White Paper

Network Security is Serious Business

Considering all the reports of hacks and breaches, one might get the feeling that data protection measures are not all they should be. More than ever before, the products selected to protect homes and businesses is of utmost importance. The increasing availability of mobile access to home and commercial security systems via apps has escalated concerns. But based on the technology used in DMP systems and their record for maintaining reliable data security, it's clear there's someone you can trust.

Establishing Alarm Communication Over Data Networks

DMP's proven history in the high-security space began in the early 1990s with the first use of data networks for alarm panel communication, including the internet. That led to their first-ever UL High-Line Security Listings for that application.

To best protect customers in high-security applications, DMP developed a strategy called Adaptive Technology™. This exclusive feature seamlessly switches between communication links — cellular and network — with no lost supervision polling while maintaining panel substitution detection.

Furthermore, the 128-bit AES encryption — and subsequently 256-bit AES encryption — earned DMP the first NIST certification for encrypted intrusion panels. Depending on the panel programming, all alarm communication between encrypted panels and the central station receiver either use 128- or 256-bit AES encryption.

DMP's focus on system security continued into the early 2000s with the addition of commercial-grade, Two-Way Wireless technology that incorporates frequency-hopping and spread-spectrum. It changes channels every 32 milliseconds, just like many military-specified wireless radios.

This wireless technology is rock solid, and with a range of more than 1.5 miles, it sets the standard that others are measured by. In fact, that innovation qualified DMP to earn UL Commercial Fire Listings.

DMP and SecureCom Wireless™ Commit to Deliver Wireless Communication That's More Secure and Reliable

More and more clients are choosing cellular communications for their alarm systems. To provide a single source for affordable and reliable digital wireless communication for its panels, DMP created SecureCom Wireless in 2008. Rather than send alarm data to a clearinghouse where it's interpreted and retransmitted to a central station receiver over the internet, SecureCom has developed the most secure solution by working with partner cell carriers to transmit alarm signals directly from the control panel to the central station receivers. Customers appreciate a wireless system, eliminating any possibility of wires being cut by an intruder.

As wireless technology advances, so too has smart mobile technology to manage alarm systems. As DMP develops apps and browser interfaces, they've taken the most conservative approach. They adhered to internet security industry standards and designed both the architecture and the logic of solutions to incorporate security at every step. For internet connections from SecureCom servers to the Virtual Keypad app or browser, DMP uses Transport Layer Security TLS 1.2. This protocol encrypts data to ensure that eavesdroppers and hackers are unable to see what is transmitted.

"We take the security of our equipment and our apps and software very seriously," says DMP Vice President of Product Design Jeff Britton. "From the architecture of the hardware to the implementation of the software and maintenance of our servers, security is at the forefront. You can count on that."

The reliability of the SecureCom Wireless services is key. To check the status, go to: Status.SecureComWireless.com.

Taking Steps to Ensure Security Over the Internet

Between DMP and SecureCom Wireless, the list of features they've implemented to ensure the security of their Cloud-based solutions is extensive. All SecureCom cameras and NVRs use a Virtual Private Network (VPN), for instance.

Using a VPN ensures that live video sent to SecureCom servers via the internet remains private. Otherwise, in order to have access to their live video over the internet, customers would need to open a port and map it to their cameras and NVRs. Known as port forwarding, this establishes a direct connection between two parties in which one or both are behind commercial or residential firewalls. Although it's a common technique, customers can be vulnerable to hackers who find those open ports and gain access to those mapped devices.

That potential for vulnerability doesn't fly with DMP and SecureCom Wireless. That's why a VPN is standard protocol, not only for all SecureCom cameras and NVRs, but also some compatible Digital Watchdog cameras.

Encryption is a Crucial Factor When it Comes to VPNs

A VPN offers unrivaled security and privacy because it encapsulates and encrypts the traffic before it's sent over the internet to another network, thus keeping the user data secure and private. Data from the client's camera or NVR is not decrypted until it's received by SecureCom's servers.

A VPN is one of the most essential tools, not only for businesses but also homeowners. DMP is one of the only security companies that leverages a VPN in its video product offering.

Other Cloud-based solutions that DMP employs:

- 10-character app and browser passwords, with complex combination of non-alpha characters required
- Three invalid codes entered will log users out
- Video stream IDs frequently change, with URLs randomly generated at time of viewing
- Panel user code, email address and password two-factor authentication via a user code or fingerprint (2FA) on both iOS and Android apps required for login
- Touch ID supported as an option to launch the app
- Account enumeration prohibited
- 2048-bit RSA and 256-bit AES used for encryption
- No user feedback provided to users regarding email address validity
- DMP hardware and software is readily updatable
- Third-party scheduled penetration testing
- Active monitoring and patching of all discovered vulnerabilities and malware

Encrypt Network Remote

If encrypted data is a priority, the Encrypt Network Remote option on XR Series™ control panels should be enabled. This ensures that all communication from Remote Link™ to the panel or from the SecureCom servers to Virtual Keypad always uses AES encryption.

Tier 4 Data Centers

In today's digital world, mobile security is paramount. That's why for the security and redundancy of its servers and all SecureCom Wireless network assets, DMP employs the highest standards and works only with the most highly rated data centers.

SecureCom's primary assets are located within Tier 4 data centers in Dallas, Texas, and St. Louis, Missouri. Tier 4 is designed to host mission critical servers and computer systems with fully redundant subsystems (cooling, power, network links, storage, etc.) and compartmentalized security zones controlled by biometric access controls methods.

SAS/SOC Compliance

As a Tier 4, this data center’s security controls of its Cloud Services are rated “Enterprise Ready” by SkyHigh Networks, a designation which fully satisfies the most stringent requirements for data protection, identity verification, service security, business practices and legal protection. Additionally, these data centers maintain SOC 1 Type 2 and SSAE 18 compliance.

DMP also conducts off-site backups of its critical data to a secondary provider in Texas. Furthermore, SecureCom Wireless assets have N+1 electrical and environmental redundancy. The Secure Com data center has an on-site Network Operations Center that monitors the SecureCom environment and assets 24/7/365.

SecureCom Wireless also has network, security and system administrators on call around the clock 365 days per year. All networking hardware, database servers and general server infrastructure are high availability and load balanced to provide optimal connectivity. SecureCom Wireless also employs a unique hardware solution to mitigate DDoS — or global denial-of-service attacks.

Continuous Pen Testing

Every quarter, SecureCom Wireless completes third-party pen testing by a PCI/DSS-approved scanning vendor, and much more frequently, in-house pen testing is completed. Routine patches are applied to all assets monthly, and critical patches are applied much more frequently.

There’s no question that digital security should not be taken lightly or ignored. Hackers are intent on breaking into systems, whether to collect data, commit online vandalism or worse. Whether protecting home and family, retail establishments, professional spaces, bank chains or government facilities, DMP and SecureCom Wireless technology provide some of the most secure solutions available.

For additional information about server and data security, please contact a member of SecureCom Wireless or DMP’s technical team at 877-300-8030.

About DMP:
DMP is a privately held, independent manufacturer of innovative intrusion, fire, access control, network and cellular communication products designed, engineered and manufactured in Springfield, Mo., using U.S. and global components. DMP is the recognized leader in alarm communication over data networks, with products that are available through professional electronic security companies. For more information, contact Mark Hillenburg at MHillenburg@DMP.com or visit DMP.com.

About SecureCom Wireless:
SecureCom Wireless is a privately held company and offers dedicated cellular service to professional alarm companies, central stations, banks, retailers and other customers with DMP alarm systems. Plans are based on estimated data usage from the panel to the monitoring station and from the panel to the cell phone. Different plans are available based on various applications, including simple alarm communication to full support for the Virtual Keypad app, Z-Wave® devices, cameras, push notifications, traffic count and more. For additional information, visit SecureComWireless.com or contact SecureCom Wireless at 877-300-8030.

DMP®
866-266-2826
DMP.com
INTRUSION • FIRE • ACCESS • NETWORKS
2500 North Partnership Boulevard
Springfield, Missouri 65803-8877