Go Beyond SSO with Strong Auth & Provisioning

Presented by:

Todd Cramer, Director Product Marketing
Intel Application Security and Identity Products
Intel has moved up the stack with a suite of security solutions for endpoint, networking, and services.

Intel Circa 2000

- Server Security (TXT)
- Trusted Platform Module (TPM)
- AES-NI Encryption

Hardware

Clients (Mobile, Browser)

- Anti-Theft Technology
- Id Protect Technology (IPT)

Applications

- XML Security Gateway
- Tokenization Gateway
- McAfee DLP, email, Web Gateway

Cloud Enablement

- Cloud API Gateway
- McAfee Cloud Security Platform
- Cloud Access 360
- Cloud Builders

Bringing Trust to all layers of the computing stack
Intel® Expressway Cloud Access 360

Enterprise to Cloud SSO
- To the Cloud

Securing Custom or SaaS Apps
- In the Cloud

Combining Enterprise Class Strong Auth with SSO

Provision Access
- Provision/de-provision user accounts
- AD integration
- Sync Id Profiles

Adaptive Strong Auth
- Selectively apply 2nd factor OTP AuthN
- Variety of software AuthN methods & devices - mobile devices, SMS, email

Secure SSO
- Federate windows/AD log in
- To popular SaaS like Salesforce & Google Apps

Regulatory Compliance
- Rich audit trail of user login showing AuthN level
- De-provision & orphan account reports

Go Beyond SSO with Strong Auth and Provisioning
OpenID Implementation
ICAM Trust Frameworks

US ICAM LOA 1 trust framework enables U.S. federal agency websites to begin accepting OpenID and Information Card credentials from OIX certified private-industry providers.
Background

- **Background** - PayPal & Intel implemented a POC to prove how an OpenID provider can enable access to SAML aware apps
- **Challenge** - ICAM community requires LoA2 certification- to be an IdP to high assurance apps. This requires support for SAML
- **Solution** - OpenId to SAML bridge
- **Benefit** - Enables users to leverage private sector credential to access federal apps
OpenID Provider

OpenID Provider e.g. PayPal

Provider Server

Convert to SAML

Intel Expressway Cloud Access 360

User Log-in w/OpenID to access high assurance app that is SAML aware

LoA 1 App

Cost savings and expanded audience that can access app

LoA 2 App

Able to target high assurance verticals as ID provider

Login (Browser)
Enterprise Leverage OpenID w/Strong Auth

- Leverage OpenID over internal AD (e.g. Contract workers or affiliates)
- Add 2nd factor authentication to OpenID
- Convert to SAML for accessing LoA 2 level apps
Service Providers - Who want to Accept Open Ids w/Strong Auth

- Have applications accept both direct login and federated authentication
- Add 2\textsuperscript{nd} factor authentication
More Info

Cloud ID Jam Session

2 Webinars with
*Strong Auth
*Provisioning
July 27 & 28

Demos

www.intel.com/go/identity