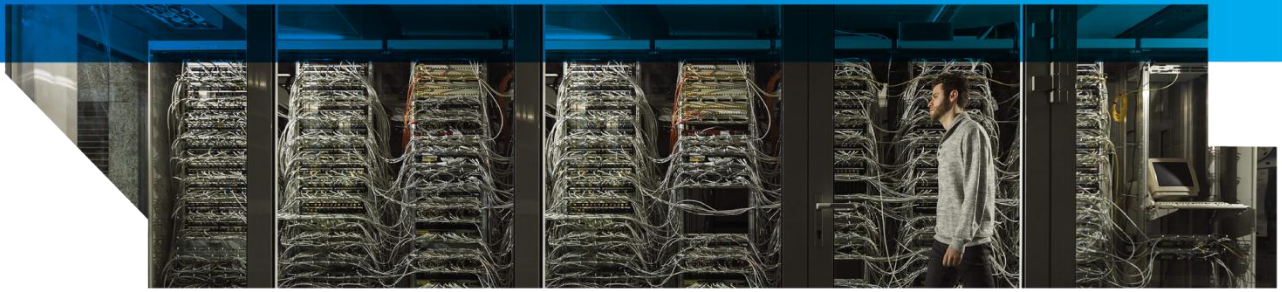
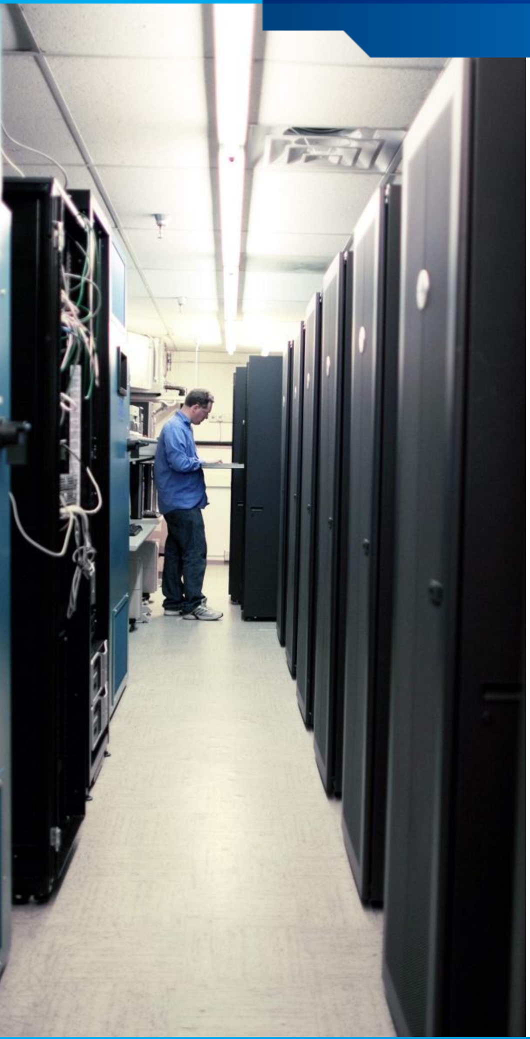
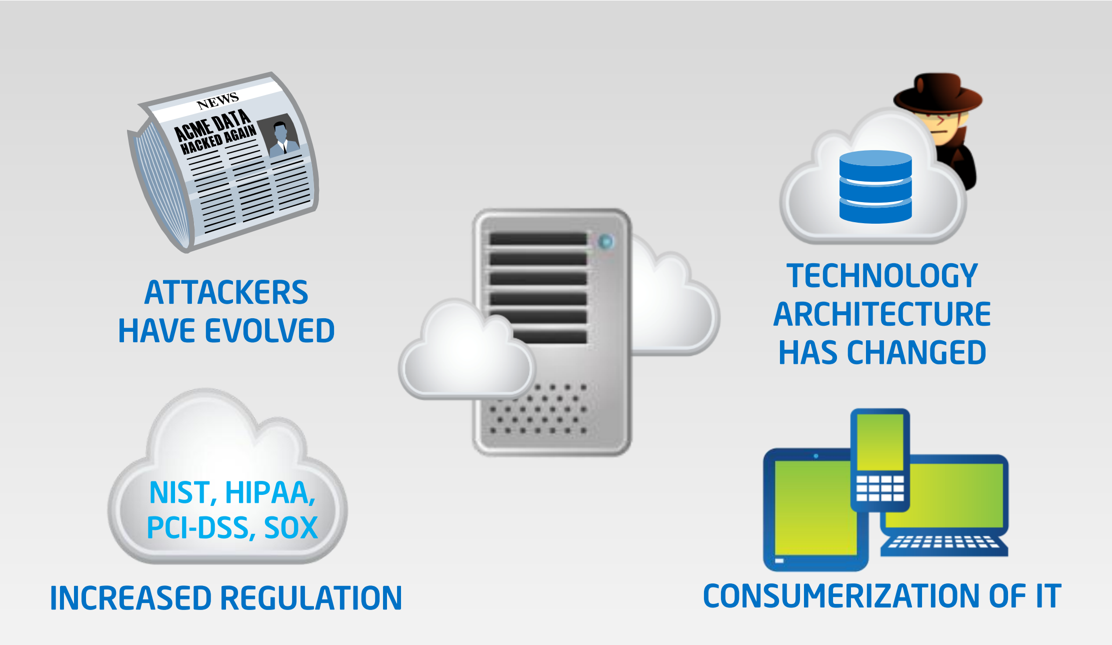
CLOUD SECURITY:
Secure Your Infrastructure



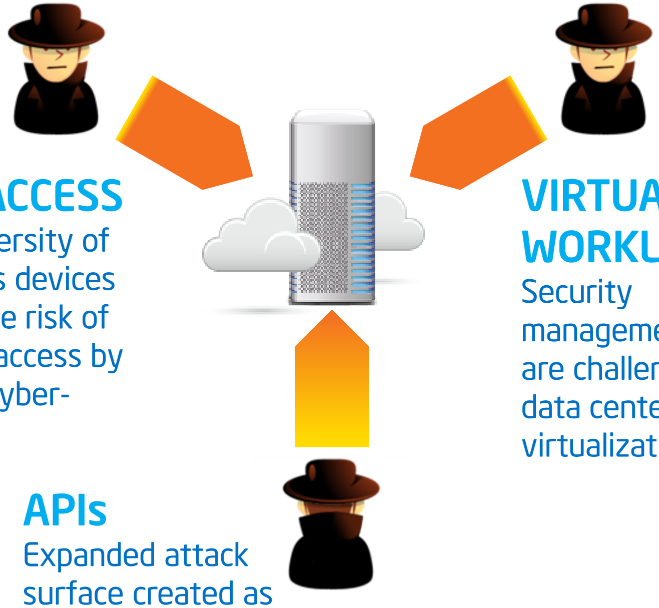
Challenges to security



Security challenges are growing more complex.



Understanding the risks



CLIENT ACCESS

Growing diversity of client access devices increases the risk of illegitimate access by hackers or cyber-criminals

VIRTUAL WORKLOADS

Security management tools are challenged by data center virtualization

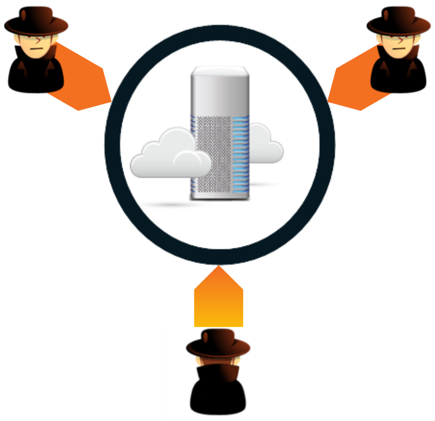
APIs

Expanded attack surface created as apps are shared via APIs from cloud to mobile

Protect yourself

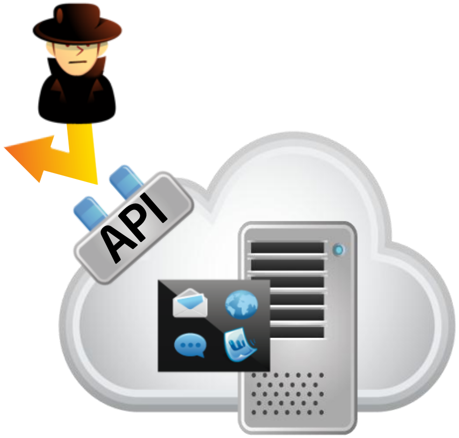
CLIENT SECURITY

Help protect client data so only authorized users can access the cloud



TRUSTED COMPUTE POOLS

Build trust and transparency in cloud infrastructure

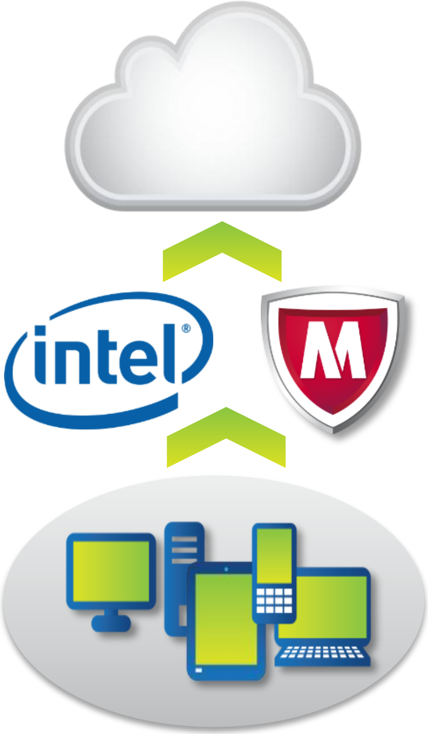


APPLICATION API CONTROL

Manage APIs at the network edge where application services are consumed and exposed with partners, devices, and developers

Secure your clients

Protection by Intel and McAfee



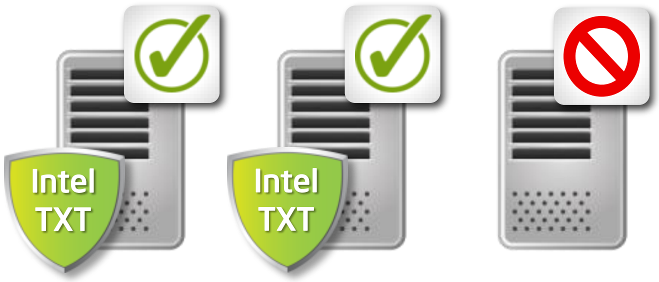
- **Intel® Identity Protection Technology (Intel IPT)[1]**— Hardware-based two-factor authentication for client access
- **McAfee Cloud Identity Manager** — Federated single sign-on to cloud applications
- **McAfee Deep Defender** — Monitors and roots out malware attacks below the operating system

[1] No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd gen Intel® Core™ processor enabled chipset, firmware and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit ipt.intel.com.

It’s all about trust

Protect your data and workloads by establishing trusted compute pools using Intel® Trusted Execution Technology (Intel TXT).[1]

- Provide a foundation for trust in cloud infrastructure by measuring integrity of virtualized infrastructure
- Protect data and workloads by deploying them on trusted virtualized infrastructure
- Create transparency to enable audit and governance in cloud deployments



[1] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit intel.com/technology/security.

Application Layer Security

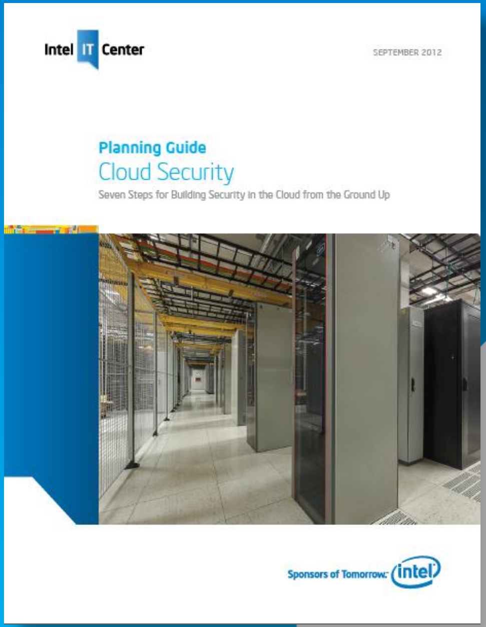
Intel Expressway Service Gateway. Software appliance that acts as an API proxy where security policy is enforced, legacy applications & data are orchestrated, and mobile APIs are exposed to developer communities.

Move to the cloud with confidence

Intel hardware-based security helps protect your infrastructure so you can feel more confident about moving to the cloud.

- More secure client access
- Trusted compute pools
- API controls at the edge

We'll help you get started



Intel IT Center

SEPTEMBER 2012

Planning Guide

Cloud Security

Seven Steps for Building Security in the Cloud from the Ground Up

Sponsors of Tomorrow. intel

> *It is no longer the case that security around the perimeter will hold. You have to assume that compromise is inevitable in any compute model. In order to manage the risk you have to set up a more granular trust model.*
>
> *Malcolm Harkins*
> *Intel Vice President of Information Technology Group*
> *and Chief Information Security Officer*

DOWNLOAD NOW!

Download the *Cloud Security Planning Guide* and discover valuable information on how to protect YOUR data, from device to data center.

http://www.intel.com/content/www/us/en/cloud-computing/cloud-security-checklist-planning-guide.html

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at any time, without notice.