WHITE PAPER:

PQ CANVASS AND CYBERSECURITY

Contributed by Joe Fackler

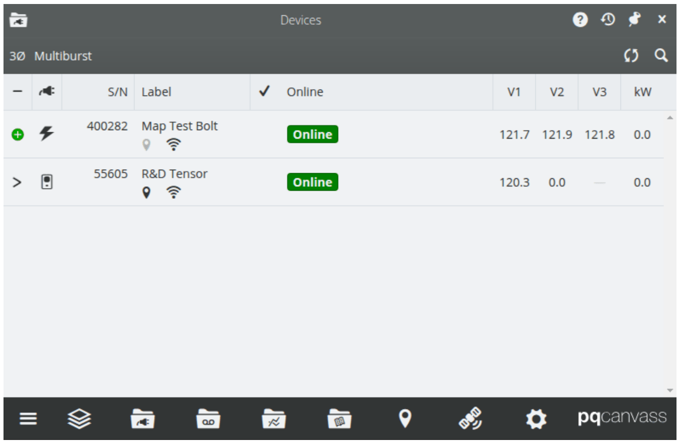
ABSTRACT

PQ Canvass is PMI's next-generation web-enabled power monitoring and analysis platform. Deploying PQ Canvass as a web application provides a number of benefits: analyzing recordings while the recorder is still installed, performance updates and new features without having to request permission to update every installation, and access from any modern computer, tablet, or smartphone. Every service exposed to the Internet is under constant barrage of traffic, some accidental and some intentional, most benign but some malicious.

In this paper we describe some of the techniques Power Monitors uses to protect both the PQ Canvass application and the data accessed through it.

SECURITY CONSIDERATIONS

The first component of security is design. PQ Canvass was not based on an off-the-shelf template for generic websites or contracted out to the lowest bidder but rather was designed, built, and is actively maintained by Power Monitors, Inc. software developers. This provides us with end-to-end granular control over authentication and authorization. While the PQ Canvass application enables access to and analysis of the stored recording data, no function of the site enables direct access to the underlying data, every request is routed through services which re-validate the user's permissions. This also means there is no way to mangle or destroy the recorded data through manipulating the web application in the browser's developer console.



		S/N	Label	✓	Online	V1	V2	V3	kW
⊕	⚡	400282	Map Test Bolt		Online	121.7	121.9	121.8	0.0
>		55605	R&D Tensor		Online	120.3	0.0	—	0.0

Figure 1. PQ Canvass.

In addition to manufacturing and support, all software development and design is done at Power Monitors' facility in Virginia, and cloud data is exclusively stored in US datacenters with AWS. This provides us with end-to-end granular control over authentication and authorization. While the PQ Canvass application enables access to and analysis of the stored recording data, no function of the site enables direct access to the underlying data, every request is routed through services which re-validate the user's permissions. This also means there is no way to mangle or destroy the recorded data through manipulating the web application in the browser's developer console.

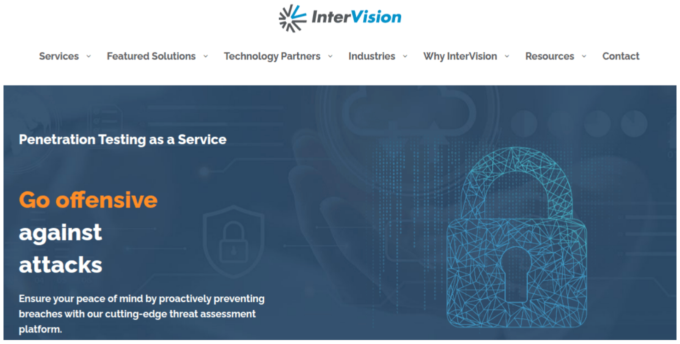
Additionally, Power Monitors, Inc. underwent an audit for NERC CIP 13 compliance. This standard, part of the North American Electric Reliability Corporation Critical Infrastructure Protection standards to ensure the reliability and security of the power grid. In the United States, the Federal Energy Regulatory Commission (FERC) enforces compliance with the NERC CIP standards. Specifically, NERC CIP 13, formally titled "Cyber Security – Supply Chain Risk Management," focuses on managing cybersecurity risks associated with the supply chain for the Bulk Electric System (BES). It mandates that BES entities develop and implement supply chain cybersecurity risk management plans to identify, assess, and mitigate risks posed by vendors, suppliers, and other third parties involved in providing products and services critical to the reliable operation of the grid. CIP 13 requires entities to establish processes for evaluating the cybersecurity posture of their suppliers, including assessing their security practices, software development processes, and incident response capabilities. Entities must also implement controls to protect sensitive information shared with suppliers and ensure that delivered products and services meet specified security requirements. Ultimately, CIP 13 aims to strengthen the overall cybersecurity resilience of the BES by addressing the potential vulnerabilities introduced through interconnected supply chains.

THE ONGOING CONCERN

However, even hiring developers with robust security experience and designing with security in mind is not a silver bullet. While Power Monitors, Inc. is not a household name like Apple or Google, the specific power data which Power Monitors, Inc. enables electrical utilities to collect and analyze is valuable in the wrong hands, so we cannot and do not rely on relative obscurity for protection. Malicious actors strive daily to create new and clever attacks to gain nefarious access to systems and data; even a system built well today will need updates and maintenance to provide the same level of security over time. With new threats emerging every day, how does a company like Power Monitors, Inc. stay on top of new vulnerabilities? Enter Intervision.

INTERVISION

Companies such as Intervision are dedicated to application and device security and can perform a wide array of penetration testing, code analysis, and customized data integrity probing. Intervision is one of many companies which provide these kinds of services. PMI chose Intervision from a number of different vendors based on ability to perform both remote and on-site penetration testing of PMI's products.



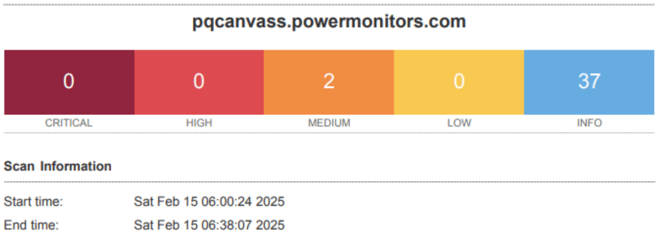
Penetration Testing as a Service

Go offensive against attacks

Ensure your peace of mind by proactively preventing breaches with our cutting-edge threat assessment platform.

Figure 2. Intervision home page.

Intervision provides automated scanning of the PQ Canvass application and all accessible cloud endpoints. The scans are regularly updated with new threat definitions and possible attack vectors. These scans allow PMI's developer team to adapt to newly discovered threats quickly, rather than waiting for an attack to occur. Intervision uses a battery of tools to emulate attacks against PQ Canvass and attempt to gain access to systems and data. The scan generates a report sent to Power Monitors, Inc. software team, who then work to mitigate any possible issues.



pqcanvass.powermonitors.com

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	0	37

Scan Information

Start time:	Sat Feb 15 06:00:24 2025
End time:	Sat Feb 15 06:38:07 2025

Figure 3. Report header page.

Among the many things tested by the Intervision team, they were able to confirm the security of PQ Canvass, that the web application successfully resisted attempts to gain access without valid credentials, that customer data was only accessible to the customer to whom it belonged, and that there is no way to manipulate the web application from within a web browser to gain inappropriate access or abuse the application's functionality.

Intervision also sent a technician to the Power Monitors, Inc. lab to test the security of the power quality recorders themselves, including the Bolt, our newest compact monitor. The Intervision tech worked against the USB, BLE (Bluetooth Low Energy), and Wifi interfaces to look for possible vulnerabilities. After passing the on-site security testing, PMI set up some devices for Intervision to scan automatically in the event of new threat discoveries.

CONCLUSION

Power Monitors, Inc. takes the security of electrical utility data seriously, from hiring security-minded developers, to designing PQ Canvass, to a commitment that security is never finished. Customers, whether electrical utilities or other entities, can rest at ease knowing that Power Monitors, Inc. takes diligent care of the data entrusted to us.

RELATED READING

Canvass and Cybersecurity

End to End Boomerang Cybersecurity