DATASHEET

imprivata

Enterprise Access: The Third-Party Remote Access Solution for PCI DSS Compliance

PCI DSS Requirements for Critical Remote Access

Managed and enforced by major credit card companies, the Payment Card Industry Data Security Standard or PCI DSS, outlines the mandatory technical and operational standards organizations must follow when handling cardholder data. The goal of these security requirements is to secure and protect credit card transactions and data against a data breach or security incident.

The Target breach in 2013 resulted in 40 million credit card numbers stolen, PCI noncompliance, and cost Target over $200 million in legal fees and settlements. The source? A small HVAC vendor with VPN access.

When compliant with these security standards, organizations are also better positioned to mitigate the risks of an attack and protect their cardholder data and networks. Better security leads to greater customer trust, loyalty, and retention. On the flip side, a security breach with stolen customer data leads to loss of revenue and customers.

Third Parties and PCI Compliance

Third parties and their remote access to cardholder data are a key component of meeting PCI requirements, as well as securing data and networks against cyber attacks. Third parties are highly targeted by attackers as easier entry points into an organization's critical systems. In fact, 49% of organizations experienced a breach caused by a third party in the past year

alone, and most attribute the breach to granting too much privileged access.

Traditional remote access tools, such as VPNs or desktop sharing, do not meet the security standards that PCI requires. They are not designed to restrict access to only authorized users and granularly control that access, and they don't provide visibility through recordings of access activity for review and examination. If access to sensitive customer information and cardholder data isn't secured against third-party risks, your business could face PCI noncompliance fines, as well as the even more costly loss of customer loyalty and revenue.

Cost of a Data Breach: The average cost of a data breach for a U.S. organization is $9.05 million.

Third Parties Are Your Weakest Attack Vector:

56% of organizations have experienced one or more data breaches caused by a third party.

Data Breaches Cost Customer Loyalty:

64% of consumers would likely end their relationship with an organization after their personal information had been exposed.

SecureLink Enterprise Access provides the means to meet PCI security requirements with regards to your third parties' access. With individual identity management, granular control over vendor access, and detailed audit trails that log all activity, Imprivata will be a valued partner in helping you mitigate the risks of third-party access and meet your PCI compliance requirements.

How SecureLink Enterprise Access Enables Organizations to Meet PCI Compliance

PCI Compliance	Requirements	How Enterprise Access Helps
Password Protection	Change default passwords	• Passwords are secured and managed in a credential vault and injected directly into the session so users never see or know them
Secure Data	All cardholder data-at-rest and data-in-transit is protected	• All audit and credentials are encrypted at rest • Data-in-transit is encrypted with AES-128, 192 or 256
Restrict Access	Restrict access to cardholder data to only authorized users	• Control access with fine-grained access controls such as access schedules and approvals • Define granular access per user based on least privilege • All access is disabled by default and defined down to the host and port level per user, dependent on role and responsibility • Require approval with reason for access before access is granted
Use Unique ID Credentials	Ensure the use of unique IDs per user	• Enforces use of individual accounts • Enforce MFA for identity verification with any TOTP-based app, SMS and email employment verification • Immediately terminate access for users no longer employed by vendor • Automatically disable inactive accounts or after failed login attempts
Log and Monitor All Activity	Track and monitor all access to network resources and cardholder data Retain an audit trail of minimum one year, with the last three months immediately available for review	• Audits all sessions with video recordings and text-based audit of all users actions by default • Can export audit and data to a SIEM solution for further analysis • Can be reviewed daily in accordance with PCI policy • Customer can define audit retention length in accordance with PCI retention policy • All activity in the audit is tied to an individual user

Risks and Consequences of Unsecured Third-Party Access

RISKS WITH THIRD PARTIES

49% of organizations have experienced one or more data breaches caused by a third party in the past year

46% of organizations have a comprehensive inventory of all third parties with access to their network

63% of organizations see third-party remote access to their network becoming their weakest attack surface

41% of organizations believe they are effective at controlling third-party access to their networks

37% of organizations have visibility into the level of access and permissions for both internal and external users

44% of companies rate the effectiveness of their third parties in achieving compliance with security and privacy regulations that affect their organization as very high

FREQUENCY AND COST OF ATTACKS

- The average cost of a data breach in the United States is $9.05 million
- By 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021
- The costs of a cyberattack last for 3 years on average, with 67% of the costs incurred in year one, 22% in year two, and 11% in year three

Unsecured third-party remote access can result in severe consequences, such as stolen credit card and customer information, loss of customers and revenue, noncompliance penalties, and even inability to operate. SecureLink Enterprise Access is built to minimize these risks. It secures your third-party remote access and equips you to meet PCI security requirements.

Contact us to learn more about how Enterprise Access can help.

CONTACT US

imprivata®

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

DS-EA/PCI_2023