General Information

Cooper Lighting Solutions views security as a cornerstone of a safe, dependable and reliable electrical system. Accordingly, the Trellix System employs current industry best practices to reduce, identify, contain and manage security risks. Trellix has been designed and engineered with security as a key requirement with flexibility to accommodate improvements if new security attack surfaces are identified. This product is developed under Cooper's Secure Software Development Lifecycle process, which is monitored and gated by the Cooper Lighting Cybersecurity Center (CLSC) team. The CLSC team provides full security assessment of the product, supports the ongoing vulnerability & threat detection and notification to the development teams.

Trellix platform uses a multi-tiered approach to addressing industry best practices for security risk management and utilizes guidelines derived from IEEE, IEC, NEMA, DoD, and UL2900 to achieve a secure and adaptable IoT platform.

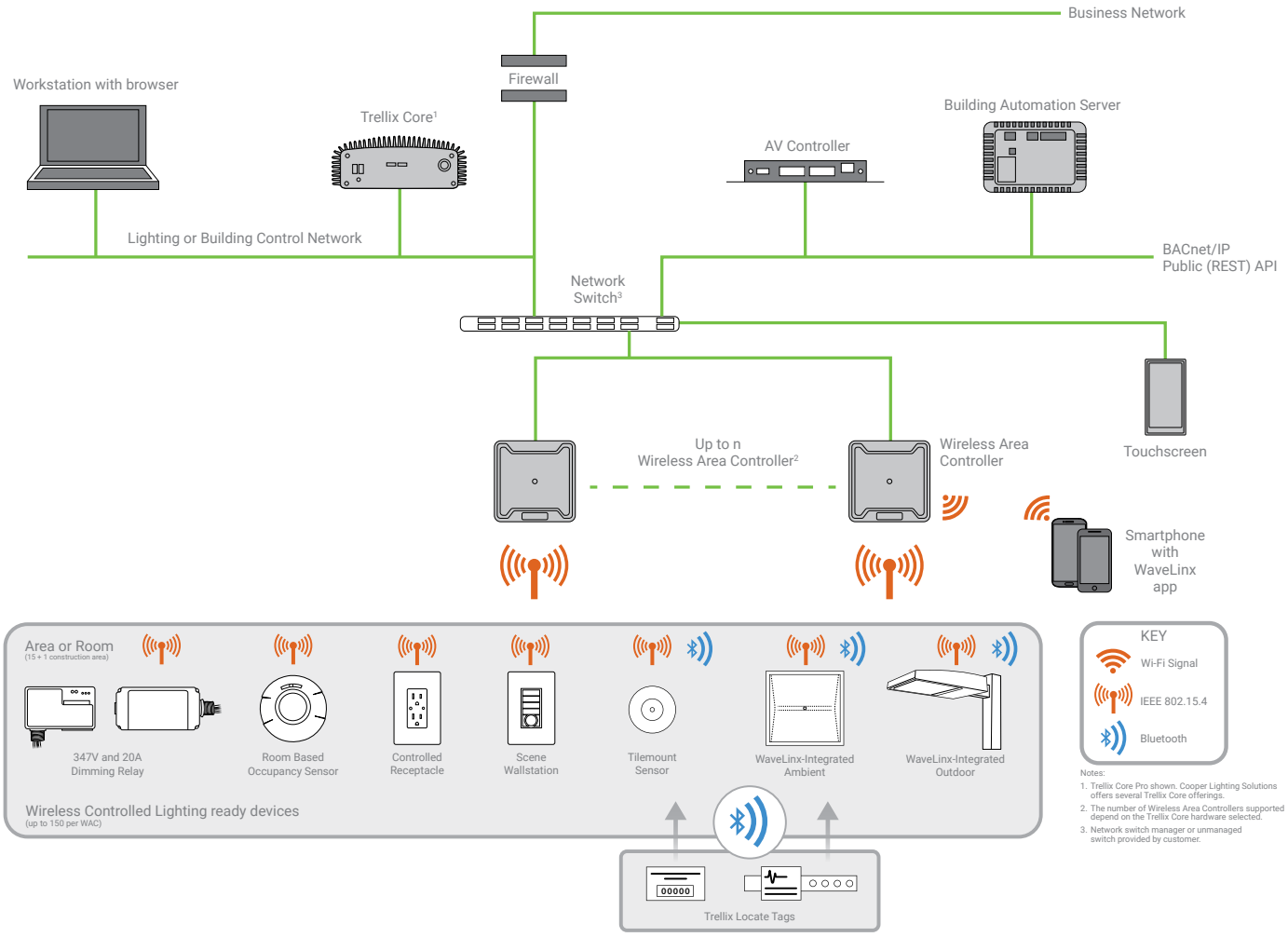
Security Features Include

1. **Physical security:**
   - An architecture that isolates the wired Ethernet network from the wireless network, which strictly limits the possibility of Trellix being used as an access point to the corporate network and gain confidential information.
   - Physical access also involves the customer location. This includes not allowing unauthorized personnel in areas where they do not belong, or access to devices they should not be connecting to, and we provide guidance to the customer on how to secure this.
2. **Customer security:**
   - Customer security process is a partnership between Cooper Lighting and the customer and involves multiple levels of password and network access protection.
   - Beyond physical access the customer provides an additional layer of security with strong authentication to access their corporate wired or wireless network and limiting the devices that can access those networks.
   - Cooper Lighting provides additional protection with unique username and password requirements for each Trellix Core that are securely stored per NIST-recommended best practices.
3. **Device communication security:**
   - For secure device-to-device communications, encryption is an important factor to reduce the potential of someone reading data sent on the network. For that reason, all Trellix communications use AES 128-bit encryption, recommended by NIST as part of FIPS publication 197.
4. **Network communication security:**
   - Trellix uses secure HTTPS (TLS1.2) protocols for securing connections to the Wireless Area Controller over the ethernet network.
   - Trellix uses secure WPA2 Enterprise technology for secure connections to the Wireless Area Controller over the Wi-Fi network when acting as an access point. If the Wireless Area Controller is connected to a ethernet network for communications this connection method is disabled.
   - WaveLinx mobile applications uses HTTPS (TLS1.2) as part of its communications to the Wireless Area Controller regardless of connection method, which means only our mobile application can send data to the WaveLinx system.
5. **Network segmentation security:**
   - Each Wireless Area Controller employs its own unique keys, which limits any potential breach to only a small area of the system.
   - The WaveLinx Wireless Area Controller (WAC) provides segmentation between the lighting Operational Technology (OT) network and the enterprise Information Technology (IT) network.
   - The IT/OT network segmentation provides a barrier to possible IT network attack surface exposure. Even if an attack within the lighting (OT) network and its devices is successful, the WAC isolates the enterprise IT network from potential attack.
6. **OTA update security:**
   - Trellix provides a method to allow for digitally signed firmware update files to be sent to the devices over the air (OTA). It is imperative as part of network security to ensure OTA update transmissions are encrypted and securely sent from their manufacturer so the devices recognize they are valid updates from that manufacturer and not sent with a malicious intent.
7. **COE assurance:**
   - CLSC involvement and guidance was key as part of the Trellix development to ensure our product incorporates industry and governmental network security best practices.
   - The CLSC also provides a publicly accessible site for information and feedback concerning cybersecurity threats and responses, as well as a method for you to monitor network breach risks.

Trellix deployments

Connected to the corporate IT network via Ethernet:

- The Trellix Core connects to the corporate network via PoE switch and must have Ethernet access. This is required for certain features such as BACnet® integration or Trellix Locate.
- This can also accommodate setting up separate networks for your lighting control or building systems than your business information network such as a VLAN.
- Wi-Fi is used for communications from the smart phone or laptop to the Wireless Area Controllers for programming, configuration and personal control through the use of internal web pages or the WaveLinx mobile application.



Cooper Lighting advises following your corporate best practices and selecting the installation method to meet your building and application requirements. Refer to the following white paper for additional guidelines about secure network configuration and management:
http://www.eaton.com/ecm/idcplg?IdcService=GET_FILE&allowInterrupt=1&RevisionSelectionMethod=LatestReleased&noSaveAs=0 &Rendition=Primary&dDocName=WP152002EN

Cooper Lighting Solutions
1121 Highway 74 South
Peachtree City, GA 30269
P: 770-486-4800
www.cooperlighting.com
For service or technical assistance:
1-800-553-3879

Canada Sales
5925 McLaughlin Road
Mississauga, Ontario L5R 1B8
P: 905-501-3000
F: 905-501-3172