What is PCI Compliance?

The Payment Card Industry Data Security Standard (PCI DSS) refers to a combination of requirements that make sure all companies that store, process, or transmit credit card information provide an environment for their customers' data that is safe and secure.

It is composed of helpful rules and guidelines that keep sellers and their customers safer from attackers. It acts as a measure to enhance the security of accounts through all stages of credit card transactions.

Why Is It Important To Be PCI-Compliant?

Businesses that store and save customer credit card data may expose their customers to fraudulent attacks and banks to potentially large losses if they do not take the proper precautions. If you maintain PCI DSS compliance, you can maintain conformity to privacy and security laws.

86% **of breaches occur** because hackers see your data as a potential source of income.

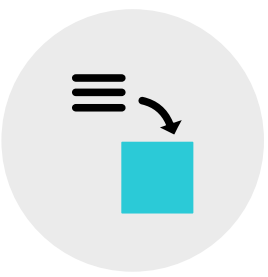
Fortinet can cut off their access by implementing PCI compliance measures.

How Do You Become PCI-Compliant?

Install a Firewall and Maintain It

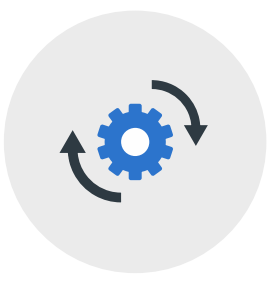
Initiate Strong Password Protections

Protect the Data of Cardholders

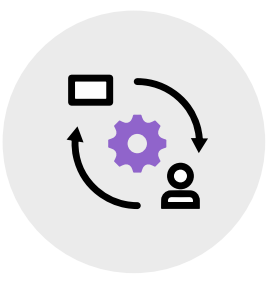


Encrypt Data That Gets Transmitted

Install and Maintain Antivirus Software

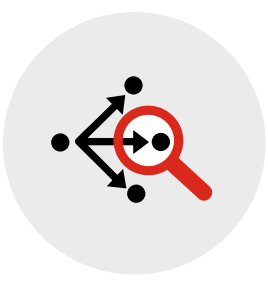


Update Your Software

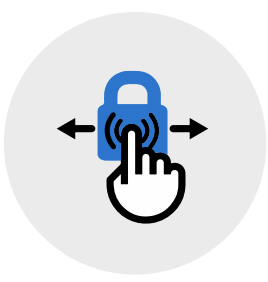


Restrict Access to Data

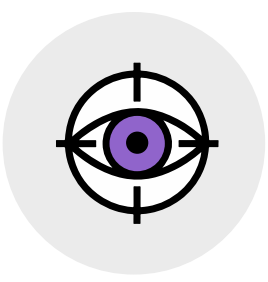
Establish Unique IDs for Those with Access



Physical Access Needs to be Limited



Establish and Maintain Access Logs



Scan and Perform Tests to Identify Vulnerabilities

Document your Policies

What Is the Cost of Being PCI-compliant?

While the cost of attaining PCI compliance varies depending on what you already have in place, the cost of not being compliant is considerable. The cost of noncompliance is best determined by calculating the cost of a security breach.

Penalties for PCI Compliance Violations

Although fines are not published for the public, they can be steep. They tend to be between $5,000 and $100,000 for each month you are out of compliance. This holds true for both on-premises and cloud systems, like those housed in Amazon Web Services (AWS).

How To Validate PCI Compliance

The validation process you go through depends on the credit card companies that you use. There are two methods for validation:

Complete your own PCI Self-Assessment Questionnaire, (SAQ)

Hire a certified PCI Quality Security Assessor or QSA.

How Fortinet Can Help?

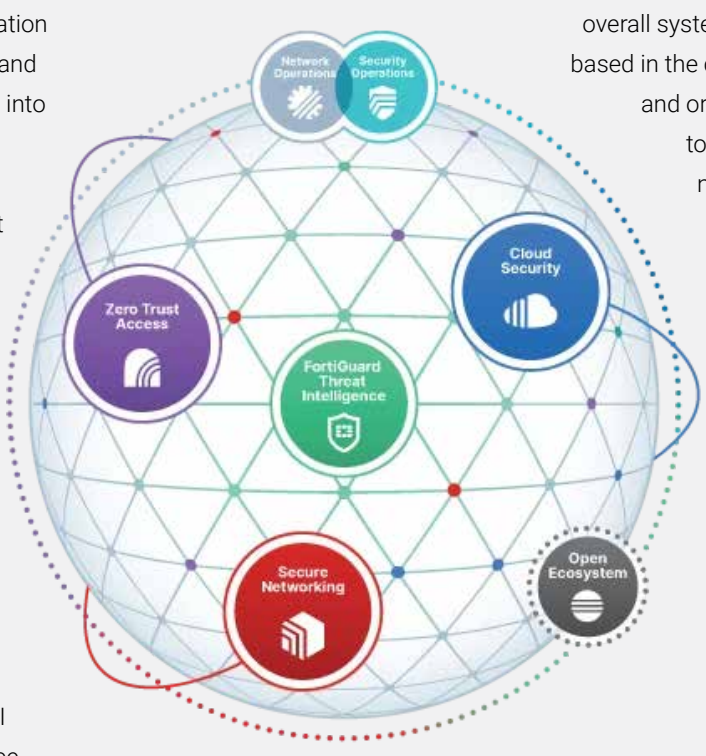
Fortinet has several tools to help you maintain PCI DSS compliance.

FortiCASB

organizes and aggregates security information from several application programming interfaces (APIs) and cloud services, combining them into compliance reports and dashboards that you can share with people and institutions that need to be kept in the loop.

FortiSIEM

gives you a wide view of how compliant your overall system is, regardless of whether it is based in the cloud or on-premises. It collects and organizes data from your security tools, whether they are Fortinet or non-Fortinet measures, and then creates reports about your compliance with only a click.



FortiAnalyzer

gets logs from different elements of the Fortinet Security Fabric. The reports are prebuilt and designed according to regulations like PCI DSS, making tracking compliance easier. FortiAnalyzer also enables you to produce real-time reports that show how you are conforming to PCI DSS standards.

FortiManager

empowers you to see, approve, and audit changes to your policy from one location. FortiManager also automates the processes needed to facilitate compliance.

For more details about securing OT and the supply chain, read the full report ***"Assessing the State of OT Security and the Cyber Supply Chain."***