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 other customers safe from attackers. It acts as a measure to enhance the security of accounts through all stages of credit card transactions.

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 follow proper procedures. If you maintain PCI DSS compliance, you can maintain your company’s privacy by doing what is best for you.

If you maintain PCI DSS compliance, you can maintain conformity to privacy and security laws.

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

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

FortiCASB organizes and aggregates security information from various application programming interfaces (API) and cloud interfaces, 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 at any time. You can also report any violations and track the compliance status of your teams.

Penalties for PCI Compliance Violations

$5,000 and $100,000 are just a few examples of the cost of noncompliance. 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).

What Is the Cost of Being PCI-compliant?

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).

Fortinet Can Help

Fortinet can help you keep up with PCI DSS compliance.

FORTINET

Why Is It Important To Be PCI-Compliant?

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

How Do You Become PCI-Compliant?

Install a Firewall and Maintain It

Initiate Strong Password Protections

Protect the Outflow of Cardholder Details

Ensure End-to-End Data Transmission

Install and Maintain Access Control Software

Update Your Software

Reduce Access to Data

Establish Unique IDs for Those with Access

Physical Access Needs to Be Limited

Balance and Maintain Access Logs

Scan and Perform Tests to Identify Security Issues

Document Your Policies

Compliance as PCI Self-Assessment Questionnaire (SAQ)

How To Validate PCI Compliance

How Do You Become PCI-Compliant?

Install of a firewall and password enforcement 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.

What Is the Cost of Being PCI-compliant?

How Do You Become PCI-Compliant?

What Is PCI Compliance?