

INFOGRAPHIC

The value of Imprivata Enterprise Access Management (formerly OneSign) data

Simplified, secure access to your apps and systems through Imprivata Enterprise Access Management (formerly Imprivata OneSign) with single sign-on (SSO) eliminates password fatigue and drives productivity.

But by how much? And how many applications are team members not utilizing?

Typically, gathering insight into SSO data requires IT teams to spend time and resources building out queries and dashboards.

But not anymore. Introducing Enterprise Access Management (EAM) Analytics

Create custom dashboards

Point, click, and know with the ability to utilize pre-built reports and customizable dashboards, eliminating the need to write queries.



Drill into issues

Dive deep into specific user issues to understand where the problems are and speed up resolution times.



Track trends

Focus IT resources appropriately with the ability to track usage trends over time.



Understand workstation usage

See various reports on workstation usage to understand application usage and spot potential areas to decrease IT operational spend (licenses, hardware, etc.)



Set alerts

Stay in the know with the ability to set alerts on specific users or use cases to investigate issues quickly



With EAM Analytics, IT teams can save time and get the answers they need quickly. Allowing them to:

- Visualize areas of success for leadership
- Notice where gaps may exist to provide additional training
- Track resolutions to ensure issues are decreasing
- Find areas where licenses or hardware can be removed to decrease IT operational spend.

Gain valuable information to help drive the adoption of EAM across departments, while finding areas where IT can reduce operational spend with EAM Analytics.

To learn more about EAM Analytics watch our video.



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 1 781 674 2700
or visit us online at www.imprivata.com

Copyright © 2024 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.

OS-EAM-Analytics-Infographic_0424



DATASHEET

Enterprise Access Management Packaging

Guide to licensing for enterprises

Streamlined Licensing for Enterprises

Imprivata Enterprise Access Management (EAM) provides secure, frictionless access to the workstations, applications and workflows that frontline workers rely on. Organizations can combine EAM's Core Access with flexible modules for a customizable approach. By unifying single sign-on, advanced authentication, identity orchestration, contextual analytics, and critical access workflows into a modular system, Imprivata enables organizations to address their immediate needs while giving them the flexibility to choose their own path for future growth.

At-a-glance benefits

- Clean, intuitive packaging and pricing
- Streamlined contracts
- Tremendous value
- Logical feature grouping

Licensing modules overview

Core Access – The essential Single Sign-On and Identity Provider capabilities that underpin every Imprivata EAM deployment. This module includes EAM Analytics for actionable insights into single sign-on usage, authentication patterns, and workstation/application activity, with customizable dashboards and alerts.

Shared Device Access – Access management for shared workstations including fast user switching and automatic workstation locking.

Advanced and Passwordless Access – Advanced identity features including passwordless authenticators, identity verification, risk-based access, VPN-less remote access and self-service password reset.

Secure Workspace Access – (formerly known as *Virtual Desktop Access*) – No Click Access® to virtual desktops and applications on individual and shared workstations and support for thin-client operating systems and secure browsers.

ID Verification (IDV) – Add-on for additional identity proofing via document authentication and biometric face matching for onboarding, enrollment, and high-risk access events.

How the licensing model works

1. Begin with Core Access

The foundation for authentication, SSO, identity synchronization, and analytics.

2. Add Shared Device Access

Secure access to shared workstations with fast user switching and automatic workstation locking.

3. Add Advanced and Passwordless Access

Strong and modern risk-based authentication for remote access and other advanced workflows.

4. Add other modules as needed

Expand capabilities with Secure Workspace Access for access to secure enterprise browsers and virtual systems or Identity Verification to securely enroll new users or reset authenticators.

5. Simplified conversions

For existing deployments, Imprivata assists with consolidation of SKUs and contracts, even across mixed entitlement counts and renewal dates.

Benefits of EAM packaging

Simplified and predictable

- A clean, intuitive packaging and pricing structure
- Streamlined contracts and licensing terms
- Logical grouping of complementary capabilities

Consistent licensing

- Per-user licensing applied across all modules
- Easily scalable as needs evolve
- Reduced complexity for procurement and renewals



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

Copyright © 2026 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.

Imprivata OneSign Overview and Architecture

Imprivata OneSign is the enterprise single sign-on (SSO), authentication management (AM), virtual desktop access (VDA) and self-service password reset (SSPR) solution specifically designed for healthcare. It easily integrates with existing IT infrastructure and scales to support hundreds of thousands of users accessing clinical applications and workflows from thousands of workstations.

The sections below describe the Imprivata appliance and the Imprivata agent – the key components of Imprivata's architecture.

Imprivata Appliance

The Imprivata appliance is the foundation of the Imprivata OneSign solution. It is delivered as an Open Virtualization Format (OVF) image that can be hosted in VMware ESX or Microsoft Hyper-V environments.

User Identities

The appliance is configured to synchronize with Microsoft Active Directory (AD) to import user identities into Imprivata OneSign. Identities can be imported based on one or more organization units (OUs), groups, or individual users. These users are enabled for SSO and other Imprivata OneSign capabilities using policies and profiles that are created and assigned by the Imprivata OneSign Administrator. During a user authentication event, the appliance binds to AD to verify a user's status and password. A single appliance can handle thousands of simultaneous authentication events from Imprivata-enabled workstations.

The Enterprise

Two or more appliances are configured to create an Imprivata enterprise. Appliances in an enterprise replicate in real time to form an active cluster. An enterprise may be further subdivided into a collection of Imprivata sites, which allows for the optimization of traffic patterns between Imprivata-enabled workstations and appliances in large networks. If one appliance in an enterprise fails, the remaining appliances handle all user authentication requests. Users do not experience downtime if the enterprise maintains enough active appliances to handle authentication requests from all users.

The Operating System

The Imprivata appliance uses a Linux-based operating system and is hardened to ensure the highest level of security. Access to the appliance is restricted to HTTPS (SSL) on port 443 for the Imprivata OneSign users and administrators, and HTTPS (SSL) on port 81 for managing the appliance device settings. Data is stored on the appliance in an encrypted database. Only signed software from Imprivata can be loaded on the appliance.

Imprivata Agent

The Imprivata agent is installed on Windows-based workstations, VDI images, and shared servers, such as Citrix Virtual Apps servers. It is a lightweight client that

- Is delivered as an MSI.
- Enforces user authentication, authorization, and user workflow management.
- Provides SSO for enabled applications.

Imprivata agents communicate with the Imprivata Enterprise using Imprivata Secure Exchange (ISX) – a proprietary Imprivata protocol that uses AES 256-bit encryption for securing user data while it is in transit.

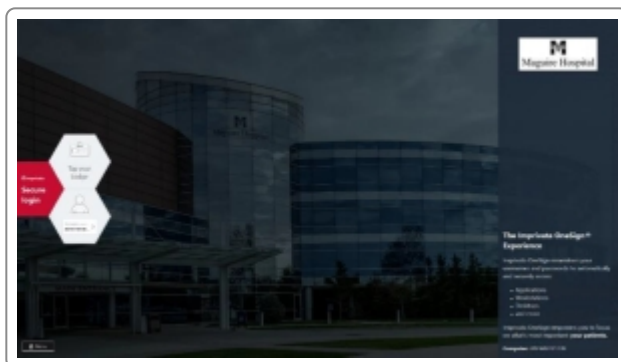
The Imprivata agent can be configured to support a variety of workstation configurations that are frequently used in a healthcare setting:

- Shared workstations – Windows-based shared workstations are configured to automatically logon to Windows using workstation-based credentials (i.e. kioskuser/kioskpassword) during the boot process. The Imprivata agent then secures the workstation with a customizable lock screen.

In this model, a full Windows logon process does not occur when a user authenticates to the workstation; rather, the user’s credentials are verified with Imprivata OneSign and then the workstation is “unlocked.” This allows for a fast logon process and switching between users. This is referred to as Imprivata OneSign Fast User Switching (FUS).

- Private workstations – with Windows-based private workstations, Imprivata OneSign integrates with the standard Windows logon process.

The Imprivata shared workstation lock screen. Click to enlarge.



Imprivata agents are also installed on virtual desktop images in a VDI environment and on Citrix Virtual Apps servers hosting virtualized applications and desktops. In these scenarios, the agent provides single sign-on and advanced authentication functionality in the virtualized environment on behalf of the authenticated user. It can also operate in conjunction with the agent installed on the remote workstation to provide “tap and go” access to virtualized resources using Imprivata Virtual Desktop Access.

Imprivata OneSign Supported Authentication Modalities

Many of the following modalities can be combined to support two-factor authentication (2FA).

For example, a policy can be created to require 2FA using a passive proximity card and domain password. This policy can be enabled for all authentication attempts or it can be configured to require 2FA only at the start of a shift, while providing users with a grace period where they are only required to use one factor (passive proximity card in this example) during the rest of their shift.

Supported authentication modalities. Click to enlarge.



Imprivata Enterprise Design

An Imprivata Enterprise consists of at least two Imprivata appliances that accommodate authentication requests from a collection of Imprivata agents. The appliances are configured to connect to existing IT infrastructure including:

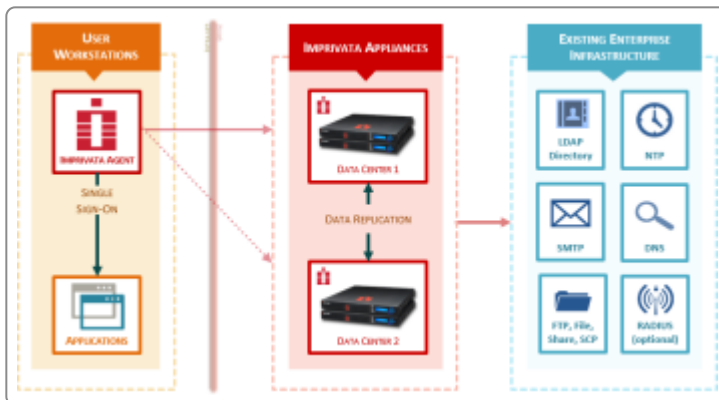
- AD domain controllers
- DNS servers, NTP servers, SMTP servers for alerts
- FTP servers or file shares for storing backups

The connections between the Imprivata agents and the Imprivata appliances use the secure ISX protocol.

Imprivata recommends deploying appliances in pairs in two or more data centers to provide data center-level redundancy. In this configuration, the appliances replicate between data centers, and the agents connect to the appropriate set of appliances based on site configuration and appliance availability.

The Imprivata appliance infrastructure should be deployed behind boundary firewalls alongside other core infrastructure servers. Appliances should never be installed in a DMZ.

The Imprivata agent and appliance architecture. Click to enlarge.



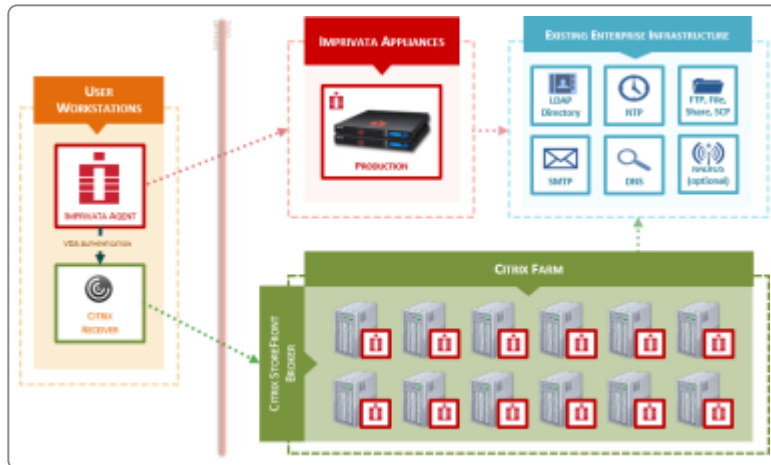
Imprivata OneSign and Application and Desktop Virtualization

Imprivata OneSign supports a variety of desktop and application virtualization delivery solutions including Citrix Virtual Apps and Desktops (formerly Citrix XenApp and Citrix XenDesktop) and VMware Horizon View.

Application Virtualization

In an environment that includes applications that are delivered via application virtualization technology, like Citrix Virtual Apps, Imprivata agents are installed on the user workstations and on each server in the Citrix farm. The agents on the user workstations interact with the locally installed Citrix Receiver to authenticate to Citrix sessions and automatically launch Citrix published applications or desktops, if needed, using Imprivata OneSign Virtual Desktop Access. The agents on the Citrix servers provide single sign-on and advanced authentication to applications hosted on the farm.

The Imprivata OneSign architecture with Citrix Virtual Apps. Click to enlarge.

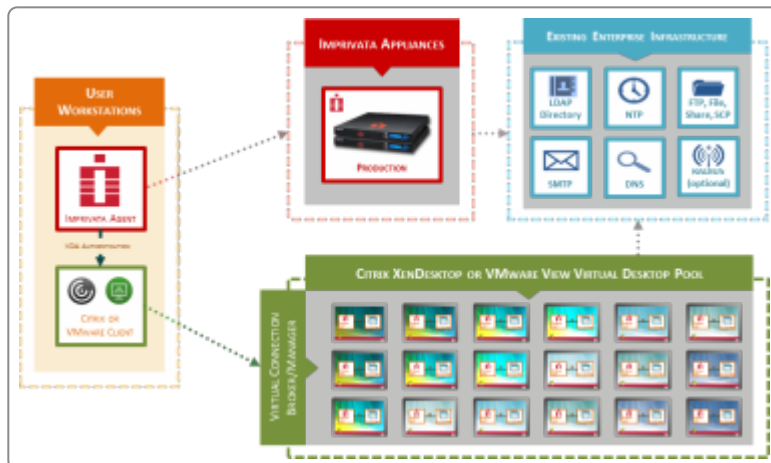


Desktop Virtualization

In an environment where virtualized desktops are delivered via Citrix Virtual Desktop or VMware Horizon View, Imprivata agents are installed on the user workstations and on each virtual desktop instance in the desktop pools that require application single sign-on and advanced authentication.

The Agents on the user workstations interact with the locally installed Citrix Receiver or VMware Horizon View Client to authenticate to and to automatically launch virtualized desktops using Imprivata OneSign Virtual Desktop Access. The agents on the virtualized desktops provide single sign-on and advanced authentication to applications installed on the virtualized desktops.

The Imprivata OneSign architecture with VMware Horizon View or Citrix XenDesktop VDI. Click to enlarge.



Thin and Zero Client Workstations

"Thin or zero" client workstations are an alternative to using Windows-based workstations when delivering virtualized applications and desktops. All applications are delivered to the user via application and/or desktop virtualization technologies.

These devices:

- Can be used to deliver the same – or very similar – end user computing experience.
- Use a lightweight operating system, which is typically Linux-based.

The authentication functionality of the Imprivata agent is built into the operating system (firmware) of most of these devices. They connect to the Imprivata Enterprise using a secure, RESTful API to retrieve configuration information and to handle user authentication requests.

- Are generally less expensive to own and operate than Windows-based workstations.

Imprivata OneSign supports a growing list of thin and zero client devices from vendors such as HP, IGEL, and Dell/Wyse. For a full list of supported application and desktop virtualization technologies, and thin and zero client devices, see the [Imprivata OneSign Supported Components Guide](#).

DATASHEET

Enterprise Access Management (formerly OneSign)

Enterprise single sign-on and virtual desktop access for fast, secure, No Click Access™ to technology endpoints



Streamline and simplify system access

Imprivata has a strong understanding of IT security requirements and offers a broad portfolio of advanced solutions that have been successfully deployed worldwide. Imprivata Enterprise Access Management (formerly OneSign) provides secure and convenient access to mobile, cloud, and on-premises applications, including old legacy applications that are difficult to enable. By improving manual, time-intensive login workflows, users can focus on doing their job instead of struggling with technology. With over 8 million users leveraging Enterprise Access Management (EAM) as their preferred solution for single sign-on (SSO) and virtual desktop access, Imprivata is the recognized leader in digital identity for companies of all sizes in all industries.

- Enables multifactor authentication at technology endpoints to improve security posture for the organization, without creating friction for the users
- Replaces passwords, improves security, and supports compliance requirements for frameworks like CMMC and NIST
- Enables fast, secure access into on-premises, legacy, mobile, or SaaS applications for all users from any device, anywhere
- Offers the industry's broadest native thin and zero client integration
- Saves users time and frustration by improving workflow in how they access applications and information.

Increase user satisfaction, protect corporate data

EAM enables organizations to leverage the full benefits of their technology investments by building transparent, seamless, and convenient security into user workflows, backed by seamless integrations with IT systems and applications. By removing barriers that frustrate users and cause friction – like repetitive manual logins and having to remember long, complex passwords – EAM saves users valuable time and increases satisfaction. In summary, EAM:

- Streamlines user workflows by delivering No Click Access™ to on-premises, mobile, and cloud applications. With just a tap of their building access card or swipe of their fingerprint, users are instantly logged in to their personal device, shared desktop, or shared mobile device. Users are automatically signed into any profiled application – without ever having to type in their username or password.

- Protects data and helps organizations meet compliance and cyber insurance requirements by preventing credential sharing, securing data on unattended workstations, and enabling easier and more thorough auditing and reporting of workstation and application access.
- Simplifies the ability to enforce multifactor authentication without placing a burden on the end user with the need to remember multiple, long, complex usernames and passwords.

Key features of Enterprise Access Management

SSO AND PASSWORD MANAGEMENT

By eliminating the need to repeatedly type usernames and passwords, users can save time and reduce frustration, and can ensure adherence to corporate cybersecurity policies. EAM supports a broad range of authentication methods and devices, including fingerprint biometrics, and FIDO keys/badges that can instantly identify users for desktop access without disrupting their workflows or thought processes.

While EAM largely eliminates the need for passwords, if users forget their password, EAM self-service password management lets them quickly and easily reset it, reducing help desk calls, and improving overall productivity.

“Imprivata has given our users secure and convenient access to data wherever and whenever they need it. This has resulted in improved users satisfaction and increased efficiency, and has ultimately helped to deliver improved productivity.”

– Commercial user, North America

SECURE, FAST USER SWITCHING FOR SHARED WORKSTATIONS

Where shared workstations are implemented, user-specific logins can be time-consuming and frustrating. In the past, organizations have attempted to use generic Windows logins, but these and other workarounds expose various security and manageability issues. Instead, EAM enables secure, fast user switching between concurrent Windows desktops or kiosk workstations, reducing login times, all while protecting data.

NO CLICK ACCESS TO VIRTUAL DESKTOPS

Imprivata EAM with virtual desktop access simplifies and expedites desktop access and application SSO for virtualized environments. These time savings, combined with the roaming capabilities of virtual desktops, deliver convenient mobility for users. EAM with virtual desktop access provides API-level support for VMware, Citrix, and Microsoft RDS. Imprivata also partners with leading thin and zero client hardware and device vendors, including IGEL, HP, and Teradici.

Embedding the Imprivata agent at the device level provides an unparalleled level of integration which gives users seamless access to their desktops, applications, and data, regardless of the technology environment.

CLOUD ACCESS VIA THE IMPRIVATA CLOUD IDENTITY PROVIDER

The Imprivata cloud identity provider (IDP) is a component of EAM that enables fast, secure access to SAML 2.0 web applications. This IDP allows users to access cloud applications from any device, and any location. The Imprivata cloud IDP also integrates with EAM badge-tap access to deliver near passwordless authentication into corporate devices, including shared workstations.

APPLICATION PROFILING

It's easy to enable new applications for SSO and keep application profiles and EAM software up to date. The Imprivata application profile generator (APG) has an intuitive graphical user interface (GUI) that enables administrators to use "drag and drop" functionality to easily profile applications. Imprivata also makes regular updates to EAM, adding new capabilities, and seamlessly accommodating new releases from software vendors, virtualization, mobile and desktop partners, as well as from other technology vendors.

COMPLETE MONITORING AND SIMPLIFIED REPORTING

EAM provides out-of-the-box reports that give administrators full visibility into system and application access and enables rapid response to audit inquiries that would otherwise require IT professionals to perform manual, time-consuming examinations of multiple system or application logs.



Imprivata Managed Services

Imprivata Services (including professional, managed, and education) helps organizations with the implementation of EAM, and informs and guides technical change management and strategic business planning. They act as a supplemental IT resource, providing hands-on support, training, and remote administration. Benefits of Imprivata Services include increased return on investment, reduced complexity, accelerated time-to-value, reduced cyber risks and threats, boosted efficiency, precision, and end user satisfaction. Imprivata Services provides tremendous value to any customers using Imprivata solutions.

Integrated platform-level solution

EAM integrates with other Imprivata and partner solutions that together create a robust digital identity platform. Advanced integration provides secure communication and transaction authentication and enables EAM users to securely access systems on premises, in remote locations, and in virtual environments.

Other Imprivata solutions integrated with EAM include:

- Imprivata Enterprise Access Management with MFA (formerly Confirm ID) – The comprehensive identity and multifactor authentication platform for fast, secure remote access and multifactor authentication workflows across the enterprise. It leverages the same infrastructure as EAM with SSO, which reduces complexity and total cost of ownership.
- Imprivata Identity Governance and Administration – Enable secure day-one, role-based access for all users with end-to-end digital identity lifecycle management. The only identity governance solution that integrates with Imprivata EAM and other Imprivata solutions.
- Imprivata Mobile Access and Control (formerly GroundControl) – Unlock the power of mobility with automated provisioning, secure checkout, fast user access, and lifecycle management for shared Android or iOS mobile devices. Integration with EAM gives users a fast, familiar workflow when accessing shared devices and mobile applications.

- Imprivata Digital Identity Intelligence (formerly FairWarning) – Monitor user activity to spot risky behavior with AI and machine learning- powered intelligence. The only risk analytics solution that integrates with EAM to normalize identities across a broad set of enterprise applications.
- Imprivata Privileged Access Management and Vendor Privileged Access Management (formerly SecureLink Enterprise Access) – Protect privileged accounts from unauthorized access from users with elevated privileges or third party vendors that require system access. A comprehensive, lightweight privileged access management (PAM) and vendor PAM solution, that integrates with EAM and other Imprivata digital identity solutions.



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 1 781 674 2700
or visit us online at www.imprivata.com

Copyright © 2024 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.