imprivata

DATASHEET

Imprivata Identity Threat Detection and Response: See the identity risks inside your clinical environment

Extend Microsoft Conditional Access with Imprivata identity intelligence from the point of care

Microsoft Entra Conditional Access provides important identity and access controls. But some of the identity signals that matter most in healthcare originate inside clinical workflows, where clinicians move between shared workstations, authenticate with badges, access applications, and change locations throughout the day.

A cloud sign-in can tell you which account accessed a resource. **Imprivata Identity Threat Detection and Response (ITDR) adds context about how, where, and from which endpoint that access occurred.**

Together, Imprivata and Microsoft can provide a more complete picture of identity risk without adding unnecessary friction to clinical work.

See more than the account

Microsoft Conditional Access	Added insights with Imprivata ITDR
Cloud identity and sign-in activity	Shared workstation and device context
Public network and location signals	Internal workstation clusters and network ranges
Microsoft authentication activity	Badge and Imprivata authentication activity
Cloud application access	Clinical session and application activity
Microsoft identity risk signals	Historical user, device, and workflow behavior

This additional context helps security teams determine whether activity that appears valid at the account level actually makes sense within the clinician's normal workflow.

Detect threats that can hide inside the four walls

Imprivata already participates in critical access workflows across the healthcare environment. ITDR can use those identity and endpoint signals to help surface threats that may be difficult to identify from cloud identity activity alone.

Impossible travel
Identify when the same identity appears in locations too far apart to be plausible.

First-time access
Recognize access to an unfamiliar facility, device, application, or resource.

Credential sharing
Surface unexpected use of one identity across workstations, devices, or applications.

Unusual shared device use
Identify activity on shared devices outside a user's established patterns.

Stolen badge use
Detect badge activity at an unusual time, location, or workstation.

The difference is context. An authentication event becomes more meaningful when it can be correlated with the user, endpoint, location, authentication method, and previous activity.

Make Microsoft and Imprivata stronger together

You don't need to choose between protecting cloud identities and understanding what happens inside clinical workflows. The stronger approach connects both.

1. **Give ITDR broader identity context**
   Microsoft Entra authentication activity can be correlated with Imprivata activity for the same user. This gives ITDR more information to assess whether activity represents normal clinical work or potential risk.
2. **Add clinical workflow intelligence to your Microsoft strategy**
   ITDR provides risk context derived from Imprivata authentication and endpoint activity. This can help security teams make more informed decisions about identities that also access Microsoft resources.
3. **Keep your security operations workflows**
   ITDR detections can flow into existing SIEM workflows, helping security teams investigate identity threats without creating another isolated security process.
4. **Avoid unnecessary authentication complexity**
   Imprivata Enterprise Access Management users can continue using existing EAM authentication methods as a second factor with Microsoft Entra ID, helping organizations strengthen identity security without introducing another authenticator into clinical workflows.

Apply stronger security when risk calls for it

ITDR helps organizations move from individual events to informed action:

Capture identity and endpoint activity. Detect anomalies and threat patterns. Assess the activity using behavioral and workflow context. Then apply the appropriate response based on risk.

This matters in healthcare because every anomaly should not interrupt care. Trusted clinicians need efficient access, while higher-risk activity requires greater scrutiny.

The ideal state: identity security informed by the clinical workflow

Microsoft provides important identity controls across the enterprise. Imprivata adds intelligence from the environments where clinicians actually work.

Together, they can help organizations:

- Gain visibility into identity threats inside clinical environments
- Make risk decisions using richer identity and endpoint context
- Extend existing Microsoft security investments
- Preserve efficient authentication for trusted clinicians
- Give security teams actionable detections within existing workflows

See what your identity strategy may be missing

Evaluate ITDR against your highest-priority internal identity threat scenarios and identify where additional clinical workflow context can strengthen your Microsoft identity security strategy.

Talk to Imprivata about an ITDR proof of value.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

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

7712-2026_EAM-DS-ITDRvsMicrosoft