solution. Their commitment to embracing the full range of SASE functionalities highlights their forward-thinking approach to network and security management. We are proud to partner with organizations like SB Energy who share our vision for a more secure, agile, and connected future."

Future Directions – Exploring SASE for IoT

During the initial stages of collaboration with Versa, SB Energy focused on establishing secure networking across users, devices, locations, and cloud applications. SB Energy has identified additional opportunities to utilize Versa's Unified SASE platform. This involves implementing micro segmentation and bolstering IoT security through the integration of Versa's advanced Next Gen Firewall (NGFW) and Zero Trust LAN architecture (Secure SD-LAN). According to Syed Abidi, who leads SB Energy's cybersecurity and network operations, "The potential of these measures to accurately identify communication protocols and promptly mitigate unauthorized or harmful communications enhances IoT security within SB Energy's solar projects."

Conclusion

SB Energy, a major renewable energy company, recognized the critical importance of enhancing its cybersecurity amidst rising cyber threats. By integrating Versa's Unified SASE solution, the company not only fortified the security of its communications between its solar plants, Azure Cloud, headquarters, and third-party contractors, but also improved the reliability and efficiency of its network connectivity. The comprehensive approach has reduced troubleshooting efforts, enhanced secure access for remote users, and provided robust internet security for all staff. With potential future endeavors in IoT security, SB Energy continues to prioritize innovative solutions to safeguard its operations.

About SB Energy

SB Energy is a leading utility-scale solar, energy storage, and technology platform operating solar plants across the United States. As part of the nation's critical energy infrastructure, cybersecurity is a top priority. The company recently deployed Versa SASE to enhance the security of their networks connecting their plants, cloud applications, headquarters, remote users, and vendors. Specifically, SB Energy uses Versa to support the following use cases:

- SDWAN for WAN traffic security and reliable connectivity between plants and Azure Cloud
- Zero Trust Network Access for secure plant access by employees and vendors
- Internet security for solar plants
- Internet security for enterprise users (headquarters and remote users)
- Internal communication security for vendors accessing SB Energy resources

VERSA NETWORKS

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com