Full Customer Communication:

Subject: Sharing Security Best Practices for Imprivata Enterprise Access Management

Dear Customer,

As AI-enabled cyber threats continue to increase in speed and sophistication, Imprivata remains focused on helping customers maintain secure, resilient environments. We are continually reviewing our products, services, systems, and deployment guidance to help raise the bar for security across Imprivata Enterprise Access Management (EAM) and our broader product portfolio.

This work reflects our long-standing commitment to security, privacy, and responsible AI by design. Our Security, Privacy/AI Governance, Security awareness and Product teams continuously assess emerging vulnerabilities, evaluate potential risks, and update our development, operational, and customer guidance as appropriate.

As part of this ongoing effort, we encourage you to review the following operational and administrative best practices for your Imprivata EAM environment. These actions can help maintain a strong security posture and ensure that your organization is well-positioned to receive important updates and support. They are also increasingly important as AI-enabled cyber threats accelerate the speed, scale, and sophistication of potential attacks.

1. Confirm that you are running a supported version of EAM

Please ensure that your organization is using an Imprivata-supported version of EAM. A list of supported versions can be found in our Product Lifecycle Matrix, available on the Imprivata Environment Reference website:
https://docs.imprivata.com/supported/content/help.html

2. Review EAM architecture best practices

Please review the Imprivata EAM Environment Architecture Best Practices guide to confirm that your environment is using recommended settings and configurations to help protect your Imprivata appliances and EAM deployment. The guide is available at:

https://docs.imprivata.com/supported/content/topics/security/bestpractices_architecture.html

3. Enable outbound communications for Imprivata appliances

We strongly recommend enabling outbound communications for your Imprivata appliances. This helps improve visibility into your EAM environment and allows Imprivata to

streamline updates, diagnostics, and support when needed. Guidance is available at: https://docs.imprivata.com/onesign/content/topics/imprivataplatform/appliance/outbounddcomm.html?Highlight=insight

4. Review and update your organization's contact list

Please work with your Imprivata account team to confirm that we have the correct operational, technical and security contacts for your organization. Keeping this information current helps ensure that important communications reach the right people as quickly as possible.

For additional resources, please visit the Imprivata Environment Reference website:

https://docs.imprivata.com/supported/content/help.html. This site includes documentation on supported components, reference architectures, and support policies. We also encourage you to read our whitepaper, Artificial Intelligence at Imprivata: Building Responsible, Explainable, and Purposeful AI.

Imprivata will continue to assess the potential impact of AI-enabled threats on EAM and our other products and services, and any customer-required action will be communicated promptly, with clear guidance and support.

Thank you for your continued partnership.

Sincerely,

Adrian Grbavac

Chief Customer Officer