Penergy / eFAACT Security Overview

8/17/2024

Penergy Technologies, Inc. (Penergy) is a Virginia-based software company focused on delivering cost effective business solutions for small to mid-sized organizations.

Penergy's eFAACT® software system integrates with Intuit's QuickBooks® and is dedicated to fulfilling the unique requirements of United States government contractors.

THE PENERGY SECURITY MODEL.

Penergy maintains a written information security program that contains administrative, technical, and physical safeguards that are appropriate to protect customer data in its possession and control. Our security program is designed to:

- Protect the confidentiality and availability of customer data in our possession or control,
- Protect against unauthorized or unlawful access to the customer data or accidental loss or destruction of Customer Data in our possession or control,
- Protect against anticipated threats to customer data or the eFAACT environment.

POLICIES.

Internal policies are designed to:

- Limit access to software and systems to authorized individuals,
- Place restrictions on software installation,
- Manage technical vulnerabilities and malware, and
- Manage data retention and deletion requirements.

SECURITY AND ACCESS CONTROLS.

Security controls are implemented and maintained in the following areas:

- Person specific access credentials to approved applications, operating systems, databases, and network devices.
- Multi-factor authentication for authorized employee access to all servers.
- System segregation and access controls for access to customer data.
- Limit software access to authorized users based on the principle of least privilege.
- Review access rights on a regular basis.
- Password complexity requirements.
- Policy for returning equipment and disabling access upon employee termination.
- Asset inventory and asset classification based on criticality for business continuity.

NETWORK SECURITY.

Penergy's FortiGate provides key security benefits for both internal user traffic and public facing web servers:

1) Intrusion Prevention System (IPS): The IPS feature detects and blocks malicious activities and exploits targeting our web servers. It provides real-time protection against known and emerging threats catalogued within FortiGuard, a suite of AI-powered security services provided by Fortinet.
2) SSL Inspection: FortiGate can inspect SSL/TLS traffic to ensure that encrypted traffic is free from threats. This includes support for the latest TLS 1.3 standard.
3) Web Filtering: This feature helps control access to web content by blocking malicious websites and filtering out unwanted content, which can prevent drive-by downloads and other web-based threats.
4) Advanced Threat Protection: FortiGate integrates with FortiSandbox to provide advanced threat detection and mitigation, including zero-day threats.
5) Centralized Management: FortiGate offers centralized management and reporting, making it easier to monitor and manage security policies across multiple web servers.
6) AV Protection: FortiGate offers comprehensive threat protection, including antivirus and anti-malware features. Helping keep our users safe from malicious software and phishing attacks. Additionally, Application Control allows monitoring and control of applications within our network, helping prevent data leaks and unauthorized activities.

ENCRYPTION.

Customer data is encrypted at rest with a minimum of AES 256 encryption. Customer data is encrypted in transit with a minimum of TLS 1.2 or greater using AES 128 or 256 encryption dependent on what the web browser supports.

DATA DELETION.

Customer data is segregated and deleted or destroyed as set forth in the eFAACT license agreement. Customer data contained in backup files is set aside until it is aged out of backups in accordance with internal policies.

LOCATION HOSTING.

All data is hosted in the United States. eFAACT is hosted in Microsoft Azure and customer data is stored in the East US region.

EMPLOYEE TRAINING AND AWARENESS.

All employees are required to acknowledge the Penergy Employee Guidebook, which contains workplace policies on use of electronic communications and computer systems; and attend initial new-hire security training, annual awareness security training, insider threat, and focused role-based security training.

INCIDENT RESPONSE.

Penergy maintains an incident response plan internally, including:

- Procedures to collect and maintain evidence;
- Planned actions for events based on government agency activities; and
- 24x7 eFAACT Helpdesk for customers to report security incidents

Penergy completes regularly scheduled security incident response/disaster recovery tests and notifies customers of security incidents as identified in the eFAACT license agreement.

ASSIGNED SECURITY RESPONSIBILITIES.

Penergy resources are assigned specific responsibilities within the security and incident response team.

TESTING AND CERTIFICATIONS

Penergy regularly analyzes its controls, systems, and procedures. This action includes internal risk assessments, NIST 800-53/171 CMCC 2.0 Level 2 compliance and SOC1 and SOC2 Type 2 audit reports.