IT@Intel Brief

Intel Information Technology

Computer Manufacturing

Client Security

November 2006

Integrated Software Enhances Enterprise Security

Intel IT is deploying an integrated security software solution that cuts our response time to threats by 90 percent, while addressing enterprise needs for rapid software installation, scalability, reliability, and reporting.

The software integrates off-the-shelf components to create a scalable global enterprise solution that we initially plan to deploy across our environment of more than 100,000 desktop and laptop clients. We tied together security applications into a single package, saving installation time. We adapted the system architecture, shown in Figure 1, to introduce a hierarchical approach that improves scalability and reporting.

Profile: Integrated Security

- Cuts response time to threats by 90%.
- Plan to deploy on more than 100,000 client machines
- Packaged installation saves up to 15 minutes per client

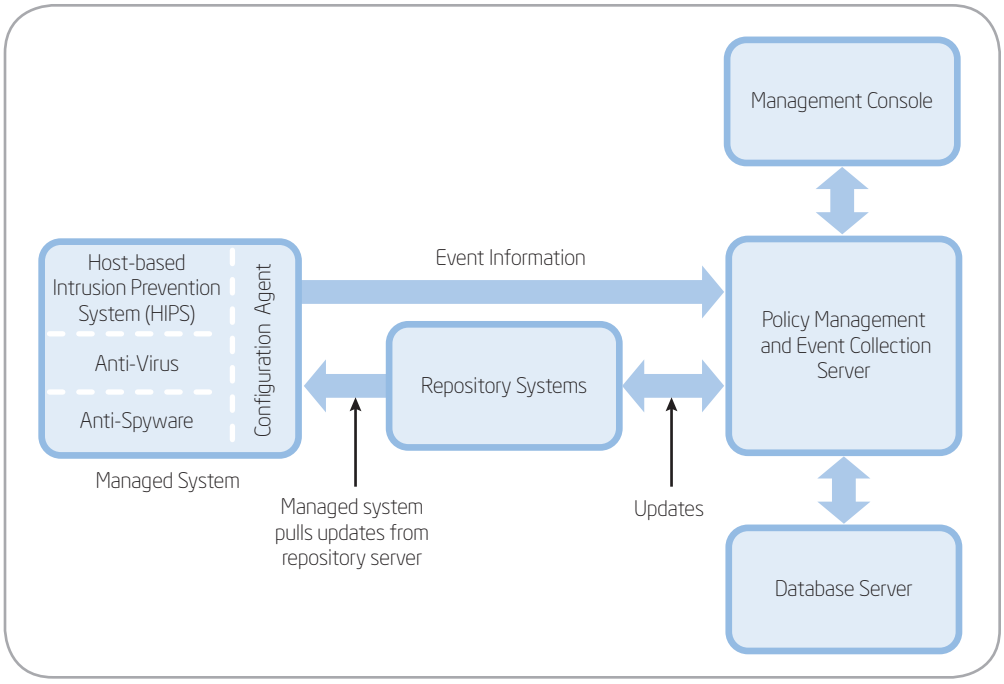

Figure 1. Integrated security software infrastructure.

IT@Intel

Background

Intel deploys a variety of security tools to protect the enterprise. We continually evaluate the need to add new technology to protect our workforce against rapidly evolving security threats. We recently selected a suite of tools to replace our existing security software and upgrade the security capabilities of client and server machines.

The suite includes four components that are installed on each managed system:

- **Host-based intrusion prevention system (HIPS).** Combines several technologies to block attacks, including firewall software, signatures to prevent known attacks, and heuristic technology to protect against previously unknown threats by identifying malicious behaviors. It also provides system call monitoring to detect buffer overflows, one of the most common methods of attack.
- **Anti-virus protection.** Defends against virus infections and Trojan horse software.
- **Anti-spyware software.** Protects against hidden tools that gather unauthorized information about users.
- **Configuration management agent.** Communicating with a central management console, relays events generated by the other components, delivers updates, and enforces security policies.

Deploying these tools enables us to take advantage of recent developments in security technology, including advanced alerting features that can quickly notify operations staff of potential threats.

However, we also needed to ensure that the technology solution could be deployed enterprise-wide. To do this, we adapted the security suite to improve software installation, updates, scalability, and reliability. Table 1 summarizes our initial requirements. We also plan to integrate the technology with our existing enterprise management console.

Software Installation

We created a wrapper around the four software components so that they are installed and updated as a single package, as shown in Figure 2 on the next page. This reduces overall installation time, because a user only reboots once, instead of multiple times after installing each component.

We estimate that this saves up to 15 minutes per client, depending on the system, which represents a considerable savings when deploying software on thousands of client machines. It is also easier to manage and helps ensure that each component is installed in the correct order and in a timely fashion. Because this approach minimizes disruption, it is also more convenient for users.

Scalability

We adapted the software architecture to improve scalability. Instead of using a single management server to support all managed systems, we introduced a hierarchical approach with a central database and several management zone servers within the enterprise, as shown in Figure 1. Each zone server collects events and other information from the managed systems within a specific zone. It also distributes policies and

Table 1. Adapting security technology for the enterprise.

Requirement	Solution	Result
Make installation of multiple security components faster and less disruptive	Add wrapper so components are installed as a single package	Savings of up to 15 minutes per client machine
Scale technology to support a massive enterprise environment	Create a hierarchical architecture dividing the enterprise into zones	Great reduction of WAN traffic; scales by adding zone servers
Access rapid and flexible enterprise reports	Consolidate selected information into a central database	Quick identification of threats and trends across the enterprise
Help ensure business continuity	Allow managed systems to get updates from any repository server	Continuous protection of systems if server outages occur

signatures to local repository servers, which then update the individual managed systems.

The zone servers exchange data by replication with the central management database, which acts as a central store for security updates and for selected information collected for enterprise-wide reporting.

This architecture has several important advantages:

- Reduced traffic on the enterprise WAN, because most event information is sent from managed systems through regional network links to the nearest zone server, rather than being transmitted across the enterprise to a central server
- Scalability by simply adding zone servers
- Improved availability because the enterprise is not dependent on a single server
- Flexibility to add servers wherever they are needed within the enterprise

Reporting

Our new architecture enhances the alerting features included in the off-the-shelf suite that enable quick identification and response to threats. We now have the flexibility to report events and trends within individual zones. We also consolidate selected data from the zones into the central database, providing us with an enterprise-wide view that accelerates our ability to spot and respond to potential problems. Overall, we estimate that the combination of standard features and our adaptations will cut our response time to threats by more than 90 percent. The software immediately alerts us to new threats and pinpoints their first occurrence.

Business Continuity

In normal operations, agents pull updates from the nearest available server, though they are

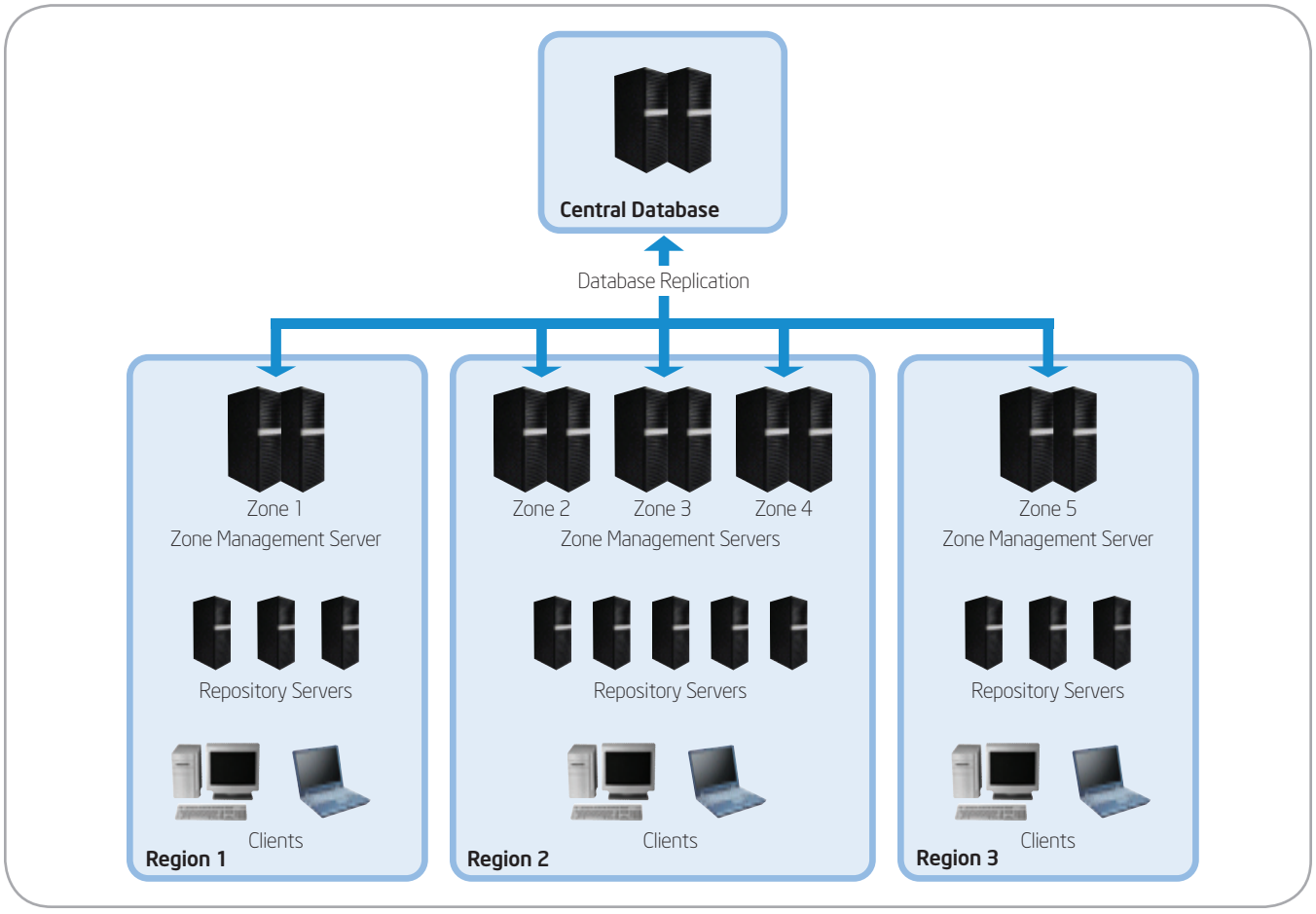

Figure 2. Integrated security software components.

capable of pulling updates from any repository in a defined list. This flexibility means that we can continue to provide clients with the latest security updates, such as signatures, if a server outage occurs—and even in the unlikely event of a more widespread system failure.

Integration

We also plan to integrate the package with our enterprise management console, which will provide our operations staff with a single view of security and other management events.

Proof of Concept Results

We conducted a successful proof of concept (PoC) to validate functionality and measure performance in a single zone with about 600 clients. We found:

- Client processor utilization increased 5 to 10 percent during brief scheduled periods when clients sent updated event and configuration information to zone servers. We consider this increase acceptable.
- Network traffic patterns clearly showed the benefit of localizing event traffic within zones, validating our architectural approach. Based on our results, we believe that if we had tried to run the entire Intel WAN as a single zone, we might have overloaded and would have needed to upgrade some lower-bandwidth WAN links.

Deployment

Based on our PoC, we are moving quickly to deploy the integrated software on desktop and laptop client systems across the enterprise. We believe that our zone architecture will help scale the system to support our large environment.

We are also looking to deploy our software on other systems, including servers running Microsoft Windows*, which are currently protected by various legacy tools. We expect that this will further enhance our ability to safeguard the enterprise.

Acronyms

HIPS	host-based intrusion prevention system
PoC	proof of concept

Printed in USA
1106/ARM/RDA/PDF

Please Recycle
Order Number: 314517-001US