Legal Disclaimers

- Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at [www.intel.com](http://www.intel.com).

- Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.


- All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Copyright © 2018 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Inside, the Intel Inside logo, and Intel Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.*
Level 100 Course Content

Technology Overview
Value Proposition
Overview
Roadmap
IsecL v1 Architecture
Use Cases
Deployment Scenarios
Next Steps
Security continues to be #1 barrier for cloud adoption

Cloud Adoption Barriers

#1 General security risks
33%

#2 Lack of staff resources or expertise
28%

#3 Integration with existing IT environments
27%

#4 Data loss & leakage risks
26%

#5 Legal & regulatory compliance
24%

Main Cloud Security Concerns

Data loss/leakage
57%

Data privacy
49%

Confidentiality
47%

Legal and regulatory compliance
36%

Data sovereignty/control
30%

Data from Cloud Research Partners
DATA CENTER SECURITY DRIVERS & CUSTOMERS ASKS

**KEY DRIVERS**

- Increased multi-cloud adoption
- More regulatory controls (GDPR, HIPPA, PCI)
- Advanced cyber threats attacks
- Increased distributed data and intelligence

**KEY ASKS**

- Platform supply chain integrity
- Platform resilience
- Platform integrity assurance
- Data protection & sovereignty
- Protect keys
- Visibility, controls & compliance
INTEL DATA CENTER SECURITY STRATEGY

Effective security is built on a foundation of trust

- TRUST
- RESILIENCE
- VISIBILITY/CONTROL

SECURE THE PLATFORM

- AT-REST
- IN-FLIGHT
- IN-USE

PROTECT THE DATA

WITHOUT COMPROMISING

PERFORMANCE
Key Customer Challenges/Questions
The need for Intel Security Libraries

Is the platform/network/application/workload safe from tampering, theft, loss, ...?

Can we TRUST the cloud provider?

Is the platform/network/application/workload running on the right HW, OS, location, ...?

Is the platform compromised in any way, ...?
What is ISecL?

Intel ISecL is a set of software libraries and components that expose and enable Intel security features. The libraries are used by ISecL services to secure platforms and protect data.

ISecL Architecture

- Library-centric model to expose & utilize Intel security features.
- Components and services to enable key Cloud security Use Cases
- Aligned with platform schedules starting Cascade lake
- Extensible “Flavor” based model for managing trusted configurations
- Support for RHEL*, Microsoft Windows Server*, VMWare vSphere*

- Allows for **Turn Key Solutions**
- **Easy & Customized Solutions**
- **Easier Upgrades**
- **Improved Code Organization**

*Other names and brands may be claimed as the property of others.
# ISEC ALIGNMENT TO PLATFORM ROADMAP

<table>
<thead>
<tr>
<th>Platform Security Technologies</th>
<th>Purley-Refresh (v1)</th>
<th>Whitley (v2 and v3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel TXT / TPM, OTA</td>
<td>Intel TXT / TPM, OTA</td>
<td>Intel TXT / TPM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure UEFI, Boot Guard, OTA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MK-TME, SGX-TEM, PFR2.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Integrity</td>
<td></td>
<td>Application Integrity</td>
<td>SSD Attestation</td>
</tr>
<tr>
<td>Data Sovereignty</td>
<td></td>
<td>VM &amp; Container Integrity</td>
<td>Verified &amp;/or Measured Boot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM &amp; Container Confidentiality</td>
<td>with HWROT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Memory Isolation for VMs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PFR Visibility</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Key Protection</td>
</tr>
</tbody>
</table>

Intel® Trusted Execution Technology (Intel® TXT)
Intel® Security Libraries v1 Architecture

- Platform Integrity Assurance
- Asset Tagging for Data Sovereignty
- Integration for OpenStack* & K8S*
- Intel’s End to End Solution
- Customer Turn Key Solution
- RH*, Windows* and VMWare*

*Other names and brands may be claimed as the property of others.
## Mapping of Libraries & Components: ISECL

### Library
- Platform Info (PIL)
- TPM Provider (TPL)
- Flavor (FVL)
- Verifier (VFL)
- Host Connector (HCL)
- Workload Measurement Library (WML)
- Workload Decryption Library (WDL)

### Components and Services

<table>
<thead>
<tr>
<th>Library</th>
<th>Trust Agent</th>
<th>Verification Service</th>
<th>Workload Policy Manager</th>
<th>Key Broker</th>
<th>Workload Agent</th>
<th>Application Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Info (PIL)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TPM Provider (TPL)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flavor (FVL)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verifier (VFL)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Connector (HCL)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workload Measurement Library (WML)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workload Decryption Library (WDL)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Intel Security Libraries Main Use Cases

**Use Model 1: Platform Integrity**
Attestation provides information to inform us of which systems are trustworthy for hosting our workloads.

**Use Model 2: Data Sovereignty**
Hardware-based TPM Asset Tags allow individual platforms to be location tagged to control the physical location of workloads.

**Use Model 3:** Individual libraries can be used to expose and utilize security features built into Intel Silicon in custom applications.
Deployment Scenarios with ISECL

Scenario 1
- Verification Service
- Trust Agent

Platform Integrity & Data Sovereignty for Windows®/RHEL®

Scenario 2
- Verification Service
- VMWare Vsphere®

Platform Integrity & Data Sovereignty for VMWare®

Scenario 3
- PlatformInfo
- TPM Provider

Secure Discovery of Intel Security Features

Scenario 4
- Trust Agent
- Customer Verification Service

Custom Implementation of Platform Integrity

*Other names and brands may be claimed as the property of others.
For more Info:

Reference Collaterals:

ISecL v1 Product Guide
ISecL v1 100-LVL Training
ISecL v1 200-LVL Training
ISecL v1 Package

Next Steps: Refer to ISecL v1 200-Level Training
Detailed Features and APIs, BKCs, Deep Dive Functional Flows and Library Integration and Key Learnings
BACKUP
## Library Functions

<table>
<thead>
<tr>
<th>Library</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Info</td>
<td>Collect server hardware information (e.g, Intel® TXT, TPM version, etc.) and OS information</td>
</tr>
<tr>
<td>TPM Provider</td>
<td>Provides a coherent APIs for basic TPM functions to support verification service, regards of TPM version, type, and OS</td>
</tr>
<tr>
<td>Host Connector</td>
<td>Connects to different types of host (Linux*, Windows*, ESX*) to retrieve host and TPM quote information</td>
</tr>
<tr>
<td>Verifier</td>
<td>Verifies host report against a defined flavor</td>
</tr>
<tr>
<td>Flavor</td>
<td>Create flavors (trusted information) from a host report</td>
</tr>
<tr>
<td>Privacy CA</td>
<td>Generates and manage certificates for AIK certificate, binding and signing certificates</td>
</tr>
<tr>
<td>SAML Generator</td>
<td>Generates a SAML report for attestation report</td>
</tr>
<tr>
<td>Tag Creator</td>
<td>Utility library to help create asset tags and generate asset tag certificates</td>
</tr>
</tbody>
</table>

*Other names and brands may be claimed as the property of others.*
What Do We Mean When We Say...

**Integrity**

Integrity is the state of being whole and undivided.

In the context of a platform, this means the state of the platform being whole and un-tampered.
Attestation is the process of validating that something is true or trusted.

In the context of a platform, attestation means the process of validating that the platform is trusted or maintains its integrity.
What Do We Mean When We Say...

Assurance

Assurance is a positive declaration intended to give confidence.

In the context of a platform, assurance means providing the confidence that the platform components are authentic.