Advanced Network Security with Intel-Based Security Appliance Solutions

What keeps IT managers up at night?

Whether they work at a small business or the largest enterprise, IT managers are under tremendous pressure to protect corporate assets. Malicious software, also known as malware, includes a class of threats that are described by terms like viruses, trojans, spyware, worms, and zombies. These threats can cause damage ranging from the slightly inconvenient to the utterly catastrophic.

In the past, corporate networks were protected from these threats at the perimeter by a firewall appliance, with additional software protection on all client PCs and servers. Today, the notion of a perimeter is outdated, thanks to the ubiquity of portable, connected devices that let workers log onto the network from public hotspots, hotel rooms, or home. This new network access paradigm is great for employee productivity and morale, but it comes at a significant cost to corporations—a much more vulnerable network. Now threats can come from anywhere outside or inside the network. A hacker could hijack an unsuspecting employee at an airport hotspot, or an employee working at corporate headquarters could unwittingly download malicious code from a website. On top of all this, IT managers have to face a dangerous new class of malicious attacks. Known by such names as blended threats and packet sniffing, these attacks specifically target the networks themselves.

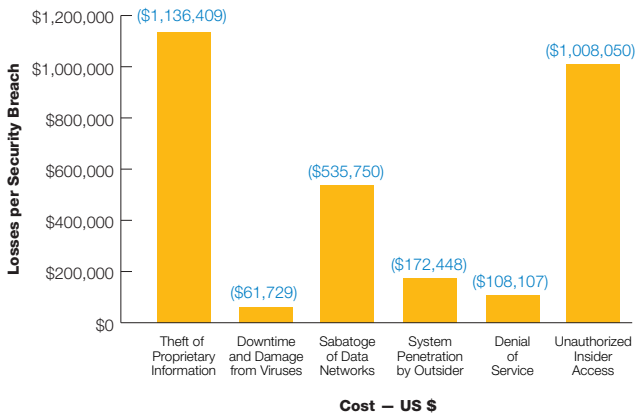
The problem is getting worse.

Security threats have increased tremendously in speed, complexity and volume in recent years. Threats propagate very quickly these days, in some cases circumnavigating the globe in ten minutes or less. Attacks come from outside the network, and increasingly, from inside.

Companies are spending a great deal of money on technology to protect their networks from attacks. Obviously, it could cost them much more if their networks are not adequately secured. An attack could prevent legitimate users from accessing the company by clogging the network with bogus requests or traffic. Additionally, corporate and personal information could be stolen or edited. An attack could even wipe out an entire corporate database. Preventing attacks by using the best performing, most cost-effective technology available is a top priority for IT organizations. See Figure 1.

More pressure on IT managers: it's the law.

On top of warding off and handling attacks, companies also have to contend with new regulations in many countries that focus on safeguarding financial information and sensitive personal data, including: the International Financial Reporting Standards (IFRS), the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), the UK Data Protection Act and more. In most cases, these requirements apply to all systems that access, or could be used to compromise, sensitive applications—including the corporate network. This puts even more pressure on IT managers to find the most effective protections for data as it travels along the network.



Source: CSI FBI Computer Crime & Security Survey 2004

Figure 1. **Average losses per security breach.**

Some of the threats facing corporate networks:

Spam

A general term that refers to unsolicited email sent to a mailing list. Spam is costly because it clogs networks with unwanted traffic and can take a considerable amount of time and resources to filter out. It can take 10 minutes per day per user and 43 minutes per IT administrator per day to deal with Spam (IDC Spam Study 2005). This really adds up over the long term.

Blended Threats

The newest mutations of computer viruses are known as blended threats. These combine the traditional malice of email-borne viruses with new network-based capabilities that quickly seek and find security vulnerabilities across the enterprise network, spawning further destruction such as denial of service attacks, crashed servers from executing worms, and root vulnerability from the launch of Trojan Horse .exe files.

Hackers/Attackers

Hackers use their computer expertise to find weaknesses in programs. While hackers challenge themselves to break into what is "unbreakable," attackers steal or destroy the information or resources of others. Attackers can be either inside or outside the network.

Insider Threats

E-business extranets allow access to internal company information by partners, contractors, temporary employees—and malicious insiders. Those inside the firewall have the ability to break into password files or human resources files without raising suspicion.

Packet Sniffing

Also known as a "man in the middle" attack, a packet sniffer is an application that sniffs, or spies on, the data packets moving within networks, without altering the data. The passwords, financial information or other critical data that they "sniff" can then be used for malicious purposes.

Spyware

Spyware refers to programs that secretly gather information about the user and send it to an interested party. They can infect a computer through a virus or upon the installation of a seemingly harmless application. Spyware programs can cripple a system's performance and lead to loss of corporate data or identity theft.

Viruses and Worms

Viruses are concealed strings of malicious code that replicate themselves, spreading through email attachments, shared files, downloads, or moveable storage media. Worms are viruses that attack several computers, through self-replication. A worm gestates in a networked environment and then spreads by spawning copies of itself onto other computers on the network. Worms eat up computer resources, such as memory and network bandwidth.

Zombies

A computer that has been infected with malicious code that places it under the control of a hacker without the user's knowledge. Zombies are often used as a participant in a distributed Denial of Service (DDoS) attack.

It takes a lot of processing power to secure a network.

Today's corporate networks operate at bandwidth speeds of up to 10 Gigabits per second—that's a lot of data moving quickly through the pipe. Every packet needs to be analyzed for security concerns.

In the past, security applications checked only the packet headers, not the data itself. The trend in enterprise security is moving towards deeper inspection of the data objects themselves for prohibited content and attacks. As hackers and virus writers become more sophisticated, security appliances go beyond inspecting individual packets and assemble them into the objects they represent (an .exe file for example) and analyzing the objects themselves for potential security risks. More thorough inspection requires additional processing power, and also benefits from larger cache sizes, in order to provide the security that businesses require without becoming a performance bottleneck.

IT managers need security solutions that work at wire speeds.

IT departments are expected to provide protection against threats while maintaining fast network performance and the pace of business itself. To augment client security software, companies are now relying upon powerful security appliances to protect the network from the inside out. Deployed in a layered approach for redundant protection, these specialized pieces of network hardware run dedicated security applications, which work in concert to closely scrutinize the contents of the packets without degrading network performance. Security appliances include:

Firewall—A firewall is a barrier deployed at a network's edge or internally that evaluates packets and the objects carried by those packets as they attempt to enter the network. A firewall checks data for unwanted content and keeps undesirable traffic from the trusted network. Firewalls protect networks against: Unauthorized Users. Denial of Service Attacks. Viruses. Worms. Trojan Horses. Spam.

Virtual Private Networks (VPNs)—A VPN creates a secure tunnel through the Internet, connecting outside users to a corporation's LAN. VPNs authorize users, encrypt data, and perform packet inspection of all the traffic at the edge of the network. VPNs protect networks against: Back Doors. Sniffing. Man in the Middle.

Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS)—Intrusion Detection Systems monitor traffic anomalies and alert administrators when a firewall has admitted undesirable traffic. Intrusion Prevention Systems are also used to trace and block attacks. IDS/IPS devices discover undesirable traffic that was not intercepted by firewall security.

SSL Acceleration Device—Used for e-commerce "lock and key" web transactions, SSL acceleration devices are often used to improve the performance of an encrypted channel between a user's web browser and the company's web servers. This creates a protected path for online transactions. SSL Acceleration Devices protect networks against: Unauthorized access to data.

Anti-Virus/Anti-Spam Appliances—These specialized appliances perform comprehensive analysis on data packets, a sequence of packets, and objects in email and attachments. Anti-Virus and Anti-Spam appliances protect networks against: Viruses. Spam.

The growing sophistication of attacks is driving the integration of multiple security features into single appliances with additional functionality such as intrusion detection. This requires enough processing power to ensure that security does not become a bottleneck to productivity.

Did you know that up to 70% of the security appliances used by businesses today run on an Intel® processor?

The market segment share leader in servers, desktops and notebook computers also happens to be the market segment share leader in solutions for security appliances.

The high-performance computing power that Intel delivers in servers and workstations is also available in leading infrastructure security appliances. Check under the hood—it's likely the Intel processors in your security appliances are based on the same processors powering your servers and desktop computers. See Figure 2.

As more security functionality is added to a solution, performance requirements increase.

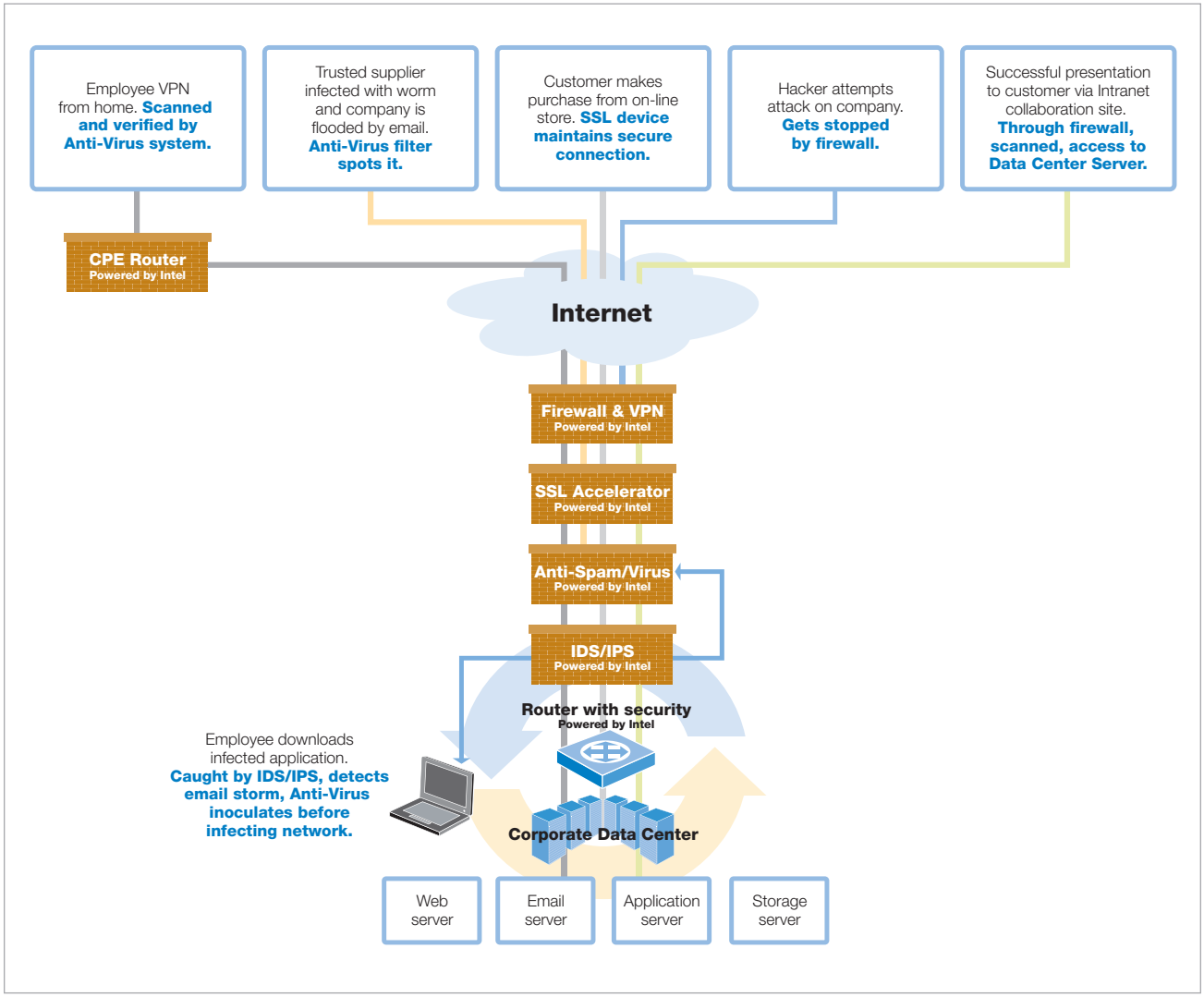


Figure 2. Intel-based security appliances maintain productivity for employees, customers, and suppliers while providing protection against malicious attacks.

Why does it matter whether an Intel processor is powering your security appliances?

"Not all security appliances are created equal. Vendors' architectural choices have profound implications for both the throughput that your appliance will handle and your ability to upgrade in response to new threats."

Paul Stamp, "Security Appliances Unwrapped," Forrester Research, Inc., March 14, 2005.

Intel creates processors that deliver uncompromised levels of performance.

Intel processors are well suited for security appliances, providing a highly tested and reliable foundation for your most critical security gateways.

Intel offers the broadest range of processors with robust feature sets, performance capabilities, and development support. These building blocks enable OEMs to deliver more powerful and reliable security appliances to the marketplace. For Small Office Home Office (SOHO) implementations, Intel network processors provide performance, low power, and small footprint solutions. For mid-market applications, the Intel® Celeron® M, Intel® Pentium® M, Intel® Celeron® and Intel® Pentium® 4 processors deliver high performance. Enterprise-class protection requiring the highest levels of processing performance is delivered by Intel Pentium 4 processors and Intel® Xeon™ processors. See Figure 3.

Intel works closely with developers and vendors to optimize their security solutions.

As security threats adapt and become ever more sophisticated, firms need their optimized security software working in concert with high-performance platforms to provide the highest levels of protection against threats.

For years, Intel has collaborated very closely with the market-leading security vendors to ensure that their solutions leverage the full computing power of Intel® architecture (IA). Intel has developed an extensive set of software tools and resources that are designed to help tune any solution to get the maximum performance from Intel architecture. Intel offers software development tools (compilers, analyzers, development kits) and dedicated support engineers.

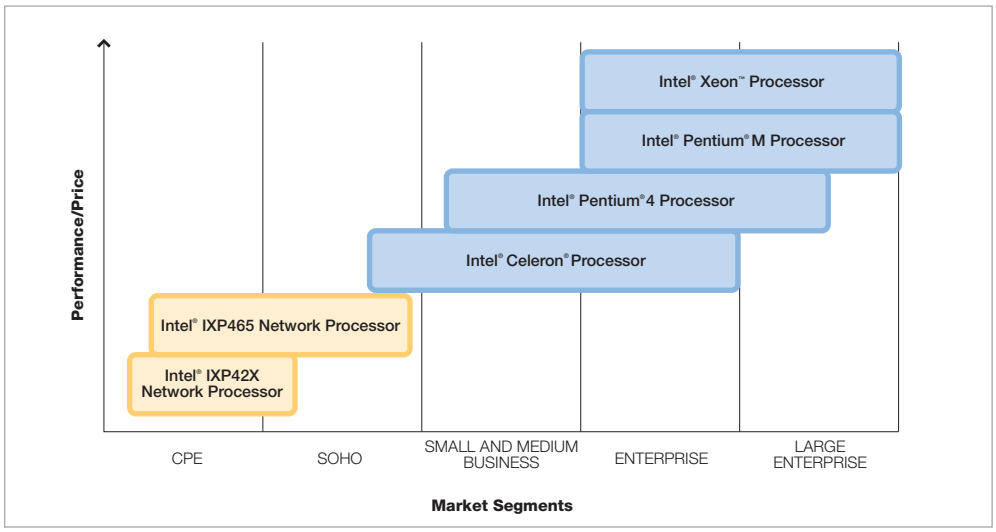


Figure 3. Intel processors power a broad range of security appliances used in small, mid-market and large enterprise businesses.

Intel collaborates with a broad ecosystem of vendors to maximize the performance of their product offerings.

Intel works with other companies that share a common commitment to developing modular, standards-based building blocks, platforms, and solutions based on technologies, processors, products, and services from Intel. Working together allows leading security OEMS and ISVs to innovate more rapidly through multiple levels of integration—silicon, software, boards, and complete systems, resulting in greater choices for IT managers.

Intel's global manufacturing and support capacity is unparalleled.

Intel has the manufacturing capacity and commitment to the embedded marketplace to supply its processors and other embedded components for seven or more years, several years beyond the industry standard of five years. This allows vendors to provide a more stable set of products to their customers. What's more, Intel has the manufacturing capacity to develop customized product lines to meet different customer requirements.

Intel invests substantially in Research and Development.

Intel invests over $4 billion annually so that it can remain on the leading edge of performance breakthroughs. True to our heritage of performance, Intel is introducing important new technologies into our product lines, such as cache improvements and multi-core processors, which will bring new levels of computing capabilities to security.

Intel has unmatched depth of experience and industry leadership.

Intel has been actively involved in developing networking standards since the invention of Ethernet more than 30 years ago. Intel participates in standards and specifications bodies at the heart of the security industry, including IEEE, PCI-SIG (PCI Express), and the 10 Gigabit Ethernet Alliance, helping to create consistency and longevity in the rapidly changing computer industry.

Intel technologies in today's security appliances

Intel® Architecture

Intel has the most extensive product roadmap to support performance requirements.

A key reason so many vendors have selected Intel processors for their security appliances is that Intel has a more extensive roadmap than any other company. And while Intel is constantly migrating its products to higher performance envelopes, it maintains support for existing products. The unique combination of stability and performance in a deep roadmap offers OEMs a solid foundation upon which to base their products. IT managers can rely on a stable set of offerings as well as predictable performance improvement for enhanced choice, flexibility and a pay-as-you-grow capability.

Many IT managers may not be aware of the extensive support services that Intel provides to OEMs. Intel offers our OEM customers reference designs and engineering support, software tools and services, and a third-party ecosystem of suppliers that can provide them with additional support from BIOS to assembly. Using an Intel-based solution ensures that the OEM has the tools and support they need to deliver appliances you will rely on to protect your business.

With over ten years experience creating Intel architecture processors including the Intel Xeon processor, Intel® Pentium® processor, and the Intel Celeron processor, Intel has devoted tremendous amounts of resources to extending the product roadmap well into the future. Intel is well able to keep up with increased network performance needs.

Intel® Network Processors

As a leading innovator in network processing, Intel has created a packet-processing technology known as the Intel® Internet Exchange Architecture (Intel® IXA). These

processors specialize in analyzing and routing network packets efficiently at wire speed. The Intel® IXP 2800 network processor family is a good example of Intel research and development innovation at work. Intel has provided integrated security capabilities for cryptography on a single chip. This critical functionality can spread security intelligence around the network, helping to bolster protection and alleviate network congestion. Intel IXA technology includes many network processor families, each one optimized to meet the specialized packet-handling requirements of network applications.

Intel IXA network processors are highly integrated and flexible. They include programmable microengine blocks, so that, using an interface, developers can program and alter various security functions such as cryptography and signature matching as needs change. Traditional, fixed-function ASIC (application-specific integrated circuit) technology cannot be redesigned easily to respond to changing system requirements. The flexibility and efficiency of Intel IXA network processors offer OEMs customized processors for optimal combinations of performance, power usage, and cost.

PCI Express* I/O Technology

Many security appliances are taking advantage of PCI Express* I/O technology, which enhances security appliance performance with fast industry-standard serial link technology. PCI Express reduces the latency or idle time between the processor and other systems, improving the overall security appliance performance.

Intel spearheaded the new PCI Express specification.

Unlike PCI, its parallel predecessor, PCI Express is a serial point-to-point interconnect capable of extremely high-bandwidth transfers. Performance ranges from 250 Megabytes per second (MBps) for a single “lane” implementation and up to 4 Gigabytes per second (GBps) for the 16 “lane” implementation. It is designed to feed the advanced I/O processing capability of today’s CPUs.

90 Nanometer Manufacturing Process

The smallest, highest performing transistors in production today are at the heart of high-performance security appliances. The 90 nanometer manufacturing process used by Intel is the most advanced semiconductor manufacturing process in the industry.

Moore’s Law, the prophetic prediction that the number of transistors in a given space will double every two years, has held true as a result of the pace of Intel innovation. The 90 nanometer process is the latest generation process technology that changes not only the size but also the way that microprocessors are produced. It makes it possible for electrons to flow through the microprocessor with less resistance, so that security appliances consume less power, run cooler, and can offer better performance than previous generations.

New and Emerging Intel Technologies

"I know that companies like Intel are working to integrate hardware acceleration techniques with their processor product line to deliver the necessary power for application-layer computing."

Mark Stevens, Chief Strategy Officer,
WatchGuard Technologies, Inc.

It is difficult for traditional signature-based technologies used in anti-virus and intrusion prevention software to keep up the pace of enforcing protocol standards, matching signatures, and other security tasks. It's becoming increasingly necessary to rely on hardware to handle the security inspection and processing of data.

Intel research and development teams continue to push the performance envelope by developing new technologies to increase overall computing power. Intel is developing larger caches into its processors as well as new technologies like Intel® Extended Memory 64 Technology (Intel® EM64T), Intel® Virtualization Technology (VT), and multi-core architectures to enhance the power and efficiency of security appliances.

Cache Size

Security appliances, like any PC or server, utilizes ultra-fast on-chip memory, known as cache, that brings a copy of data closer to the processing core. This memory, or cache, will hold pieces of data or an application locally while the processor executes instructions and performs tasks and reduces the frequency that an application has to wait for data to transfer from comparatively slow external memory. The cache needs to be able to match the speed of the processor to maintain optimal performance. Intel designs its processors and cache to work in concert to perform the necessary data processing quickly. Cache not only comes in sizes (i.e. 512 KB, 1 MB, 2 MB etc.) but also in "levels" (i.e. L1 is faster and closer to the processing core than L2). Larger and faster caches help reduce the reliance on external memory and allows Intel-based security appliances to better perform useful degrees of data security at wire speed.

Intel® Extended Memory 64 Technology (Intel® EM64T)

Some security appliances, such as Intrusion Detection devices (IDS/IPS), need a great deal of memory in order to run effectively, because many instructions need to be executed and an enormous amount of data needs to be stored and analyzed.

Intel EM64T is an extended memory technology that provides faster storage access and processing. This enhancement to Intel's IA-32 architecture gives security appliances that are based on Intel processors a larger pool of memory available for applications to run. Intel EM64T provides users with the ability to extend past the 32-bit limit of 4GB for large storage cache without paging latency, so that they can execute larger quantities of more complex software instructions as well as enabling faster operations on 64-bit data. With Intel EM64T, security appliances are able to provide more comprehensive protection without sacrificing network performance.

Intel® Virtualization Technology (Intel® VT)

Intel Virtualization Technology is part of a collection of premier Intel-designed and manufactured silicon technologies that deliver new and improved computing benefits. This enhancement will allow a platform to run multiple applications in independent partitions, so that one computer system can function as multiple "virtual" systems. This makes it possible for a security appliance to separate and handle more complex security operations that are independent of general security processing. This approach lets single appliances provide fast network performance, while simultaneously providing robust network protection.

Multi-Core Architecture

Intel is on a fast track to deliver multi-core processors in high volume across all platform families, including those for communications. Intel dual-core processors are the first step in this transition. A dual-core processor includes two complete execution cores per physical processor for simultaneous computing. This will provide security appliances with more processing power for deeper packet inspection and improved throughput. Security appliances using Intel dual-core processors will be better equipped to handle complex, simultaneous transactions and escalating workloads.

Security appliances in the future.

As the sophistication of attacks grows, so too must defenses enabled by security appliances. The deep packet inspection capabilities and object inspection of security appliances will continue to become more thorough. Appliances will update the signature files of threats more frequently thereby providing stronger protection levels. Security appliances may heuristically learn the characteristics of malicious attacks and protect against them in near real-time. Another trend, particularly at the mid-range of required performance, is to consolidate functionality into fewer appliances. In a few years, many functions that are handled today by separate appliances will likely be combined. See Figure 4.

The evolution of threats will push the pace of innovation and performance in security appliances. New and improved security appliances will require more powerful processors, faster memory technologies, and utilize countless new technology innovations to protect corporate and personal data. Intel is committed to supplying the best technology and products that power the devices that protect your business.

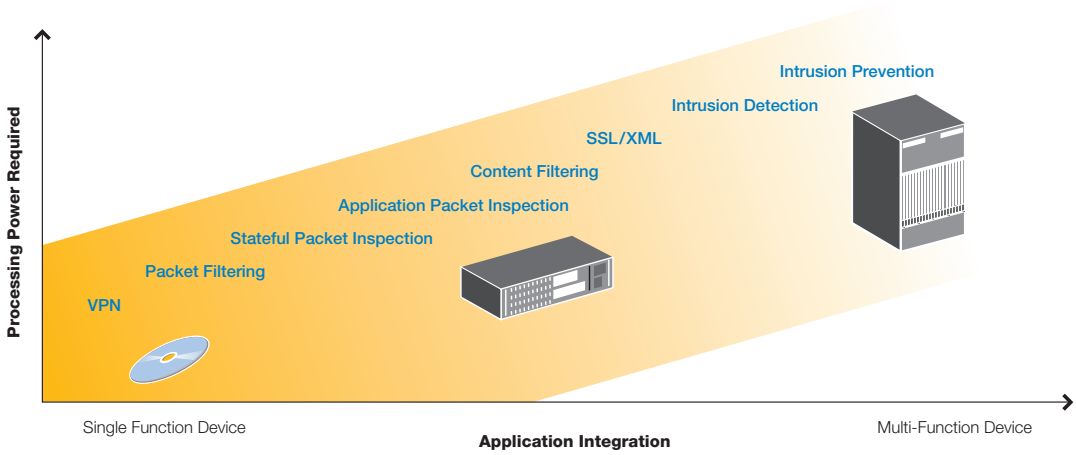


Figure 4. Relationship between processing power and application integration.

Intel is devoted to protecting the enterprise and its data. We're in the business of providing the most effective building blocks for safeguarding data security and privacy.

Make sure your business is using Intel-based security appliances.

Find out more:
intel.com/netcomms/technologies/security

 Printed in USA/0905/LKY/PMS/PDF Order Number: 309614-001US