SXi CyberCare Access™

Maintaining and optimizing Cybersecurity via NSA Approved Commercial Solutions for Classified technologies

Allowing remote access to your installation's IT resources can be risky, whether cloud-based, on-premises, or hybrid deployment. SecureXperts CyberCare Access provides password-free credentialed access to your staff using Department of Defense-approved methods to secure access to your environment from any geographic location seamlessly and securely.

SecureXperts Incorporated
NASA Astronauts Memorial Foundation
Kennedy Space Center FL 32899
Phone: 888-804-4674
Email- admin@securexperts.com

Despite its benefits, most IT admins and Cyber Risk Management are wary of remote access. To address these concerns, the SXi CyberCare Access™ service uses immutable encryption and trusted devices, giving authorized third-party vendors, contractors, and administrative personnel auditable permission to enter secured networks through secure access points.

Using a decentralized solution, CyberCare Access™ ensures strict separation between your networks and outsiders using Private cellular LTE network technology.

Our US-based personnel have security clearances up to and including Top Secret. We work vigilantly to protect you and our nation's most critical assets 24/7/365.

SXi CyberCare Access™ is rigorously tested to safeguard against unauthorized penetration and meets regulatory requirements, including NIST 800-53 and proposed Department of Defense mandates for Safeguarding Controlled and Unclassified Defense Information.

Our on-premises and hosted options comprise flexible engagement models that can meet your needs, ranging from localized on-premise solutions to enterprise commercial and other high-risk critical computing environments.

SecureXperts CyberCare Access™ can seamlessly integrate into your Systems Development Lifecycle Plan without replacing existing components.

Your Mission is our Focus

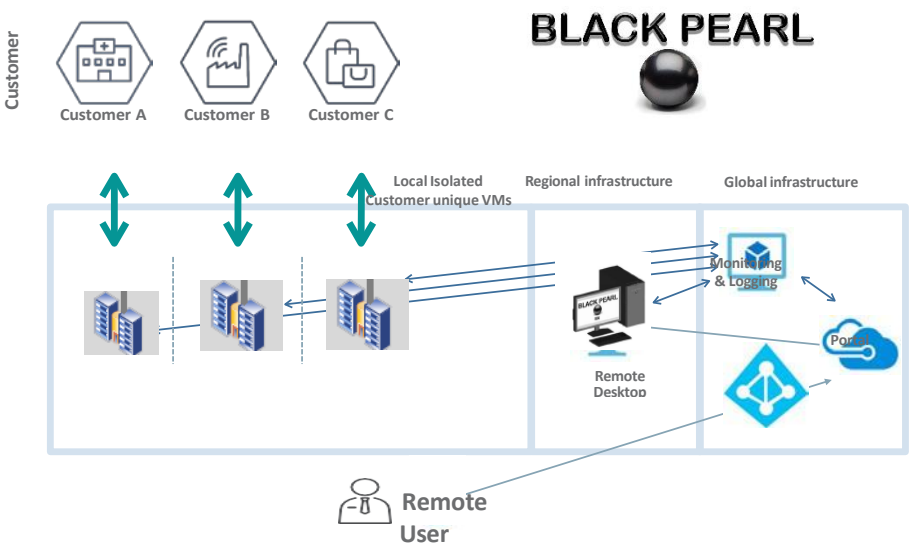
SXi CyberCare Access™

Typical Configuration Models

1. **Client VPN**
2. **Site-to-site VPN**
3. **Ad Hoc-Remote**

Users are authenticated by two-factor authentication, which consists of a Smart Card and PIN. Dual Encryption tunnels provide secure access using privatized cellular network connections inaccessible to traditional Wi-Fi or wired access.

CyberCare Remote Access Architecture



Configuration method 1:

Client Virtual Private Network

Client (VPN) in the virtual workstation within the remote access network. The virtual workstation is accessed via a web browser using the secure HTTPS communication protocol through a Smart card with secure digital certificates bound to the individual user. A virtual session is then used to access those services in the customer network managed by your IT staff. The virtual workstation is isolated and can only communicate with a specified customer's network. Communication with the customer's network is only permitted once the SecureXperts support engineer authenticates himself/ herself via the two-factor authentication portal.

Configuration method 2:

Site-to-site VPN

This method configures a site-to-site Virtual Private Network (VPN) link between the remote access system and a customer network. A virtual session is created via a virtual machine or web browser using the secure HTTPS communication protocol. Using a double encrypted tunnel, it uses a zero-trust network configuration to connect to those services in the customer network managed by your company. The virtual session is isolated and can only communicate with a specified customer's network.

Configuration method 3

Ad-Hoc Remote

Communication with the customer's network is only permitted through the isolated virtual workstation once the user successfully authenticates himself/herself via the two-factor authentication portal. The support engineer authenticates himself/herself with a username, password, and a one-time password.

- Following successful authentication, the SecureXperts support engineer is presented with a portal containing links that connect exclusively to the specific systems for which authorization has been granted.
- When the SecureXperts support engineer accesses one of the links, the support engineer is granted access by the portal to the virtual machine uniquely set up for the specific customer.
- The audit logs are captured for each customer and provided as needed to identify trusted connections and activities (without capturing any client data).

SecureXperts, Incorporated, "SXI", founded in 2001 by a team of industry experts in cybersecurity, is recognized as an industry leader in the evaluation of cyber security posture for cyber-physical systems used in critical infrastructure protection such as the energy and power grid industrial control systems, healthcare, Military, law enforcement and financial sectors to name a few.