

Why Imprivata Insight?

Your success is our mission at Imprivata – and with a view into anonymous summary usage data and statistics, we can help you realize even greater value from your partnership with us.

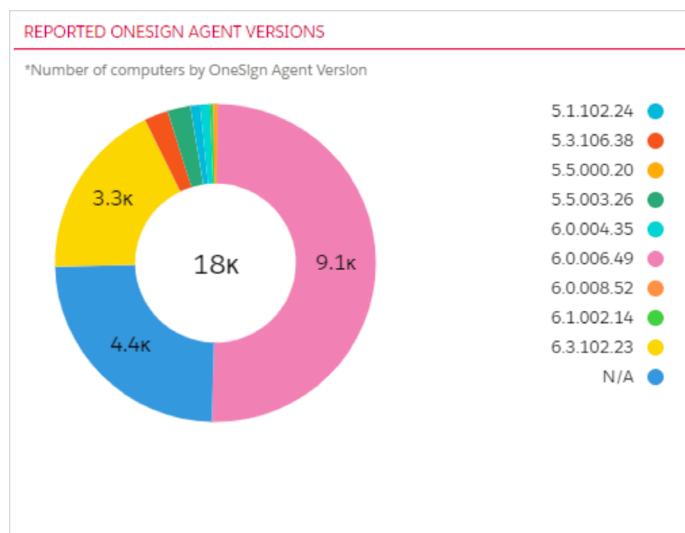
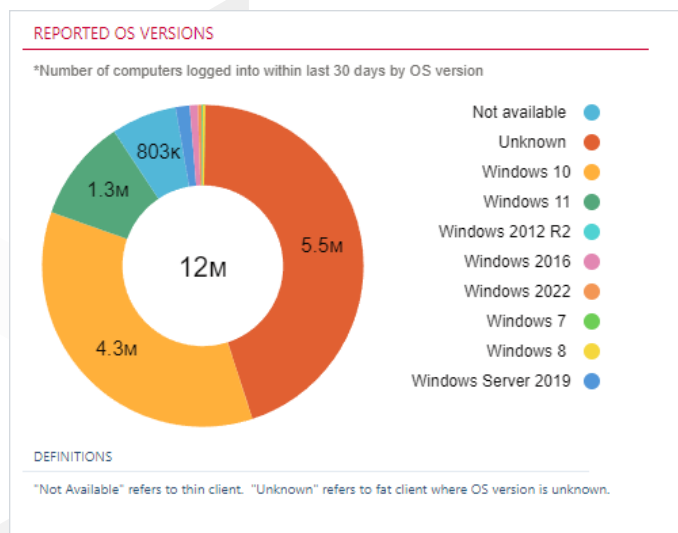
This is where Imprivata Insight comes into play. Imprivata Insight is a tool that captures deidentified aggregate-level usage data and statistics that can be securely reviewed by Imprivata on behalf of our customers for Imprivata Enterprise Access Management (formerly Imprivata OneSign and Imprivata Confirm ID) solutions.

Here's how it works.

Generated reports will look similar to the admin center deployment reports you may be used to, but are aggregated and completely anonymized. Imprivata will have access to dashboards and reports that show usage statistics on a retrospective basis as well as real-time system status and performance statistics.

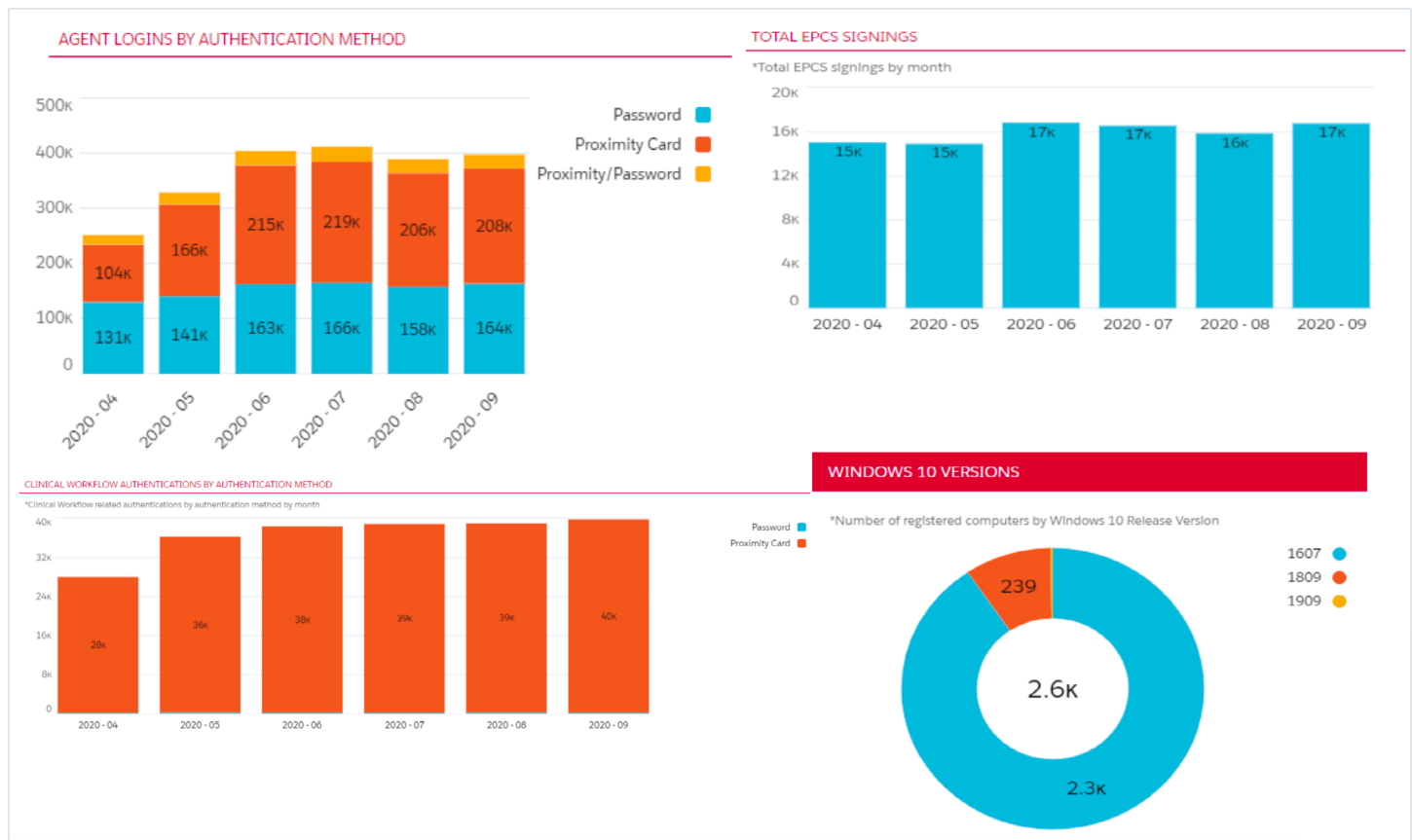
Imprivata Insight data items include:

- License assignment levels
- Aggregated Imprivata Enterprise Access Management (EAM) solution usage trends
- Type of appliance
- Appliance and agent software versions
- Activity counts and audit records
- Replication error reporting



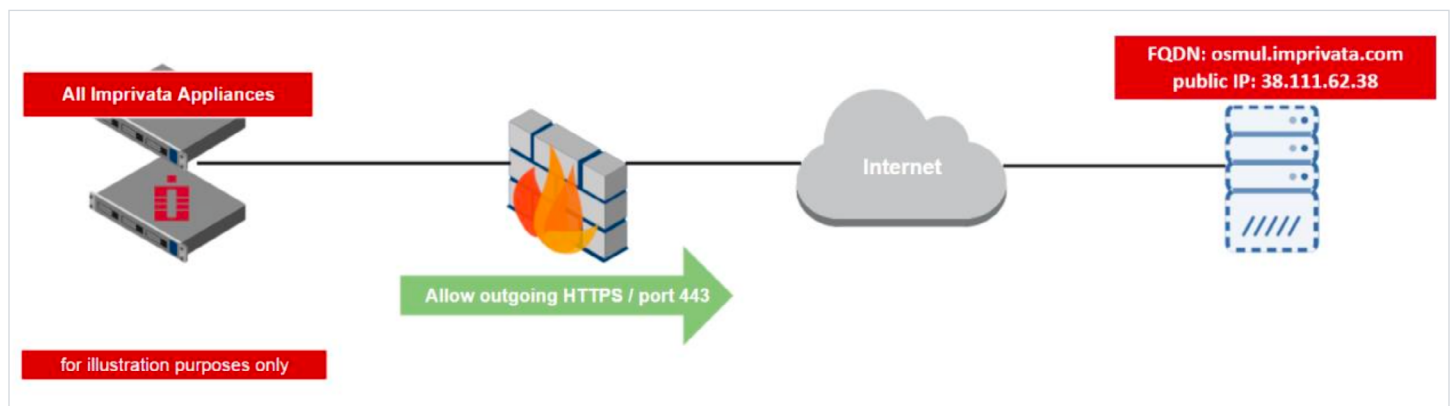
Having this data available, allows Imprivata to offer you better service by:

- Providing our customer experience teams with data driven insights based on your environment
- Allowing for us to be more prescriptive and to help drive the ROI for the Imprivata solutions at your organization
- Allowing Imprivata to proactively identify if you are at risk for a new security threat that requires critical updates to your Imprivata enterprise
- Helping drive conversations around potential software versioning issues, overall environmental compatibility, and potential available new features to your organization



In order to ensure your organization is participating in Imprivata Insight please ensure that :

- Secure HTTPS communication (port 443) is enabled from all Imprivata appliances to our Insight receiver osmul.imprivata.com. This is in your organization's firewall settings, not configurable within the EAM enterprise itself.
- You need to configure your firewall to only permit outbound HTTPS traffic to the IP address destination 38.111.62.38. As a level of assurance, the data is encrypted and sent out over an encrypted link which is restricted to a known host, reducing any security risk. Imprivata is encrypting the data and Imprivata is the only one that can decrypt it. See diagram below for illustration.
- NOTE: We recommend using the FQDN osmul.imprivata.com in the firewall configuration as the IP address can change over time.



Interested in having customized access to insights like these, and the ability to drill down into specific user data at the title- and department-level in your environment? Contact your Imprivata representative to learn about EAM Analytics.



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