PRODUCT BRIEF
Intel® Expressway Cloud Access 360
Capabilities and Features

Intel® Expressway Cloud Access 360

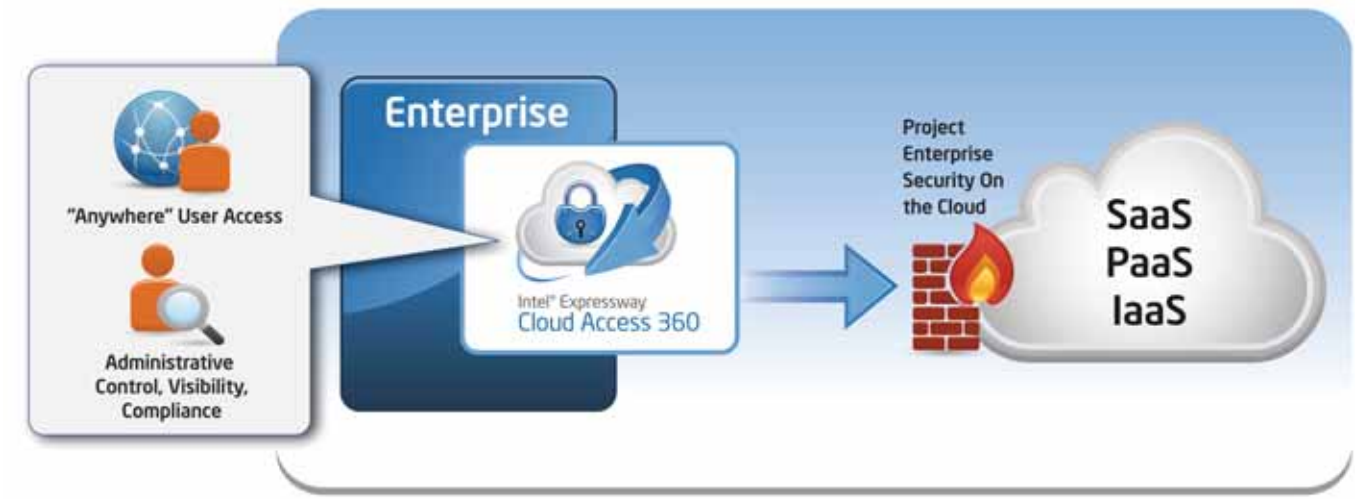
Intel's broad suite of hardware and software security solutions delivers unmatched endpoint, identity assurance, and application security. Unifying these foundational components across Intel technologies is core to Intel's 2015 Cloud Vision for a Federated, Automated, and Client Aware cloud.

Product Highlights:

Intel® Expressway Cloud Access 360 (Intel® ECA 360) software is the first solution suite designed to control the entire lifecycle of access security for enterprises and their partners connecting to the cloud applications.

- **Control:** The identity lifecycle with account de-provisioning and automatic identity data syncronization to maintain data quality. Enforce context-aware authorization, deliver integrated strong and elevated authentication, and empower users with seamless SSO from multiple devices–all tied to authoritative IdM systems.
- **Visibility:** Monitor user, administrator and API access activity…receive alerts against SLAs…all from a central administrative console.
- **Compliance:** Protect access to sensitive information with strong authentication soft/hard OTP, maintain audit records of identity lifecycle events, and correlate cloud user activity with on-premise logs for end-to-end compliance. Detect orphan accounts and de-provision to meet industry regulations.
- **Protecting Client to Cloud:** Deploy mission critical apps in the cloud and apply sophisticated client aware security policies to ensure requests are received from an attested client device or application.

Figure 1: 360 Access for the Cloud



Cloud Security Complexity

The Barrier to Adoption

Cloud applications are enabling new business and IT models through hosted and elastically scalable applications. Yet, the adoption has been slow due to overwhelming security complexity and lack of solutions that can effectively project an enterprise class security model on the cloud. As Figure 2 indicates, key barriers are focused around loss of control, lack of visibility, and adherence to regulatory compliance.

Drilling deeper into these concerns reveals specific functional gaps (Figure 3) with cloud security. Today users have set up redundant accounts with weak passwords that are disconnected from the corporate identity infrastructure, user actions in SaaS apps have no oversight or authorization—leading to sensitive data leakage and compliance risks, and lack of standardized logs block administrators from monitoring or correlating cloud user activity with internal audit repositories.

Figure 2: Barriers to Cloud Adoption

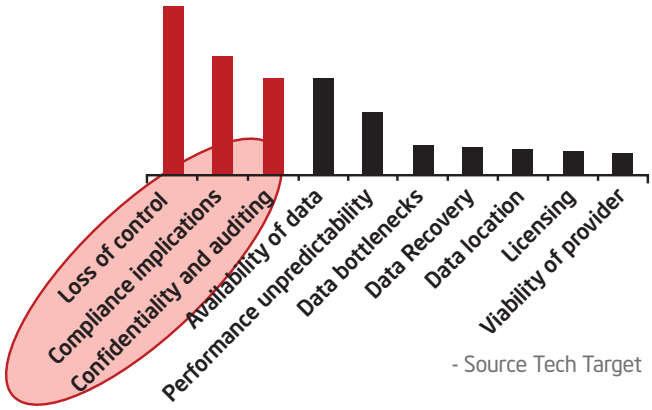
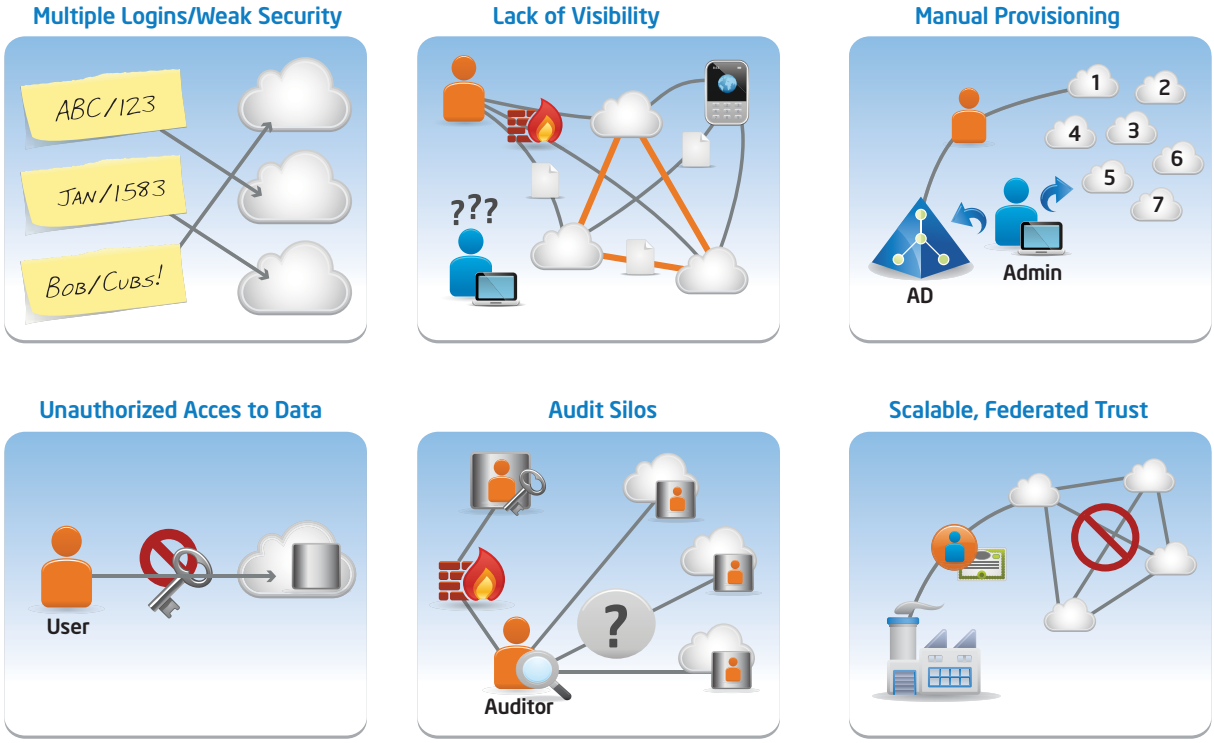


Figure 3: Functional Gaps



The Federation Glass Ceiling

So how does the Enterprise regain control in an environment where security models change by cloud provider or are left entirely up to the enterprise?

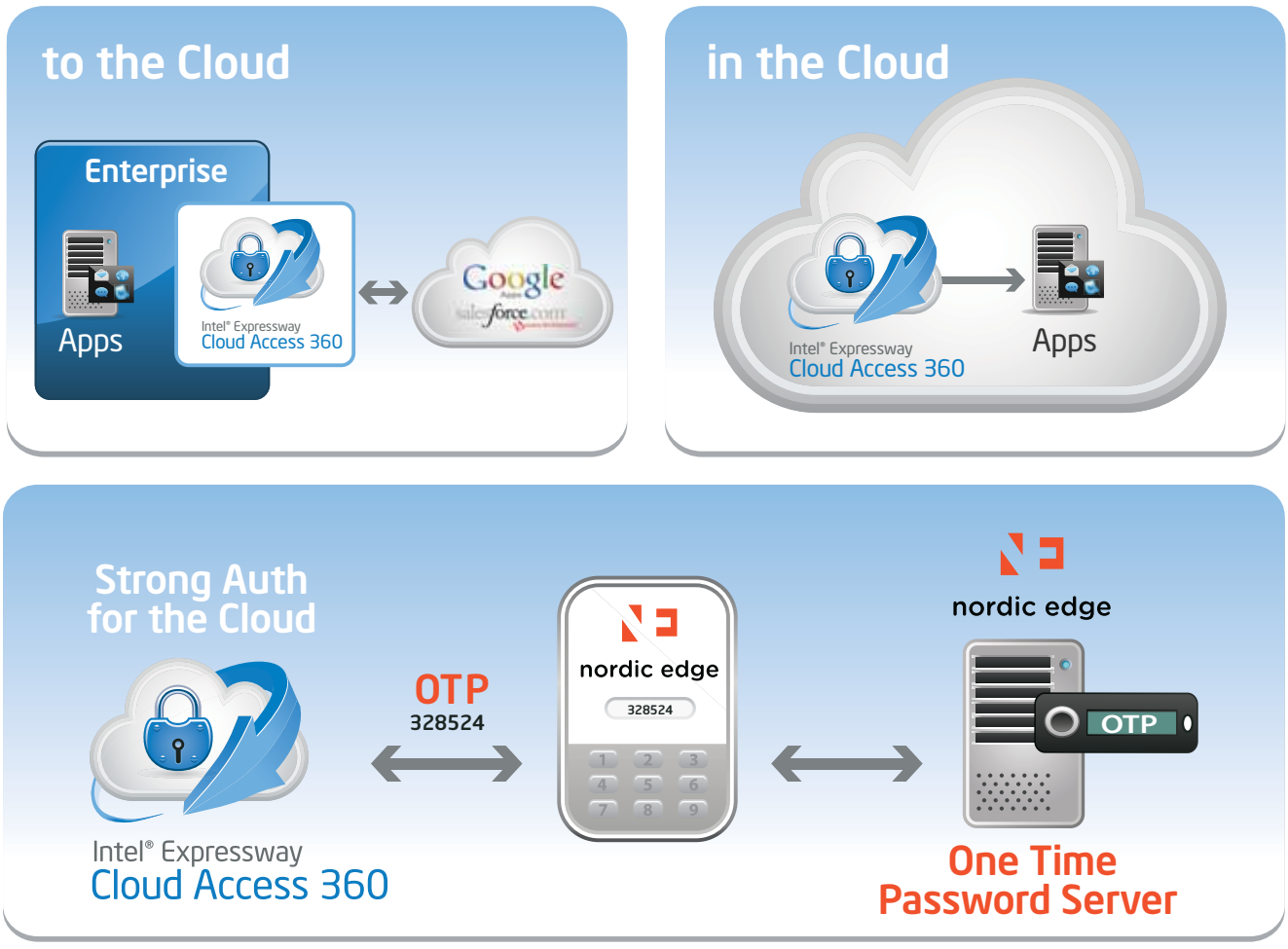
Why not just extend internal access management systems? These systems were designed to work inside of the firewall where trust is implied and proprietary agent based integrations could be forced on one or two departmental application domains.

Point federation solutions based on SAML emerged as a light weight approach to provided simple authenticated access to SaaS applications. While limited adoption solutions occurred, enterprises found federation had a glass ceiling that could not be scaled fast enough across providers. The cause? Federation solutions had a narrow scope that still required manual provisioning of accounts, provided no authorization model, and lacked integration with strong authentication technologies- a prerequisite for access to sensitive corporate data. Until the full spectrum of requirements are met corporate America has been hesitant to move beyond simple pilots or tightly controlled private clouds.

Solutions to Control the Lifecycle of Access to the Cloud

Intel® ECA 360 forms a suite of Intel & Nordic Edge identity technologies that can be deployed to secure enterprise user access to SaaS providers and to protect access for custom enterprise applications deployed in the cloud.

Figure 4: Intel & Nordic Edge Solutions



Solutions to Control the Lifecycle of Access to the Cloud (continued)

Intel® ECA 360 is based on proven, standards-based, technology previously only available from point solution vendors but now available as an integrated suite:

Intel® Expressway Cloud Access 360

Nordic Edge™ One Time Password Server (Add on)

SSO-Intel® ECA 360 has a web based administrative console, (see Figure 5 below) that makes it easy to view, author, and control access policy by cloud provider. Packaged with the solution are first mile "session look-up" connectors to common IdM & enterprise platforms such as Microsoft* SharePoint and "last mile" session creation & account provisioning connectors to popular SaaS and PaaS platforms. Federated authentication and authorization protocols are based on SAML, XACML, and emerging OAuth & Open ID identity standards that can connect internet based identity providers (e.g. Facebook) with corporate identities and authorization policy.

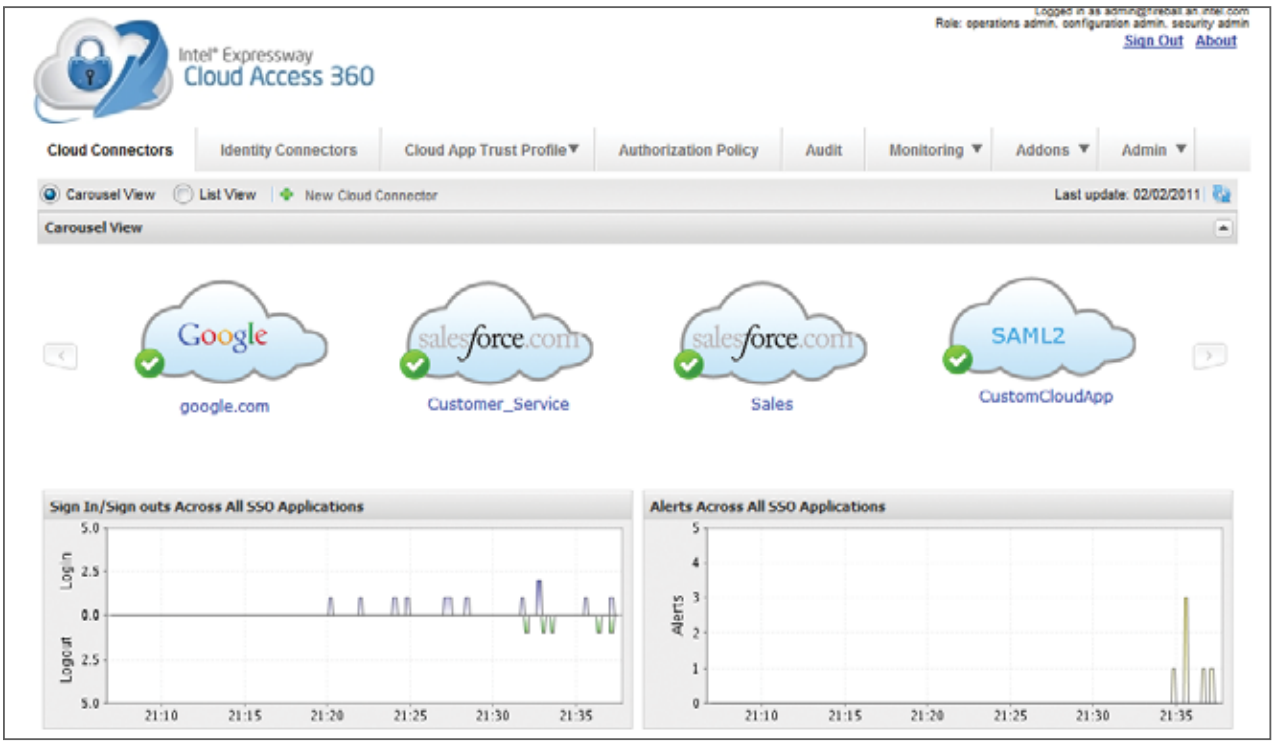
Provisioning-A rich set of account provisioning & de-provisioning functions are delivered by the embedded provisioning engine. No more manual account creation as provisioning of accounts is seamlessly pushed from the enterprise to all cloud applications authorized for corporate use. Key attributes can be fetched from multiple authoritative attribute sources (SPML capable provisioning systems, directories, databases) and kept in sync across cloud providers as updates are made.

Mobile Strong Authentication- Cloud access is becoming increasingly mobile. This means that the access to your cloud applications must be accessible regardless of time and place. This requires a higher step up to strong authentication, going beyond basic user name and password. The Nordic Edge™ One Time Password Server delivers second factor authentication from mobile clients. When logging into enterprise or cloud applications, after entering username and password, a one-time password is required. The OTP can be delivered to cell phones via SMS (Flash or storable), e-mail, chat programs, or generated using the mobile client-Pledge.

"With increased SaaS adoption, our clients are seeking a full spectrum of Enterprise class IT controls to improve manageability, visibility, security & compliance for the cloud applications. Our strategic partnership with Intel enables us to deliver Expressway Cloud Access 360, one of the most complete suite of cloud access control capabilities in market today."

- Sudip Banerjee
CEO, Larsen & Toubro Infotech

Figure 5: Centralized Admin Console & Visibility



Enterprise Client Attestation- For sensitive cloud applications, the enterprise will only allow access from attested enterprise laptops or PC clients that are confirmed to be free of malware. Federated SSO a nd even strong authentication technologies do not present enough assurance to allow access to mission critical cloud applications. To solve this weakest link in the secure client to cloud connection, Intel has released:

Intel® IPT Identity Protection Technology (on all 2011 Intel® Core™ Platforms)

With a computer using Intel IPT, a web-site/enterprise can now validate that you are logging in from a trusted PC. In addition to your username and password, the PC will generate a unique code at time of log-in to verify you are using the PC registered with your account. The technology works within the embedded Intel® Chipset ME (Management Engine) isolated from the operating system. The one time codes are supported by multiple third party security solutions providing an end-to-end solution.

Protecting Cloud Services- Cloud security is not just about safe user access…its also about ensuring on premise or cloud hosted apps can securely expose and initiate system to system web service interactions for internal developers, or any application that needs to access data on the user's behalf. Based on mature, ten year old technology, Intel has provided the leading XML Security Gateway in market:

Intel Expressway Service Gateway (Software and Tamper Proof Hardware Appliance Editions)

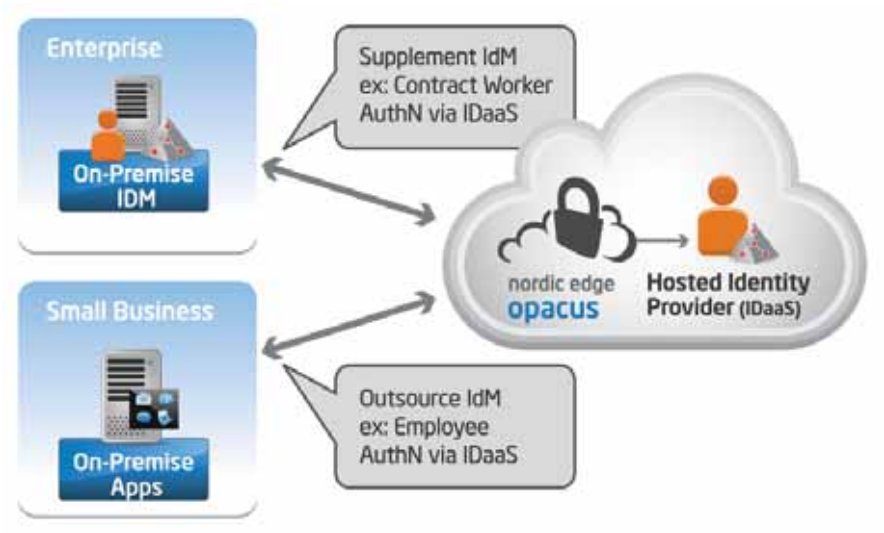
The appliance is deployed as a proxy at the network edge to address common XML, and SOA problem areas such as acceleration, SOAP & REST security, service mediation, runtime governance, API security, and STS security token mapping for enterprise to cloud services.

Identity as a Service IdaaS (IDaaS)
For SMB and many enterprises, the time has come to supplement their internal IdM or Active Directory based infrastructure with a more agile cloud hosted identity solution. Larger companies commonly benefit from the IDaaS approach when managing contract workforce identities that should not be co-mingled in the corporate directory. In either case, existing on-premise IdM infrastructure can be leveraged as needed for a blended on-premise and IDaaS approach. Intel & Nordic Edge stands apart from start-up solutions in the IDaaS market to bring a new level of trust and world class service with:

Nordic Edge* Opacus (Hosted, on demand, multi-tenant IDaaS)

Nordic Edge Opacus provides a fully hosted solution designed to provide 360 access for multi-tenant, SaaS and custom cloud applications. SSO, provisioning, strong auth, monitoring, and connector integration can easily be managed from a single cloud console- all tied back to on-premise applications and infrastructure. With an IdaaS solution, your company can focus on administration versus SLAs, scalability, and software upgrades.

Figure 6: Identity as a Service



Bringing it All Together- Intel Trusted Client to Cloud

Ubiquitious User Access

So what does 360 access mean for the user? 360 access means a trusted client to cloud session from any mobile device, browser, any corporate or home network, or even using preferred Internet identity accounts such as Facebook-all connected to corporate access policies and accounts.

Administrative Control, Compliance, Visibility

For administrators, 360 access and CONTROL is achieved from a single administrative console where complex role-based access, time, network, and location based authorization policies are authored and enforced by provider. COMPLIANCE is delivered with account de-provisioning reports and aggregated audit logging correlated with log management platforms. VISIBILITY means monitoring user activity and developer API access across cloud applications and provider platforms.

Enterprise Class Security and Trust

Corporations can venture beyond private clouds with the addition of enterprise class security for the cloud. Intel enables step-up OTP strong authentication from mobile devices or trusted corporate PCs—effectively extending a dynamic enterprise security perimeter around user and system interactions with the cloud.

Cloud Standards

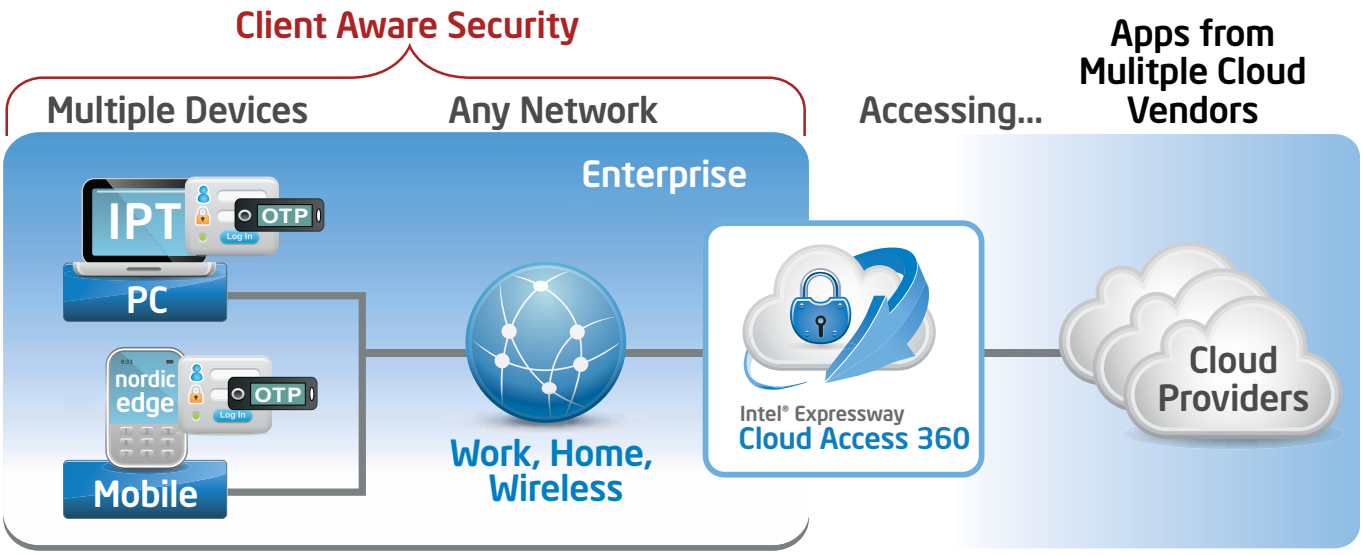
At an industry level, Intel & leading solution providers have formed the Intel® Cloud Builders program to define and prototype reference cloud architectures. Intel Expressway has a reference architecture for the "Cloud Access" usage model. Intel is also a member of the Cloud Security Alliance which promotes the use of best practices for providing security assurance within cloud computing.

Intel is a proud sponsor of the CSA

cloud security alliance℠

Intel® Cloud Builders Reference Architectures

Figure 7: Trusted Client to Cloud



Intel® Expressway Cloud Access 360 Capabilities

Category	Description
Control	• Cloud access management (authentication, authorization, SSO, federation, SLO) • Cloud provisioning & de-provisioning (account, role, automated & bulk provisioning) • Embedded Virtual Directory to support split users and split profile scenarios • Auto-sync of identity data between enterprise and cloud applications for change management scenarios • First mile SSO with on-premise apps • Last mile Federated SSO with cloud apps • 2 factor strong authentication: soft & hardware OTP including Intel Trusted Platform Module (TPM).
Visibility	• Monitoring of user activity using charts and reports across providers • (Change) Alerts (email/SMS/SNMP) for provisioning/de-provisioning, and access SLA events • Export report data to CSV for import into 3rd party tools
Compliance	• Audit of end user and admin activity • Orphan accounts reporting • Single audit repository and common record format across cloud applications • Export audit report to CSV or pdf for importing into 3rd party tools • Audit stores: Database, File

Technical Specifications

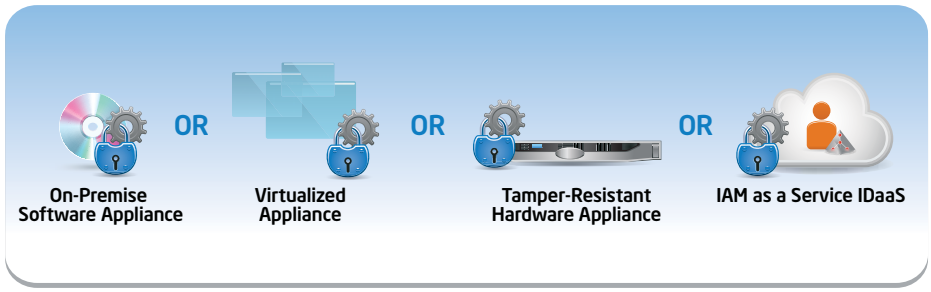
Category	Description
Salesforce.com Connector	• Federated SSO • Salesforce data access using OAuth • Multiple connectors supported by a single product instance • Salesforce Connect for Outlook • 3rd party vendor and custom apps deployed on Force.com platform • Automated account (de) provisioning, user identity attribute synchronization, support for split users and split profiles
Google Apps Connector	• Federated SSO • Google data access using OAuth • Multiple connectors supported by a single product instance • 3rd party vendor and custom apps deployed on Google AppEngine • Automated account (de) provisioning, user identity attribute synchronization, support for split users and split profiles
Custom Connector	• Federated SSO into any 3rd party vendor or custom app that supports SAML, OpenId or OAuth standard
Application Integrations	• Sharepoint 2007/2010, .NET 2.0 and above
Manageability	• Centralized admin console • Command line and scripting support • Test to Production Migration
Certificate Management	• CRL and OCSP based certificate revocation check
User & Data Stores	• Any LDAP v3 compliant directory • Central Authentication Service (CAS) 3.3/3.4.2 • Data Store(Optional) for monitoring & auditing. • Any JDBC supported database
Standards	• SAML 2, Open Id, OAuth, XACML, LDAP v3, JMX
Deployment	• On premise or in the cloud • Look aside or reverse proxy mode • Software, virtual appliance, Amazon EC2, or DMZ ready hardware appliance (Cloud IAM in a box) •Horizontal migration for test to production support

System Requirements	• Browser: Intenet Explorer 6, 8, Firefox 3.6
	• Server Operating System: 32 bit or 64 bit
	  • Redhat Enterprise Linux Server and Advanced Platform 5.0
	  • Windows 2003, 2008
	• Hardware requirements: Any Intel multi core server with 2 GB RAM

Select from Multiple Form Factors

Intel Expressway products are available in multiple form factors. Choose to deploy flexible software on generic server hardware or opt for high assurance hardware with Common Criteria EAL 4+, FIPS 140-2 Level 3 Crypto, and optional HSM Module.

Figure 8: Form Factors



SOLUTION PROVIDED BY:

Intel® Expressway Cloud Access 360

Enabling Trusted Client to Cloud Access

More Information and Partner Program Details

Expressway:
www.dynamicperimeter.com

Nordic Edge OTP Server:
www.nordicedge.se

IPT (Identity Protection Technology):
http://ipt.intel.com

North America Phone: 978-948-2585

EMEA Phone: +46 8 122 07 500

E-mail: intelsoainfo@intel.com

Printed in USA

Please Recycle

Cloud Access Product Brief 324905-002 US