IT@Intel White Paper

Intel IT
IT Best Practices
Information Security
January 2011

Rethinking Information Security to Improve Business Agility

Omer Ben-Shalom
Principal Engineer, Intel IT

Manish Dave
Senior Security Engineer, Intel IT

Toby Kohlenberg
Senior Security Analyst, Intel IT

Dennis Morgan
Security Strategist, Intel IT

Stacy Purcell
Senior Security Architect, Intel IT

Alan Ross
Senior Principal Engineer, Intel IT

Timothy Verrall
Principal Engineer, Intel IT

Tarun Viswanathan
Security Architect, Intel IT

Executive Overview

To enable rapid adoption of new technologies and usage models—and provide protection in an evolving threat landscape—Intel IT has embarked on a radical five-year redesign of Intel's information security architecture.

We believe this architecture, designed to support key initiatives such as IT consumerization and cloud computing, represents a novel approach to enterprise security. It provides more flexible, dynamic, and granular security controls than traditional enterprise security models. For example, the architecture is designed to dynamically adjust a user's access privileges as the level of risk changes, depending on factors such as location and the type of device used—such as a trusted mobile business PC or an untrusted personal smartphone. The architecture also focuses heavily on survivability, based on the assumption that compromise is inevitable.

The new architecture is based on four pillars:

- **Trust calculation.** This calculation dynamically determines whether a user should be granted access to specific resources and the type of access that will be provided. It is based on factors such as the user's client device and location, the type of resources requested, and the security controls that are available.
- **Security zones.** Our environment is divided into zones, ranging from trusted zones containing critical data, with tightly controlled access, to untrusted zones containing less-valuable data and allowing broader access. Communication between zones is controlled and monitored; if one zone is compromised, this prevents the problem from spreading to other zones.
- **Balanced controls.** To increase flexibility and the ability to recover from a successful attack, the model emphasizes the need for a balance of detective and corrective controls in addition to preventative controls such as firewalls.
- **User and data perimeters.** Recognizing that protecting the enterprise network boundary is no longer adequate, we need to treat users and data as additional security perimeters and protect them accordingly.

Not all of the security technologies required for full implementation of this model exist today; we are actively encouraging development of technology to support capabilities such as the trust calculation.

We have begun implementing this architecture and plan to drive adoption across Intel over approximately five years. Use of this approach has already delivered results by helping us deliver innovative solutions to challenging use cases while actually reducing risk.

Use of this approach has already helped us deliver innovative solutions to challenging use cases while actually reducing risk.

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BUSINESS CHALLENGE

Intel's enterprise security requirements are changing—and expanding—rapidly. This is due to the adoption of new usage models such as cloud computing and the consumerization of IT, as well as the rapidly evolving threat landscape.

Intel's risk profile is shown in Figure 1. Key trends include:

Consumerization of IT

Many of Intel's highly mobile employees want to use their own consumer devices, such as smartphones, for work. This increases productivity by enabling employees to collaborate and access information from anywhere, at any time. To support this, we already provide limited access to corporate data, such as e-mail, from employee-owned smartphones and tablets.[1]

As this trend grows, we will need to provide employees with a level of access to Intel resources from an expanding continuum of client devices, some of which have much weaker security controls than mobile business PCs.

We need a security architecture that enables us to more quickly support new devices and provide access to a greater range of applications and data, without increasing risk to Intel. We need to be able to dynamically adjust the levels of access we provide and the monitoring we perform, depending on the security controls of the client device. For example, an employee should have more limited access to valuable enterprise resources when using a less-secure device such as a smartphone than when using a secure, managed PC.

1 "Maintaining Information Security while Allowing Personal Hand-Held Devices in the Enterprise." Intel Corporation, November 2010.

New Business Needs

Intel is expanding into new markets through both organic growth and acquisitions, and is also developing systems for online collaboration with business partners. As a result, we need to provide access to a broader range of users, many of whom are not Intel employees.

To support and fuel this growth, we are implementing new systems, such as an online sales portal, that expose Intel data to new customers. We also need to be able to smoothly integrate acquired companies and provide them with access to the resources they need. In general, we need to quickly enable access by new users while minimizing risk and providing selective, controlled access only to the resources they need.

Cloud Computing

Intel IT is implementing a private cloud based on virtualized infrastructure, and we are also exploring the use of external cloud services for non-critical applications. In these cloud

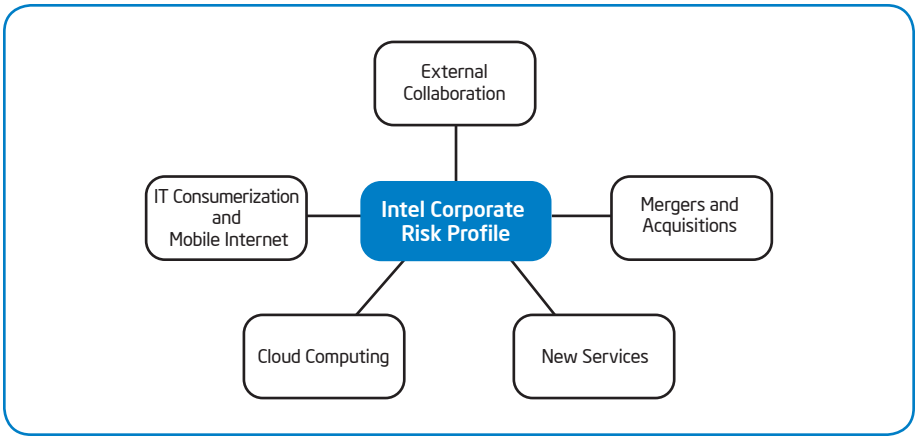

Figure 1. Evolving security requirements drive the need for a new security architecture.

environments, systems and their data are virtualized and may migrate dynamically to different physical or logical network locations. This makes it difficult to effectively restrict access using traditional security controls such as firewalls, which assume that the locations of systems and the data they contain are static. We need much more granular and dynamic controls that are linked to the resources themselves rather than just their network location. We also need security technology that provides better platform protection and better protection of data both in flight and at rest, and we are evaluating new Intel®-based server technology that provides this.

Changing Threat Landscape

The threat landscape is evolving rapidly. Increasingly, attackers are taking a stealthy approach, creating malware that quietly gains access and attempts to remain undetected in order to maintain access over time. As the number of threats increases and new types of malware emerge, we need to assume that compromise is inevitable.

Traditional enterprise security architectures have relied largely on preventative controls such as firewalls located at the network perimeter. However, our primary focus has shifted to providing controlled access to a broader range of users and devices, rather than simply preventing access. In addition, the continually changing threat landscape makes it necessary to assume that compromise will occur. Once an attacker has gained access to the environment, the preventative controls they have bypassed are worthless. Although these perimeter controls will continue to have some value, we need to emphasize tools that increase the ability to survive and recover once attackers have gained access to the environment.

The Need for a New Architecture

We realized that as security requirements continue to evolve and expand, traditional enterprise security strategies would no longer be adequate. We need a more flexible and dynamic architecture to enable faster adoption of new devices, use models, and capabilities; provide security across an increasingly complex environment; and adapt to a changing threat landscape.

Accordingly, we formed a team, which included members from across Intel IT, to devise a fresh approach to enterprise security, design an architecture from scratch to support new requirements, and then determine how to implement this new architecture across our existing IT environment.

SECURITY ARCHITECTURE

The team developed a radical five-year redesign of Intel's security architecture. We believe our plan represents a novel approach to enterprise security.

Our goal was to develop an architecture that enables greater flexibility and employee productivity while supporting new business requirements and technology trends, including IT consumerization, cloud computing, and access by a broader range of users. At the same time, the architecture is designed to reduce our attack surface and improve survivability—even as the threat landscape grows in complexity and maliciousness.

We have set a five-year timeline for adoption because implementation requires extensive effort across Intel IT, and because not all of the required technologies exist today.

The architecture moves away from the traditional enterprise trust model, which is binary and static. With this traditional model, a user is in general either granted or denied access to all resources; once granted, the level of access remains constant. The new architecture replaces this with a dynamic, multi-tiered trust model that exercises more fine-grained control over access to specific resources. This means that for an individual user, the level of access provided may vary dynamically over time, depending on a variety of factors—such as whether the user is accessing the network from a trusted managed PC or an unmanaged personal smartphone.

Five Irrefutable Laws of Information Security

Our new model assumes that compromise is inevitable; therefore, the ability to survive and recover from compromise is key. These five laws of information security, devised by Malcolm Harkins, Intel Chief Information Security Officer and General Manager, Information Risk and Security, explain why compromise is bound to occur.

1. **Information wants to be free.** People want to talk, post, and share information—and they increase risk by doing so.
2. **Code wants to be wrong.** We will never have 100 percent error-free software.
3. **Services want to be on.** Some background processes always need to be running and can be exploited by attackers.
4. **Users want to click.** People naturally tend to click when they see web links, buttons, or prompts. Malware creators know this and take advantage of it.
5. **Even a security feature can be used for harm.** Security tools can be exploited by attackers, just like other software. This means that laws 2, 3, and 4 are also true for security capabilities.

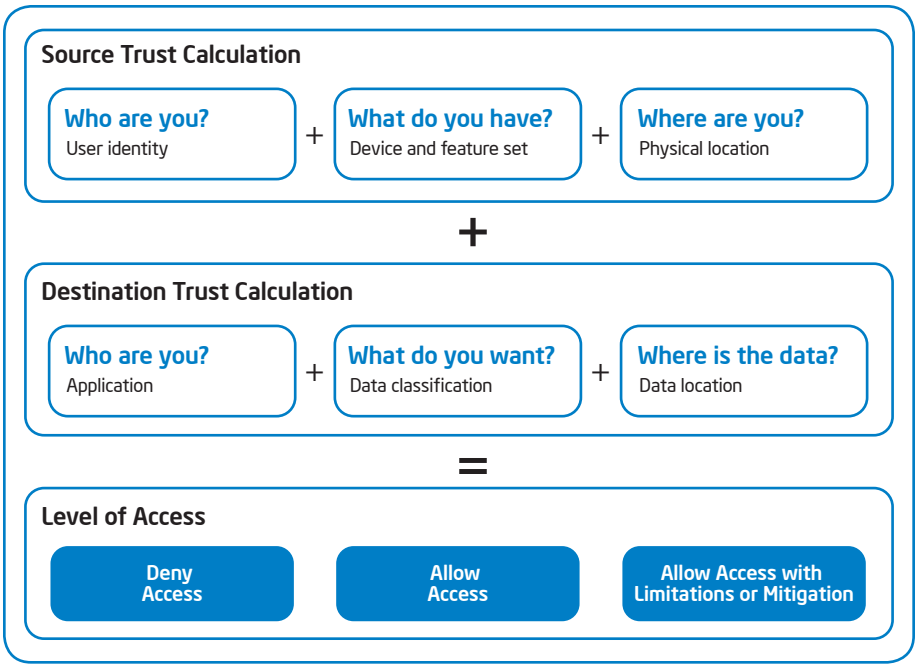

Figure 2. The trust calculation takes into account who, what, and where for both source and destination.

The architecture is based on four pillars:

Trust calculation. This unique element of the architecture is used to dynamically determine whether a user should be granted access to specific resources and, if so, what type of access should be granted. The calculation is based on factors such as the user's client device and location, the type of resources requested, and the security controls that are available.

Security zones. The environment is divided into multiple security zones. These range from trusted zones containing critical data, with tightly controlled access, to untrusted zones containing less-valuable data and allowing broader access. Communication between zones is controlled and monitored; this helps ensure users can only access the resources for which they have been authorized and prevents compromises from spreading across multiple zones.

Balanced controls. To increase flexibility and the ability to recover from a successful attack, the model emphasizes the need for a balance of detective and corrective controls in addition to preventative controls such as firewalls.

User and data perimeters. Recognizing that protecting the enterprise network boundary is no longer adequate, we need to treat users and data as additional security perimeters and protect them accordingly.

The four pillars are described in more detail below.

Trust Calculation

The trust calculation plays an essential role in providing the flexibility required to support a rapidly expanding number of devices and usage models.

The calculation enables us to dynamically adjust the level of access provided as well as the level of monitoring performed, depending on factors such as the user's current client device and the network they are using.

It calculates trust in the interaction between the requestor (source) and the information requested (destination). The calculation consists of a source score and a destination score, and also takes into account the controls available to mitigate risk. As shown in Figure 2, the result of this calculation determines whether the user is allowed access and the type of access provided.

The calculation also takes into account our confidence in each element of the scores, to address the challenge of not always being able to trust the data at our disposal.

Not all of the technology required for the trust calculation exists today; we are actively encouraging development of this technology within the information security industry.

SOURCE SCORE

Trust in the source, or requestor, is calculated based on the following factors:

Who. The identity of the user or service requesting access and our confidence level in the authentication mechanism used—how confident are we that users are who they say they are?

What. The device type, its control capabilities and our ability to validate those controls, and the extent to which Intel IT manages the device. For example, a managed mobile business PC is more trusted than an unmanaged consumer smartphone.

Where. The user or service's location. For example, a user who is inside the Intel enterprise network is more trusted than the same user connecting through a public network. There may also be other considerations, such as the geographical region where the user is located.

DESTINATION SCORE

This is calculated based on the same three factors, but these are considered from the perspective of the destination—the information the source is trying to access:

Who. The application that stores the requested data. Some applications can enforce greater controls, such as enterprise rights management (ERM), and therefore provide a higher level of trust.

What. The sensitivity of the information being requested and other considerations such as our ability to recover it if compromise occurs.

Where. The security zone in which the data resides.

AVAILABLE CONTROLS

The trust calculation also takes into account the security controls available for the zone. If the only controls available are controls that simply block or allow access, we might deny access due to lack of other options. However, if we have extensive preventative controls with highly granular levels of access, detailed logs, and highly tuned detective controls—as well as the ability to recover from or correct problems—then we can allow access without creating additional risk.

CALCULATING TRUST

The trust calculation adds the source score and the destination score to arrive at an initial trust level. The available controls are then considered to make a final decision about whether access is allowed and, if so, how. This calculation is performed by a policy decision point (PDP), a logical entity that is part of the authentication infrastructure and makes access control decisions based on a set of policies.

Based on the results of this calculation, the PDP may make of the following decisions:

- Allow access.
- Deny access.
- Allow access with limitations or mitigation.

The trust calculation allows us to dynamically apply granular control over access to specific Intel resources.

For example, employees using IT-managed mobile business PCs with Intel® Core™ vPro™ processors and additional hardware features such as a trusted platform module (TPM), a cellular data communications card with global positioning system (GPS), and full disk encryption would be allowed access to more resources than when using their personal smartphones. In turn, they would be allowed more access with smartphones than when using public kiosks.

Employees directly connected to the Intel network would be provided with greater access than when using a public network. If we are unable to verify the location of a high-security device such as a managed PC, we would allow less access.

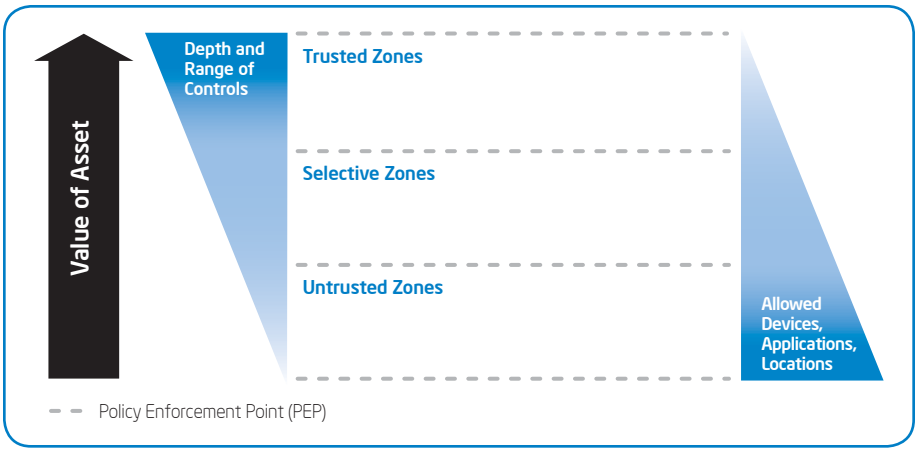

Figure 3. As the value of an asset increases, the depth and span of controls increase, while the number of allowed devices, applications, and locations decrease.

The trust calculation also can be used to differentiate between smartphone models; we could provide different levels of access based on smartphone manageability, authentication capabilities, and installed applications.

We anticipate situations in which the trust level is not adequate to allow any access, but there is still a business requirement to allow a connection or transaction to occur. In these conditions, the result of the trust calculation could be a decision to allow access with limitations or with compensating controls that mitigate the risk. For example, a user might be allowed read-only access or might be permitted access only if additional monitoring controls are in place. One method may be to use a system that displays the requested information to the user, but does not actually transmit the information to the user's device.

Security Zones

We segment the environment into multiple security zones. These range from untrusted zones that provide access to less valuable data and less important systems to trusted zones containing critical data and resources.

Because the zones requiring a higher level of trust contain more valuable assets, we protect them with a greater depth and range of controls, and we restrict access to fewer types of devices and applications, as shown in Figure 3. However, devices allowed access to higher-trust zones also have more power—they may be able to perform actions that are not allowed within lower-trust zones, such as creating or modifying enterprise data.

Aligning the infrastructure in this fashion provides an excellent way to right-size security controls so that security resources are utilized effectively. It also improves the user experience by enabling employees to choose from a wider range of devices, such as smartphones, for lower-risk activities.

Access to zones is determined by the results of the trust calculation and is controlled by policy enforcement points (PEPs). PEPs may include a range of controls, including firewalls, application proxies, intrusion detection and prevention systems, authentication systems, and logging systems.

Communication between zones is tightly restricted, monitored, and controlled. We separate zones by locating them on different physical LANs or virtual LANs (vLANs); PEPs control communication between zones. This means that if one zone is compromised, we can prevent the problem from spreading to other zones or increase our chances of detection if it does spread. In addition, we can use PEP controls such as application proxies to provide devices and applications in lower-trust zones with limited, controlled access to specific resources in higher-trust zones when required.

We anticipate three primary categories of security zone: untrusted, selective, and trusted. Within the zones, there are multiple subzones.

UNTRUSTED ZONES

These zones host data and services (or the interfaces to them) that can be exposed to untrusted entities. This allows us to provide widespread access to a limited set of resources from non-managed devices, such as smartphones, without increasing the risk to higher-value resources located in other zones. Untrusted zones might provide limited access to enterprise resources, such as corporate e-mail and calendars, or they might simply provide Internet access.

We regard these zones as "shark tanks," with a high risk of attack and compromise. Accordingly, we focus on detective and corrective controls to mitigate this risk. These might include a high level of monitoring to detect suspect activity and correction capabilities such as network-based system shunning and dynamic removal of user privilege.

We anticipate a need to provide controlled access from these zones to resources in higher-trust zones. For example, an employee using a smartphone might be allowed limited, read-only access to customer data located in a trusted zone; or, the smartphone might need access to a directory server in a trusted zone to send e-mail. We expect to provide this controlled access using application proxies. These PEP controls act as secure intermediaries—evaluating the request from the device, gathering the information from the resource in a trusted zone, and passing it to the device.

SELECTIVE ZONES

Selective zones provide more protection than untrusted zones. Examples of services in these zones are applications and data accessed by contractors, business partners, and employees, using client devices that are managed or otherwise provide a level of trust. Selective zones do not contain critical data or high-value Intel intellectual property. Several selective subzones provide access to different services or users. As with untrusted zones, application proxies can be used to access resources in selected zones when needed.

TRUSTED ZONES

Trusted zones host Intel's critical services, data, and infrastructure. They are highly secured and locked down. Examples of services within these zones are administrative access to data center servers and network infrastructure, factory networks and devices, enterprise resource planning (ERP) applications, and design engineering systems containing intellectual property. Accordingly, we might only allow direct access to these resources from trusted systems located within the enterprise network, and all access would be monitored closely to detect anomalous behavior.

Balanced Controls

Over the past decade, enterprise security has focused heavily on preventative controls such as firewalls or intrusion prevention systems. This approach offers clear benefits: It is less expensive to prevent an attack than to correct problems after one has occurred, and it is easy to see when firewalls have successfully prevented an attempted compromise.

However, the new security model requires that we balance preventative controls with detective (monitoring) and corrective controls, for several reasons.

First, the focus of the new model is on enabling and controlling access from a wider range of users and devices, rather than on preventing access. Second, the continually changing threat landscape makes it necessary to assume that compromise will occur; all preventative controls will eventually fail. Once attackers have gained access to the environment, the preventative controls they have bypassed are worthless.

By increasing the use of detective controls, and implementing more aggressive corrective controls, we can mitigate the risk of allowing broader access. These controls also increase our ability to survive and recover from a successful attack.

We can use security business intelligence (BI)—analysis and correlation of data gathered by monitoring—to detect and thwart possible attacks. For example, security BI can detect and prevent anomalous situations such as a user who apparently logs in from two different locations at the same time.

The balance between preventative, detective, and corrective controls will vary, depending on the security zone. For example, in untrusted zones, we allow broader access to very limited resources and mitigate risk by increased use of detective and corrective controls. Redundancy within each type of control can be used to provide additional protection.

Possible examples of using detective and preventative controls include the following:

- An Intel employee attempts to send a classified document to a non-Intel e-mail address. Monitoring software detects the attempt, prevents the document from being sent outside the firewall, and asks the Intel employee if he really intended to do this. If the employee confirms that this was intended, the document may be transmitted—or if the document is highly sensitive, a redacted version may be sent.
- Inappropriate use of an ERM-wrapped document results in revocation of access to the document.
- The system allows access to specific documents but tracks the activity. A user can download a few documents without causing concerns. However, if the user attempts to download hundreds of documents, the system slows down the speed of delivery (for instance, only allowing 10 to be checked out at a time) and alerts the user's manager. If the manager approves, the user is given faster access.

- The detection of an infected system places the system on a remediation network, isolating the system and restricting access to enterprise information and applications. The system may retain some ability to access corporate assets, but all activity is closely logged to enable incident response if necessary.
- When a system is found to be compromised, we examine all its recent activities and interactions with other systems. Additional monitoring of those systems is automatically enabled.

Users and Data: The New Perimeters

With the proliferation of new devices, and users' expectations that they should be able to access information from anywhere at any time, traditional enterprise network security boundaries are quickly becoming more porous.

This means that network perimeter defenses become less and less effective on their own. While we must continue to protect the network perimeter where it makes sense, we need to supplement this with a new focus on the primary assets we are trying to protect: Intel's intellectual property, infrastructure, other critical data, and systems.

To protect these assets, the new architecture expands our defenses to two additional perimeters: the data itself and the users who have access to the data.

DATA PERIMETER

Important data must be protected at all times—when it is created, stored, and transmitted. To this end, we are implementing technologies such as ERM and data leak prevention (DLP) to watermark and tag data, and integrate protection with the data itself. For example, with ERM, the creator of a document can define exactly who has access rights throughout the life of the document and can revoke access at any point.

The Security Architecture in Action: A Day in the Life of an Intel Employee

This example (see Figure 4) describes how the new security architecture enables the Intel sales force to access the information they need in the course of a day. At the same time, the architecture protects Intel's security by dynamically adjusting the level of access provided, based on the user's device and location, and by monitoring for anomalous behavior.

1. **The employee travels to a customer site.** The employee is using a personal smartphone and is allowed access only to services in untrusted zones. From here, the employee can view limited customer information, including recent orders, extracted from an enterprise resource planning (ERP) system in a trusted zone—but only through an application proxy server, which protects the trusted zone by acting as an intermediary, evaluating information requests, accessing the ERP system, and relaying the information to the user.

   If the smartphone requests an abnormally large number of customer records—an indication that the smartphone may have been stolen—further access from the smartphone is blocked. To help understand the reason for the anomalous access, there is increased monitoring of the employee's attempts to access the system from any device.
2. **The employee reaches the customer site** and logs into the Intel network from an Intel-owned mobile business PC. Because this device is more trusted, the employee now has access to additional capabilities available in selective zones, such as the ability to view pricing and create orders that are relayed by an application proxy to the ERP system in a trusted zone.
3. **The employee returns to an Intel office** and connects to the corporate network. Now the employee is using a trusted device from a trusted location and has direct access to the ERP system in a trusted zone.

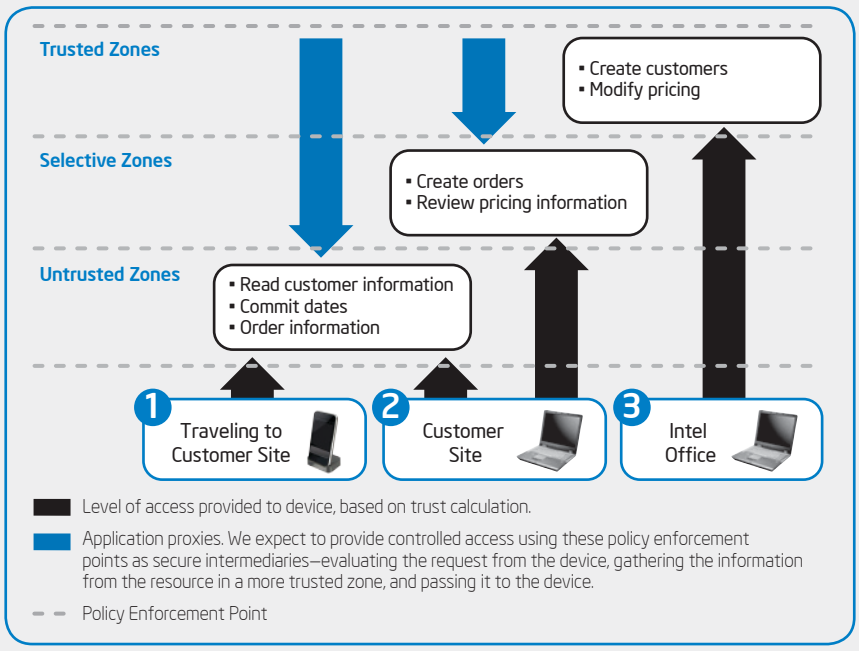

Figure 4. Our new security architecture provides the information employees need to do their jobs while protecting Intel's information assets.

USER PERIMETER

Users can become security risks for a variety of reasons. They are targeted more frequently in social engineering attacks, and they are more vulnerable to these attacks because their personal information is often readily available on social networking sites. They may also click on malicious links in e-mail, download malware, or store data on portable devices that then are lost.

Detective controls can be used to encourage more secure behavior; for example, alerting users when they attempt to send classified documents outside the firewall may make them more security-aware in the future. We have also found that a combination of training, incentives, and other activities can help instill information security and privacy protection into the corporate culture, and successfully encourages employees to own responsibility for protecting enterprise and personal information.

CONCLUSION

Our enterprise security architecture is designed to meet a broad range of evolving requirements, including new usage models and threats. Our goal is to allow faster adoption of new services and capabilities while improving survivability.

We began implementing this architecture about one year ago and plan to drive adoption across Intel over approximately five years. We have already seen some successes. Use of this approach has enabled us to deliver solutions to challenging use cases while actually reducing risk. For example, we implemented balanced controls and trust zones to enable network access from employee-owned devices. In some cases, projects have seen their security overhead decrease by adopting this model.

We anticipate that the architecture will be valuable in addressing the security challenges of cloud computing. In a virtualized cloud environment, it is difficult to effectively restrict access using traditional security controls such as firewalls, which assume that the locations of systems and the data they contain are static. The new architecture, by employing tools such as the trust calculation, provides more dynamic and granular control over access to specific resources. In addition, by increasing the use of detective and corrective controls, we are able to mitigate the weaknesses of currently available preventative controls.

While not all the security technologies required for full implementation of this model exist today, we do not believe any of them are out of reach. We are actively encouraging research and development of technology to support all required capabilities, such as the trust calculation. At the same time, to realize the full benefits of this architecture, we are working to ingrain it into all aspects of Intel IT, from development to operations.

FOR MORE INFORMATION

- "Maintaining Information Security While Allowing Personal Hand-Held Devices in the Enterprise" http://download.intel.com/it/pdf/Maintaining-Info-Security-while-Allowing-Personal-Hand-Held-Devices-in-Enterprise.pdf

ACRONYMS

BI	business intelligence
DLP	data leak prevention
ERM	enterprise rights management
ERP	enterprise resource planning
GPS	global positioning system
PDP	policy decision point
PEP	policy enforcement point
TPM	trusted platform module
vLAN	virtual LAN

For more information on Intel IT best practices, visit www.intel.com/it.

Printed in USA
0111/IPKA/KC/PDF

Please Recycle
324166-001US