DATASHEET

How Enterprise Access helps achieve compliance

Third parties continue to be one of the biggest cybersecurity risks to an organization. Last year, nearly half of organizations experienced a **data breach caused by a third party** and with ransomware on the rise, businesses need to lock down their third-party security strategy before a hacker finds a vulnerable access point. Staying compliant is an easy step to secure third-party access and prevent threats.

The problem with vendor access and compliance

Compliance requirements are particularly strict around **third-party remote access** into an organization's network, and the tighter the regulations, the harder it is to be compliant. Organizations tend to find difficulty achieving third-party compliance with three main problem areas: time, resources, and knowledge. Most businesses don’t have the time to gather all the information auditors are looking for about their third parties, nor do they have the resources (like reporting systems and compliance team employees) to collect all the documentation needed. Meeting regulatory compliance can also be a challenge because organizations don’t know what requirements need to be met or how to best collect information on third-party users, their access levels, and their session activity. This lack of knowledge can lead to non-compliance, regulatory fines, and decreased employee productivity and morale, all because a business is burdened with digging itself out of a metaphorical compliance hole.

Last year, nearly half of organizations experienced a data breach caused by a third party

Auditors across all industries are looking at a business’ third-party access and asking these questions:

- Are you able to individually identify and verify the third parties who have access to your network?
- Do you have the proper access controls in place?
- Do you have visibility into their access?
- Are you able to document and prove that all of these are in place?

With automated third-party remote access, the answer can be “Yes.” Rather than being penalized for failing to meet compliance requirements, companies are seeking out streamlined solutions that automate processes like user identification and network session recording.

How Enterprise Access achieves compliance

Enterprise Access is a streamlined third-party remote access platform that securely connects technology vendors and service providers to a business' network. The standard approach to remote access has traditionally been through VPN connections, but these have proven to be inefficient, faulty, and not safe enough to prevent cyber criminals from hacking third-party access connections. Enterprise Access has unique features that answer the specific questions auditors are asking when checking third-party access for regulatory compliance.

ARE YOU ABLE TO INDIVIDUALLY IDENTIFY AND VERIFY THE THIRD PARTIES WHO HAVE ACCESS TO YOUR NETWORK?

Enterprise Access offers user registration, meaning each third-party vendor or rep registers within the system so every user identity is logged and managed. A business' Enterprise Access administrator is able to see the inventory of all third-party reps who can access the network as well as verify each user through multi-factor authentication (MFA) methods. This brings added protection to the network by ensuring each identity registered within Enterprise Access matches the same being who is trying to access the network.

DO YOU HAVE THE PROPER ACCESS CONTROLS IN PLACE?

Along with MFA, Enterprise Access features more access control methods, like the ability for administrators to set up time-based one-time passwords (TOTP), access requests and approval processes, notifications, and zero trust network access. These controls restrict vendor access down to the most minimal amount of exposure in a business' network, isolating the user to only the applications needed for their assignment and preventing any lateral movement to other systems or access points.

DO YOU HAVE VISIBILITY INTO THEIR ACCESS?

Monitoring user access is a huge component of compliance, yet 51% of organizations aren't tracking and monitoring access to network resources and critical data. Visibility into third-party sessions allows you to observe vendors in real-time for any suspicious behavior. Monitoring access proactively protects a business' network and provides the evidence needed for compliance and in the case of a breach, investigation. Enterprise Access features monitoring and audit capabilities that record all details of a third-party session. HD video and text-based recordings are captured for audits, observation, and analysis of third-party activity.

ARE YOU ABLE TO DOCUMENT AND PROVE THAT ALL OF THESE ARE IN PLACE?

Auditors can easily look at the Enterprise Access server to see that all of these processes and requirements are in place—from vendor identity management and access controls to video recordings and reports. System administrators can pull reports from Enterprise Access to give auditors any information they want on third-party activity within the network. It's a comprehensive platform that makes compliance easier to meet and not as threatening of a task.

Healthcare and third-party compliance

Healthcare facilities heavily rely on third parties like billing services and machine technicians, which is why the healthcare industry is one of the most vulnerable and susceptible to cyber attacks. Between HIPAA, HITECH, and HITRUST regulations, it also faces some of the heaviest compliance requirements. Healthcare compliance teams are under-resourced and underfunded, so to meet compliance and save facilities and patients from the fallout of a data breach, automation needs to be implemented. Enterprise Access can help healthcare facilities stay compliant by providing a comprehensive remote access platform to consolidate access of all third parties. With all third parties in one system, healthcare compliance teams can establish access controls, audit session activity, manage vendor identities, and monitor network behavior using one platform. This helps track all third-party behavior and possible threats without taking up additional resources that a hospital might not have.

If you're in a regulated industry, our compliance checklists can help you identify if your third-party software is meeting industry compliance requirements.

- HIPAA Compliance Checklist
- HITRUST Compliance Checklist
- CJIS Compliance Checklist
- PCI DSS Compliance Checklist

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

Copyright © 2023 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.