

Features

- User-friendly remote access to IEDs and other devices
- Comprehensive NERC CIP access controls
- Works with Magnum DX, DynaStar, dial-up port switches and other network devices
- Integrates with Enterprise authentication systems: RSA SecurID and Active Directory
- Extensive activity logging, reporting and audit tools

CROSSBOW

Secure Access Manager

CrossBow™ Secure Access Manager is both a productivity tool for workers requiring remote access to industrial devices and an access security management tool, focused on utility compliance with NERC CIP cyber security standards.

CrossBow provides user-friendly access to Intelligent Electric Devices (IEDs) and other remote devices via a PC-based client or web interface. The user interface organizes permitted devices by name, type, location, sector or other criteria and then enables one-click access to administrative interfaces. The CrossBow client launches vendor-specific software applications automatically. Device profiles are established for many SEL, GE, ABB, Areva and other vendor devices, and the architecture is open to virtually any other device with a remote administrative interface, providing access as if local to the device console port.



NERC CIP cyber security standards compliance is a specific focus of CrossBow, with an emphasis on both completeness and ease-of-implementation. All connections to remote devices are authorized via CrossBow Secure Access Manager and all user sessions are logged. Administrative tools make it easy to set up and centrally control security and access profiles based on an individual person and their functional or organizational role, and by individual devices and device location or category. Reporting tools facilitate administration tasks and compliance auditing. CrossBow optionally integrates with other enterprise systems, including RSA SecurID and Active Directory for user authentication.



CrossBow has an open system architecture that supports many network types and vendors, including leading dial-up port switches, Serial-IP terminal servers and router/firewalls. As part of GarrettCom's Magnum Secure Networks Framework, CrossBow integrates with Magnum DX and DynaStar routers and serial device servers to provide a comprehensive Electronic Security Perimeter at power utility substations or other harsh industrial environments. IP Firewall, stateful logging, IPsec Virtual Private Networks (VPNs), and SSL/SSH encryption are among the integrated electronic perimeter security tools. CrossBow provides integrated security management of these remote network devices, including retrieval and central storage of log files for future audits or forensics.

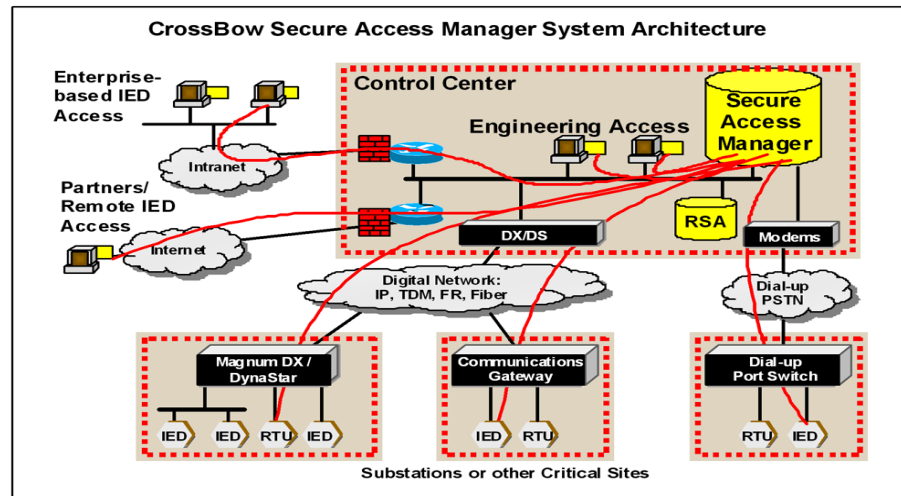
The CrossBow system architecture consists of distributed clients on end-user computers, a central control communications and management server, and secured communications to remote target devices via secure networking gateways.

PC-based clients provide a Windows-like directory structure of authorized remote devices, arranged in flexible directory structures sortable by type, location, control domain or other factors. Target devices have icons and descriptive names. A single click launches the appropriate local application software for use with the particular target device and makes what appears to be a transparent network connection, as if to the local device console port.

All client communication is routed to a central communications server. These connections are secured via SSH. Upon first connecting, each user is authenticated by the server. Optionally authentication may be integrated with Enterprise authentication mechanisms such as Active Directory. Two-factor authentication may be provided using an interface to an RSA SecurID server.

The CrossBow server maintains individual profiles for each user and only permits network connections to authorized devices.

Connections from the CrossBow server to end devices are transparent to the end user. These connections are secured using various secure networking techniques, depending on the specific gateway used. CrossBow certified gateways include the GarrettCom Magnum DX and DynaStar families of router/firewalls and terminal servers, with options for secure communications and enhanced management interfaces with the CrossBow server for provisioning and log archival. Other supported gateway devices include Bow Networks' eLAN Substation Communications Server, SEL PRTU/2020/2030/2032 and Teltone Gauntlet Gateway.



©2009 GarrettCom, Inc. Printed in United States of America Doc No. CrossBow-R2 03/09
 GarrettCom, Inc. reserves the right to change specifications, performance characteristics and/or model offerings without notice. GarrettCom is a registered trademark of GarrettCom Inc. Magnum, Dymec, DynaStar, Personal Switch, Link-Loss-Learn, S-Ring, Convenient Switch and Converter Switch are trademarks of GarrettCom, Inc. NEBS is a registered trademark of Telcordia Technologies. UL is a registered trademark of Underwriters Labs. CrossBow is a trademark of Bow Networks. RSA is a trademark of RSA Security. Gauntlet is a trademark of Teltone.



GarrettCom®

Industrial Networking at Its Best™

GarrettCom, Inc.

47823 Westinghouse Drive

Fremont, CA 94539

PH: (510) 438-9071

FAX: (510) 438-9072

Email: mktg@garrettcom.com

Web: www.GarrettCom.com