

### Securing Remote Site Access: A Defense-in-Depth Approach

Todd Nicholson, Chief Marketing Officer  
Industrial Defender

Our nation's resources, as well as our interconnected global economy, depend on the security of our critical infrastructure systems, which include the power, oil and gas, transportation, water and chemical industries. And yet, despite the grave potential social and economic consequences of a critical infrastructure security breach, these systems face growing risk from cyber security threats that are doubling each year.

Why? The need for real-time business intelligence has spurred changes in the critical infrastructure environment that, while resulting in increased convenience, have also increased cyber security risk.

Remote sites present a unique security challenge in that they are often in relatively isolated locations, and therefore not readily accessible as they are frequently unattended and remotely operated. In addition, many remote sites use legacy equipment (intelligent electronic devices, meters, etc.) that support aging protocols, and may be accessible only via dial-up telephony. Further, these devices were first and foremost designed with production and operational resiliency as top priorities and security second.

#### Security of Legacy Systems

Traditionally, the security of legacy industrial control and Supervisory Control and Data Acquisition (SCADA) systems was inherent in their forced separation. By "air gapping" the systems, the plant environment was purposely disconnected from the enterprise, creating an island of protection for mission-critical equipment.

Industrial control and SCADA systems were typically used by the control automation experts in the plant or factory; management interested in obtaining data from this environment had to pick up the phone or read the information from a hard copy report. This has all changed due to increased global competition as well as regulatory compliance requirements which have driven the need for real-time industrial control system data to enable timely strategic business decisions.

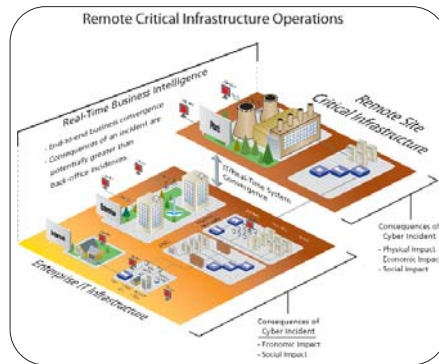
Today, critical business data and information extracted

from the industrial control system environment is being used to maximize production lifecycles, profit margins and the return on corporate assets.

Thus, the need for the convergence of both enterprise IT and industrial control system and SCADA domains has emerged as both a necessary — and dangerous — initiative in terms of cyber security protection. In order to effectively protect a critical infrastructure network, developing a comprehensive defense-in-depth security strategy is no longer an option, but rather a critical requirement.

#### Performance Challenges and the Increased Use of Remote Access Methods

It is essential that the plant environment is both reliable and accessible. Without exception, plants must operate reliably 24x7x365. Remote access methods including virtual private networks (VPN), dial-up technology and terminal servers enable flexible remote access to be more conveniently achieved.



Previously, when the majority of plants were purposefully air-gapped, there was no real need to provide remote access capability to support the plant network. Today, with an increase in resource constraints of plant operations staff and a shortage of qualified industrial control system and SCADA expertise, some

plant employees (and even in some cases vendor personnel) are routinely allowed to remotely access the plant network. With this increased convenience and emphasis upon increased productivity undoubtedly comes the increased threat of a major cyber security breach or incident.

The requirement, then, is for a method of securing central and remote plant systems while providing convenient access to approved personnel. Current security best practices require active, real-time detection of suspicious activity, from within or outside the facility, powerful tools for management of user privileges and port access, comprehensive logging and reporting features and ongoing software updates to ensure protection from the latest malicious activity.

#### A Unified Security Strategy: Defense-in-Depth

According to a 2005 study from the UK-based company NTA Monitor, over 90 percent of remote access VPN systems have exploitable security vulnerabilities due to a lack of security best practices. Clearly, the need for a secure remote access strategy is inherent in order to effectively support any type of remote access to the plant network. The solution? A comprehensive defense-in-depth approach to cyber security effectively enables the efficient protection of the industrial control and SCADA plant network environment.

This approach begins with securing the perimeter of the network, specifying who is allowed access to the network, as well as the explicit user privileges granted to each individual user. Further, using this approach will provide end customers with the ability to maintain full control of all critical network devices while maintaining the option to outsource the security management, monitoring and reporting of those devices to experts with industrial control system and SCADA cyber security experience.

This unique method provides customers with the flexibility to augment their plant network staff and selectively choose the level of plant network control that is required depending on the customer comfort level, experience and resource availability.

Ideally, a comprehensive and fully unified defense-in-depth approach would offer comprehensive security protection via the following components:

- **UTM / Firewall Perimeter Protection**

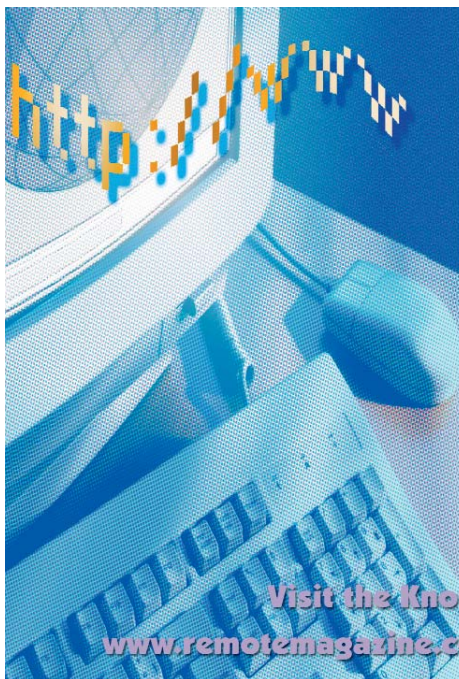
A comprehensive defense-in-depth approach to securing remote critical infrastructure sites begins with perimeter security protection. A UTM/firewall device is used for creating a boundary of the control system network to form a virtual electronic perimeter. A UTM / firewall device can be used for firewall protection, virus protection, intrusion prevention, virtual private networking, and pre-planned lockdown states.

- **Security Event Management**

A security event management appliance is used for monitoring, control, alarm management, analysis, storage and reporting of security and performance information. In addition, historical data is captured and used to generate trend graphs, reports and other data analysis functions.

- **Network Intrusion Detection System**

A network intrusion detection system is a sensor-based device which detects attacks, rogue systems and unauthorized traffic within your network perimeter. The network sensor should also proactively detect the addition of new computers to the network, for example, a contractor plugging in a



### Introducing the Remote Site and Equipment Management Online Knowledge Center

Never before has more information on remote site equipment and the industry been in one, easy to use, location!

White Papers • Web Seminars

Articles • Market Reports

Training Courses • Industry Links

Application Profiles • Literature/Text

Visit the Knowledge Center at

[www.remotemagazine.com/r\\_knowledgecenter.html](http://www.remotemagazine.com/r_knowledgecenter.html)

laptop or a new connection to a wireless access point. Since industrial control networks tend to be quite stable, it is fairly simple to detect rogue devices being connected with a NIDS sensor.

### • Host Intrusion Detection System

Host intrusion detection sensors are miniature software applications residing on control system computers used to detect control application issues, internal or external intrusions and misuse, as well as performance bottlenecks on key servers and HMI's. Security sensors are available for Unix, Windows or Linux operating systems. In addition to specific control applications, the sensors report on platform-specific information such as failed login attempts, password age, logged-in user counts, event log activity and insertion of removable media.

### • Secure Remote Communications

An effective secure remote access solution provides authorized users with transparent access to remotely located devices, while also ensuring that only individuals with appropriate credentials are allowed access to the equipment, and proactively blocking all other access attempts. All activity at each point in the system must be logged and collected at the central administrative server, for inventory management, usage analysis, fraud detection, etc., or to support regulatory reporting requirements. Management software tools should be provided for administration of user rights (especially immediate revoking of rights for problematic or former employees), specific port access for remote gateway devices, provision of certificates and password maintenance, report generation, and providing software updates to all system elements.

A decentralized architecture should be implemented for maximum resiliency; a failure of one element shouldn't affect other parts of the system. Most importantly, user access should always be available, especially in critical conditions which might require real-time configuration of remote device settings. In addition, the system should be designed to be protocol agnostic, supporting the many legacy installations as well as modern control equipment.

Roaming technicians requiring access to remote devices should be able to use their normal communications/polling application without hindrance from excessive login routines or network latency. In this scheme, they are required to occasionally download time-based, port-specific access credentials from the central host for access to secured devices for a limited time.

A fundamental component of the remote access system is the secure gateway or firewall device (either dial-up or IP based depending on the environment) which proactively blocks all access unless from authorized users possessing current security credentials and approved equipment IDs. No device ports must ever be exposed to the public network; rather they should passively "listen" for a predetermined signal, after which a multipart handshake process will grant port access.

### Conclusion

In summary, it is important to develop a comprehensive defense-in-depth cyber risk protection strategy for securing remote critical infrastructure environments. With the rapid adoption of converged corporate IT and critical infrastructure plant networks in order to drive real time business intelligence, the need for remote access capabili-

ty will continue to increase over time. Implementing a defense-in-depth approach to cyber risk protection will ensure the continuous reliability, availability, and security of your industrial control system or SCADA network as the needs of your company's business evolve.

*Todd Nicholson is responsible for leading Industrial Defender Inc.'s global marketing and product strategy. Todd brings over 16 years of experience in corporate and product marketing, product strategy, business development and sales working for emerging and mature technology companies including Digital Equipment, EMC, IBM and InfiniSwitch. Todd joined Industrial Defender from EMC, where he was responsible for directing prod-*

*uct marketing and product management for the company's grid and utility computing business unit. Todd holds a B.S. in business administration from Nichols College with a major in marketing.*

*Industrial Defender, Inc. offers a completely integrated Defense-in-Depth cyber security solution designed to protect the industrial control system and SCADA environment in a flexible and cost effective platform. Formerly known as Verano, Inc., Industrial Defender is a privately held company with over 17 years of industrial control system and SCADA industry experience, and more than 6 years of industrial cyber security experience. For more information please visit: [www.industrialdefender.com](http://www.industrialdefender.com).*

# Remote 2008

## CONFERENCE AND EXPO

SCADA, Device Networking, M2M, Wireless Technology, Onsite Power, And Security for Remote Sites and Equipment

### Expanded Exhibit Hall and Speaker Sessions Highlight Changes for 2008!

To better serve the remote site and facility market, the Remote 2008 Conference and Expo has made a few changes. First we've book the largest exhibit hall in the show's history, while also expanding the program to better serve your needs.

The largest addition to the program is an entire track, two days of sessions, covering cyber and physical security measures in remote applications. With the influx of new standards, wireless and homeland security concerns, this will be a popular topic in 2008 and beyond! Also new for the program are sessions relating to power protection in remote environments (UPS, lightning, back-up power) and sessions covering Remote Smart Services. To see our preliminary program please visit: [www.remotemagazine.com/rem08\\_program.php](http://www.remotemagazine.com/rem08_program.php). Contact Nick Depperschmidt at [nickd@infowebcom.com](mailto:nickd@infowebcom.com) or 800-803-9488 for more information.

### Recently Introduced ISA Workshops!

Practical Applications of SCADA Systems Integration  
Tuesday, November 4, 2008 - 8am - 4pm

Securing Industrial Networks: Cyber Protection for  
Automation, Control, and SCADA Systems  
Tuesday, November 4, 2008 - 8am - 4pm

Visit [www.remotemagazine.com/rem08\\_workshop.php](http://www.remotemagazine.com/rem08_workshop.php)  
for full workshop descriptions and information on how  
to register via the ISA website.

For more information about sponsoring or exhibiting contact Scott Nash at:  
[ScottN@infowebcom.com](mailto:ScottN@infowebcom.com) or 303-317-2505

NOVEMBER 5-6, 2008 - ATLANTA, GA.  
[WWW.REMOTEMAGAZINE.COM](http://WWW.REMOTEMAGAZINE.COM)