zscaler™ Healthcare Solutions | imprivata®

SOLUTION BRIEF

Zscaler and Imprivata

Delivering Zero Trust security for shared workstations in healthcare organizations

Challenges

The healthcare industry is facing an increasing number of ransomware attacks, as well as enhanced regulatory and compliance requirements. Paying a ransom can cost hundreds of thousands of dollars in addition to reputational damage. Above all else, any downtime can be at great risk to patient safety.

Legacy perimeter-based networks and firewall- based architectures don't protect you against these attacks. A hacker can compromise your network by gaining access to a single workstation. Given that hospitals and healthcare organizations have large numbers of shared workstations, these devices are primary attack targets.

What you need

Doctors and nurses constantly log in and out of workstations throughout the day. Ensuring that the right users have access to the right applications is critical for cyberthreat protection and regulatory compliance.

Security policies should follow the user, and user activity should be tracked to distinguish actions between users – even on shared workstations or different workstations at different times. To ensure protection, the user's identity must be secured and the application access control and context must be understood.

A Zero Trust approach is needed

A Zero Trust security architecture is required to provide protection and ensure compliance. Zero Trust starts with identity. Imprivata is a leader in identity for healthcare organizations, providing capabilities that enable, control, and monitor digital identities to deliver fast user access, improve security, and ensure compliance across all systems.

Healthcare has unique requirements. Clinicians can't afford delays when securely accessing the applications they need to provide patient care, yet healthcare organizations must ensure they protect PHI from internal, external, and third- party threats. Managing and controlling digital identity and ensuring security follows the user instead of the device is the only way to keep data and applications secure while ensuring quick and proper clinician access.

Zscaler is a pioneer in Zero Trust with the cloud native Zero Trust Exchange platform that helps stop cyberattacks using its proxy architecture, prevents lateral movement by connecting users directly to their apps (not networks), and minimizes the attack surface by making apps invisible to hackers (you can't attack what you can't see).

Best-in-class zero trust

Zscaler and Imprivata have joined forces to provide a Zero Trust security solution for multi-user workstations in healthcare organizations. By integrating with the Imprivata Enterprise Access Management with SSO (formerly Imprivata OneSign) identity management platform, the Zscaler Zero Trust Exchange can adaptively enforce access control policies, ensuring that only authenticated users are allowed to access authorized applications. Clinicians can seamlessly and securely authenticate in and out of shared devices, while user actions are logged for traceability and compliance requirements.

By implementing context-aware, market-leading solutions from Zscaler and Imprivata, healthcare organizations can simplify secure access, reduce the risk of ransomware attacks and downtime, strengthen regulatory compliance, and improve clinician productivity and the user experience.

How it works

1. Clinicians use their badges to login to a badge reader on a shared workstation using Imprivata Enterprise Access Management with SSO
2. The workstation is protected by Zscaler Client Connector™
3. Imprivata determines which applications a user is authorized to access and Zscaler enforces those access policies
4. When a clinician 'taps out' using the badge reader, they are logged off the machine
5. When a different clinician enters the room and logs in on the same workstation, they will get policies relevant to their user profile

Key benefits

The Zscaler and Imprivata integration delivers the following key benefits:

- Multi-user, shared workstation adaptive policy enforcement for healthcare environments
- Zero Trust security with role-based access to protect patient data
- Traceability of user actions for regulatory compliance, including HIPAA and HITECH

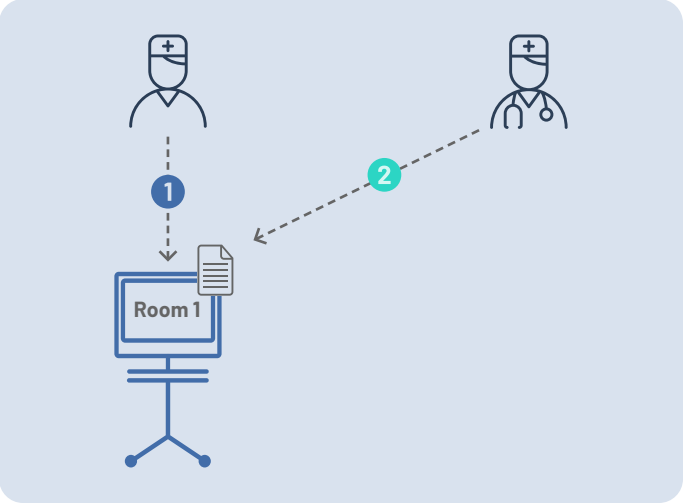
For example, if a nurse logs in to a workstation, the policy for nurses may be that they can access certain websites and applications but they can't access Google Drive where patient data is kept. If a nurse tries to upload a patient data file, Zscaler will block this action based on Imprivata's identity authentication information and the nurse's role.

However, if a doctor logs in to that same workstation, Zscaler Client Connector will silently log out the nurse and log in the doctor. The nurse and doctor are not aware of the client connector application on the workstation, making it a seamless user experience.

The doctor is able to upload a patient note to Google Drive because the access control policy applied to a doctor is different from that of a nurse, even though the doctor is using the same shared workstation that the nurse was on just moments ago. The nurse's and doctor's actions are all available in Zscaler log files for compliance purposes.

1. A nurse taps their badge to log in to a shared workstation; they can access certain applications but are not allowed to upload a patient data file to Google Drive, as defined by access control policy

2. A doctor logs in to the same shared workstation but is able to upload a patient file to Google Drive, since a different access policy is applied to their role



imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0)208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

---

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform.