CPX Security: Purpose-built for IoT Manufacturers
One platform - Full Lifecycle Security
Stand Out in the Marketplace with End-to-End Security

IoT Systems and Devices Introduce some of the Biggest IT Security Risks into the Enterprise Today
Traditional IT and SIEM tools Are Inadequate for the IoT

While safe coding techniques and penetration tools can help, no complete, on-demand and continuous security solution has existed for deployed devices – **until now**.

PXP [CPX] is the ***first*** IoT security solution designed for IoT product manufacturers, enabling them to manage the security of their IoT solution over its entire lifecycle from design through end-of-life.

CPX:

- Enables end-to-end, all-in-one visibility throughout the product lifecycle.
- Provides a comprehensive security evaluation of every customer deployed device and component.
- Displays point-in-time and over-time security performance assessments at the full portfolio or device level.
- Integrates with deployed SIEMs and enterprise security, workflow, and management solutions.
- Generates a prioritized list of activities and sends actionable alerts to your team.
- Evaluates customer performance relative to their peers. [bullets need to be properly indented.]

Your Comprehensive Security Assessment

IoT manufacturers can now have an in-depth understanding of their product security posture via 100 security measurements including:

- Software vulnerabilities
- Configuration weaknesses
- Outdated OS & libraries
- Network exposure
- User/Authorization issues
- Configuration changes
- Policy exceptions
- Threats
- Anomalous behavior

How CPX Works

CPX is a highly configurable, cloud or on premise-based service for both greenfield and brownfield environments. It uses Microsoft Axure's secure data centers for hosting. Self-hosting is also available.

[Insert PXP Product Architecture diagram, space permitting.] CPX enables you to Assess, Manage and Demonstrate your customers' IoT risk profile, as shown below:

Assess	Manage	Demonstrate
Protect the entirety of your attack surface	Identify/prioritize exposure and respond to IoT threats/attacks	Independently prove your IoT security
Comprehensive security evaluation of every device/component	Single tool visibility	Benchmarking, scoring, compliance/ end customer reporting
• Is device in secure mode? • Are communications encrypted? • Is there malware? • Is the device up to date? • Can the device be accessed remotely? • Is the device behaving unusually? • And tens of other measurements	• Allows views of data by customer(s), product(s), region(s), installer(s) …. • Provides prioritized list of actionable security issues to resolve • Integrates with key IT/ enterprise tools	• PXP framework provides guidance, scoring and benchmarking for IoT best practices • Comply with NIST CSF, NERC CIP, SOC 2 and other standards • Generate compliance reports for internal and external constituents • Provide customers and prospects with reports on their security
Monitor Entire Lifecycle *(design, build, operate, maintain)*		

CPX tracks every element of your IoT system including:

- networking information
- model number
- version information, etc.

CPX analyzes the data with its machine learning and rules engine to see if unusual patterns have occurred or if rules have been broken. It scores the results with CPX's scoring algorithm at the atomic level. CPX security and compliance assessments are continuously updated with the latest data in real-time. Assessments provide organizations with a blueprint for how to most cost effectively reduce their IoT-based cybersecurity risks and bridge any compliance gaps.

PLATFORM

- ***CPX Security Dashboard:*** Compiles insights for a single source view and drill down with action items for follow-up, including:
    - Overall compliance score
    - Product Design score
    - Product Deployment score
    - Product In-Use score

- ***CPX Deployment Toolbox:*** Ingests IoT data into the CPX system from a variety of sources including, configuration, telemetry, log, network data, device, gateway, and the cloud.
- ***CPX Security Engine:*** Performs a variety of security analytics, anomaly detection, vulnerability/threat assessment and scoring measurements; It marries this data with the threat intelligence from CPX's Threat Lab to see if malicious software or destinations are involved.

- ***CPX Portal:*** Via a responsive web-based user interface, displays compliance and benchmarking reports, data feeds and alerts; Supplies a wealth of security visibility into any vulnerabilities, threats, misconfigurations, policy weaknesses, anomalous behavior, and attacks in/to your IoT product suite.

FEATURES [Add a features call out box on the side.]

Searchable Inventory & Management

- Review detailed, **searchable bill of materials (BOM)** for all devices by customer, product line, and platform
- Centrally assess, manage, and demonstrate your security status

In-Field Monitoring & Alerting provides visibility into **deployed assets** in customer environments:

- Monitor deployed devices for anomalies and threats
- Integrate CPX Alerts into other workflows and tools

CPX:

- Provides a best practices framework to secure connected products.
- Confirms IoT solution designed and developed in a secure way.
- Verifies that underlying 3rd party software and custom code is secure.
- Confirms that installations are configured correctly.
- Ensures that the customer-deployed solution is being used in the recommended secure fashion.
- Monitors suspicious behavior.
- Measures the difference between designed security requirements and use in the field, and
- Presents and manages a plan for the remediation of issues.

Build for Compliance

The CPX platform framework provides guidance for IoT best practices. The product includes reports for complying with NIST CSF, NERC CIP, SOC 2 and other standards. Users can provide customers and prospects alike with reports on their security.

IoT security tools to date have focused on the end customer or host environment and not the IoT product manufacturers. CPX has your back.