



## Reducing cybersecurity risk is critical. Eaton can help.

Eaton takes cybersecurity seriously. That's why we've developed a network card that has enhanced protection built-in. The Gigabit Network card is the first in the industry to meet both International Electrotechnical Commission (IEC) and Underwriters Laboratories (UL) cybersecurity requirements. The card was the first UPS network connectivity device to receive UL 2900-1 certification, which provides customers with confidence that it has been reviewed, tested and met the benchmark of this trusted brand. It is also the first to be certified to the IEC 62443-4-2 standard, which further underscores Eaton's commitment to unified global cybersecurity standards. While hardware that lives behind a firewall is thought of as fully-protected, that isn't always enough to keep hackers out.

### What's the benefit to customers?

Encryption and Password management are the two key enhancements that make Eaton a leader in this space.

#### Encryption

- ✓ Uses the most current version of Transport Layer Security protocol (TLS)
- ✓ Only secure protocols enabled by default
- ✓ Firmware is signed and encrypted, and will not boot if tampered with
- ✓ Secure SMTP for email alerts



#### Password Management

- ✓ Requires change of password on setup
- ✓ Configurable requirements for password complexity
- ✓ Certificate based authentication in machine to machine connections – no username/password information saved on the client machine, separate certificates for each protocol

### How can Eaton partners benefit?

The ability to sell a unique product and generate more revenue is ideal for Eaton partners.

- ✓ Leverage the unique advantage over competitors as Eaton is the first and only in the industry with a UL certified, cybersecurity-rich network card
- ✓ Generate revenue when you upgrade your customer's 5P, 5PX, 9PX, 9SX and 9PXM UPSs with this network card for added cybersecurity
- ✓ Add more value to customers and create new revenue streams with service and configuration of IPM for customers seeking enhanced business continuity
- ✓ Gigabit Network card will be standard on most UPS network bundles
- ✓ Monitor and manage power within large environments with Eaton Visual Power Manager (VPM)

## Beyond enhanced cybersecurity, what does this card feature?



**Gigabit speed** for compliance with networking equipment and gigabit only datacenter networks



**Compatibility with Eaton Intelligent Power manager** (IPM) v1.61 or higher and several Eaton UPSs



**Connected devices** can be rebooted remotely with load segment controls automatically, or on a schedule



**Reduced setup time** and enables compatibility without changing port settings on the network switch



**Enhanced UPS capabilities** – The UPS can be linked to other systems with the network card, thereby creating a system that can be used to save costs or provide additional functionality



**Self-setting, real-time clock with battery backup and linkage to NTP (Network Time Protocol) server** ensures accurate reporting of event history



**Additional memory** allows storage of current and prior firmware versions

### What is UL 2900-1?

With more connected devices than ever, Underwriters Laboratories (UL) understands that there is increasing risk of cybercrime occurring through network connected devices. UL has developed this standard to assess the vulnerability of connected devices to known malware/exploits and protect business from these risks. **The UL 2900-1 certification is UL's global standard for connected device cybersecurity.**

Products tested undergo extensive testing, including static code reviews, vulnerability assessments and risk mitigation capabilities. The Eaton Gigabit Network card was assessed for SSH, SNMPv3, NTP, SMTPS, DHCP and MQTT via TLS 1.2.

### What is IEC 62443-4-2?

Like UL, IEC has developed standards to help safeguard against cybercrime. Within the IEC 62443 standard are several subsections, including IEC 62443-4-2, which specifies guidelines for network component suppliers to enhance security, including account, identifier and authenticator management, password-based authentication, public key authentication, use control, data integrity and confidentiality, as well as backup for resource availability. **Suppliers who follow this set of guidelines will equip operators with the best chance of protecting their networks against cyber attacks.** However, not following the guidelines leaves the network less secure and more vulnerable to malicious attacks.

For more information, please contact:

CHANNEL DEVELOPMENT  
MANAGERS  
877.233.8519

To learn more, visit  
[Eaton.com/Network-M2](http://Eaton.com/Network-M2)