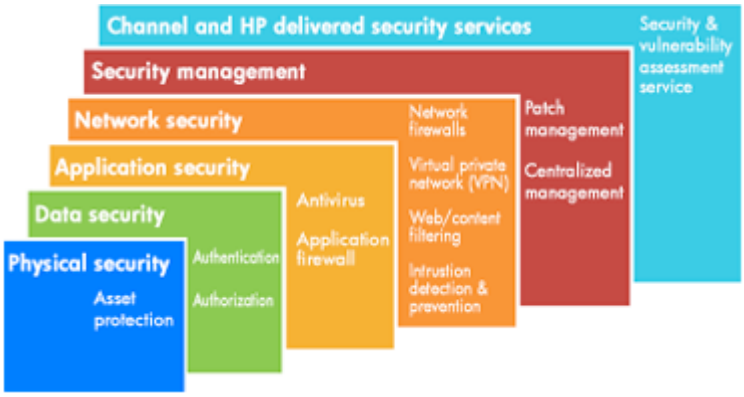
Security solutions - Protection at every layer

With HP's holistic approach to security, you can be more confident that you have secured all points of attack.

As threats become more sophisticated and more diverse, you should consider developing a comprehensive security strategy rather than implementing an uncoordinated collection of precautions to protect multiple points of vulnerability. You need to protect your hardware, data, applications, operating systems and networks. You may also need broader security management solutions and services to find and fix vulnerabilities and to keep your security defenses up to date.

Layers of security

HP has developed the layers of security approach to provide the tools you need to begin thinking of security as a business strategy. Each layer focuses on a different area of security in your business.



- **Physical Security:** Keep your computers locked down and safe from physical theft.
- **Data Security:** Restrict access to data on personal systems to only those who should have it.
- **Application and Operating System Security:** Utilize applications like antivirus software and software firewalls to block incoming attacks.
- **Network Security:** Protect your network from intruders and viruses with network firewalls, Virtual Private Networks (VPNs), intrusion detection and prevention systems, and web and content filtering.
- **Security Management:** Consolidate your approach to security management, assess your overall vulnerability, and manage patches and updates carefully.
- **Security Services:** Work with HP and our expert channel partners to get confidential and expert advice to help you protect your business from security threats.

And with HP's modular security solutions, you don't have to do it all at once. You can begin today by focusing on the layers of security and specific solutions that address your most immediate issues. Later, you can add additional solutions at any layer to enhance your overall security strategy.

While no single product can make your business completely immune to security threats, HP's layers of security can bring you closer to your goal of uncompromised security throughout your company. That makes HP security solutions altogether better for your business.

Security solutions - physical security

Hardware theft inside of an office's four walls is a surprisingly common occurrence. Unauthorized visitors can simply walk away with notebooks and thin clients if the timing is right. HP can help you secure your most vulnerable hardware.

» Notebook solutions
» Thin client solutions
» Desktop and workstation solutions

Notebook solutions

HP offers support for Kensington Slimline Security Locks on our entire line of business notebook PCs to keep your notebook and its peripherals from walking away. These locks are industry standard so you can purchase a new lock with your notebook, utilize locks you may already have, and quickly and easily find replacement locks when you need them.

Remember that you need to protect not only your notebook, but also its peripherals, like a multibay optical drive, a port replicator, or a dock. Select HP business notebook PCs make this as easy as a lock and click with built-in features that you get right out of the box.

Thin client solutions

HP offers a two-pronged approach to reducing the theft of thin clients:

- Use **Kensington Security Cables** to physically secure a thin client to a desk or table. **Mounting brackets** also allow you to attach a thin client directly to a desk or table.

- Integrate thin clients with HP servers in your secure data center so the expensive computer components and key data are safe in one location. The thin client becomes less expensive to replace because the expensive components and irreplaceable data are on the server. Stolen thin clients become useless to thieves because the clients cannot run without their integrated servers.

Beginning in December, 2004, HP Compaq t5700 Thin Clients. will be pre-loaded with Sygate Security Agent 4.0 for Microsoft Windows® XP Embedded. This solution provides an application-centric firewall, application-based intrusion prevention engine, and enhanced virus protection in server-based computing environments. Learn more about this computing model and its security benefits in the Is server-based computing right for you? white paper.

Desktop and workstation solutions

Desktops and workstations are a substantial investment and you want to protect them. HP makes it easy with a collection of optional security solutions to help protect your investment:

- A **solenoid hood lock** that eliminates the need for a physical key by making the chassis lockable through a password. You can also lock and unlock the chassis remotely over the network. The lock attaches to your system and acts as a cover lock. This locking solution is only available from HP on select desktops and workstations.
- Support for **Kensington locks**. Use industry-standard locks to tether systems to a desk so they won't find their way out of your offices and into the hands of thieves.
- A **PC chassis lock** to physically lock a chassis cover as well as the keyboard and mouse cables with a key.
- A **rear port controller** that clips into the back of a computer to secure input devices and prevent the removal or addition of cables on the back.
- An integrated work center that not only saves space by integrating the monitor and the PC, but also works with a standard Kensington lock to secure both the monitor and PC at once.
- A **wall-mounting bracket** that you can use to mount a system to a wall or under a desk to reduce risk of theft and keep the system out of site.

Security solutions - data security

Personal systems are your employees' gateway to your company data, but if not properly secured, they also give hackers and thieves access to that same crucial data. The data on your company systems, from desktops and workstations to notebooks and iPAQs as well as printers, needs to be protected in a way that doesn't hinder work, but still provides sufficient security.

» Support for Trusted Computing Group standards
» Simple but strong built-in authentication
» Authentication beyond basic passwords
» Protection for mobile devices and data
» Control access to your wired and wireless networks
» Secure printing

Support for Trusted Computing Group standards

HP is a founding member of The Trusted Computing Group (TCG), an industry-standards body that develops and promotes open industry standard specifications for trusted computing hardware building blocks and software interfaces across multiple platforms, including PCs, servers, PDAs, and digital phones.

HP builds a Trusted Platform Module (TPM) into new select HP computers that integrates the core elements industry-standard security into a computer's subsystem. TPM enhances the native Microsoft™ operating system security features for file and folder encryption and protection of secrets such as certificates and passwords. The TPM Embedded Security chip is available on select desktops, workstations and notebooks. The Embedded Security Manager for ProtectTools is a module that is supported by the HP ProtectTools security manager, which is a free download, gives you all of the tools you need to centralize management of your security solutions. Learn more about HP ProtectTools in the Management section of this site.

Simple but strong built-in authentication

Several products in HP's line of business computers and handhelds come complete with a combination of features designed to simplify and strengthen security:

- A **power-on password** that requires a user to type a password before the BIOS boots and the operating system loads.
- **Drive locks** for notebook hard drives and multibay drives that put a BIOS-level password on a computer's hard drive. Even if someone does manage to bypass the standard Windows login, they will need to know yet another password to access the hard drive.
- An **administrator password** that allows a computer to boot, but restricts access to the BIOS so settings like drive lock can't be changed.
- A **biometric fingerprint reader** offered as a standard feature on select iPAQs and as an add-on for desktops, workstations, and notebooks; with this device, a fingerprint becomes a user's password.
- Full support for **802.11 security standards**.

To make individual systems and the networks they access immediately more secure, you can start using these features every time you power on your computer.

Authentication beyond basic passwords

You have several options for adding additional authentication security to your company computers*:

- A **biometric fingerprint reader** that you can purchase as an accessory for a computer so a fingerprint becomes a user's password.
- Smart Card security that protects a computer in several different ways:
    - A patented **pre-boot Smart Card** prevents the computer's operating system from loading if the proper Smart Card isn't inserted in the integrated or PC-card

Smart Card reader.

- **Secure lock** that helps prevent unauthorized access to your unattended computer by locking it if the Smart Card is removed.

- A **USB keyboard or card reader** that use Smart Card technology to prevent unauthorized access to a system and the network.

When you purchase select new HP business computers you can add an integrated Smart Card reader and a Smart Card to the system (see individual product specifications for more details). For computers without the integrated Smart Card option, or for those you already own, you can purchase a PC Smart Card reader to easily add Smart Card security functionality.

* Not all features available on all models. See product specifications for details.

Protection for mobile devices and data

HP has developed HP ProtectTools, a family of security products, to give you safer ways to stay in control and secure your data while you're on the go so you can reduce the technical and financial risks to your business.

HP ProtectTools for notebook PCs

The foundation for HP ProtectTools for notebook PCs begins with the HP ProtectTools Security Manager, an extensible console you can download free from the HP site for older HP notebooks and that will be factory-installed on next generation HP notebooks. The ProtectTools Security Manager gives you a single point of control over all elements of security for your notebook.

HP has developed four modules to work with HP ProtectTools Security Manager to allow you to customize your security.

- **BIOS configuration for HP ProtectTools** gives you control over your computer's BIOS settings and can prevent anyone who doesn't know your BIOS password from even booting your system. This feature is only available on notebook PCs.

- **Credential Manager for HP ProtectTools** supports multifactor Windows Authentication and single sign-on so you can have strong authentication that is simple to use.

- **Smart Card security for HP ProtectTools** allows you to easily add Smart Card security to your notebook by managing the card initialization, security settings, and integration with the BIOS.

- **Embedded Security for HP ProtectTools** allows you to configure and manage your notebook's built-in Trusted Computing Module security chip.

Select HP notebooks come with the BIOS configuration and Credential Manager modules already installed, and you may download others free from HP if your notebook hardware supports them. Review your product information or work with your local HP product expert for more details on which HP ProtectTools modules your notebook supports.

HP ProtectTools for iPAQ handheld PCs

HP's ProtectTool solutions for iPAQs are powered by Credant, a best-in-class security partner, and give you solid device-level security right out of the box on iPAQ hx2000 and hx4700 models with the ability to add additional Credant Management solutions later. With the pre-loaded HP ProtectTools, you can password protect your iPAQ and encrypt its data, so even if it is lost or

stolen, the information on it is secure. When you add Credant Mobile Guardian solutions to your IT toolkit, you can tighten security policies as well as disable communication ports and file sharing functions for any iPAQ that has an active wireless LAN or WAN connection.

Control access to your wired and wireless networks

The ProCurve Networking by HP Access Control Security Solution helps you ensure that only authorized users are allowed access to your wired and wireless networks. The solution protects the LAN by restricting key network resources and services access to authenticated users. This built-in, standards-based approach to security helps shield your valuable network resources and intellectual property from internal and external security threats.

This HP solution efficiently delegates access, authentication, and tracking capabilities to switches and software that sit at the very edge of network LANs. Pushing access control to the LAN edge enables decisions to be made immediately at the boundaries of your network, rather than deferring them to the core. This smarter, safer security solution also helps prevent potentially malicious traffic from gaining access to your LAN.

Secure printing

HP and its industry-leading partners provide a variety of integrated printer-based security solutions-from physical safeguards to document tracking or sophisticated encryption/decryption capabilities-that meet your most stringent demands for information protection and confidentiality. HP's secure document delivery solutions increase the capabilities of HP LaserJet printers, MFPs, and Digital Senders beyond the range of their standard features. HP and its third-party partner offerings give you the power to:

- Securely erase confidential print, scan, fax, and copy jobs from HP LaserJet 9000, HP LaserJet 9000L, HP LaserJet 4100mfp, and other similar devices with HP Secure Disk Erase so you know your sensitive data cannot be accessed or stolen by unauthorized users.
- Protect your company's intellectual property with secure PageRecall and NetRecall, document sharing solutions that allow control and sharing of confidential information at all times, even after recipients receive it.
- Alert users when an important or proprietary document has been printed with an Alarm DIMM in the printer.
- Maintain accountability for printing sensitive documents-paychecks, invoices, insurance forms, patient records-at the printer when they are produced with an Audit DIMM.
- Restrict access to printed documents with FollowMe Printing that issues digital rights to printer access with portable cards, biometric identification, or numeric passcodes.
- Securely print to parties outside your organization through various delivery and notification options using SD Express Printing.
- Use a SecureDIMM to protect information as it travels from the host to the printer with encryption and decryption technology.
- Authorize and track encrypted or non-encrypted printing, copying, scanning, or digital sending jobs by requiring users to access printers and multifunction products with a

personal identification number or smart card with SecureJet 4.0.

- Manage the delivery of point-to-point fax transmissions or encrypt documents for delivery via email with Genifax and Genidocs software.
- Accommodate NT, Novell, LDAP, or Kerberos authentication and works by prompting the user for a username and password prior to allowing the user to access any of the digital sending functionality with HP Digital Sending Software (DSS) 4.0.
- Autofill the "from" portion of an email sent by an authenticated user on an MFP and then encrypt that email for total security with HP Digital Sending Software (DSS) 4.0.

Security solutions - application security

Hardware and software work hand in hand to protect your business from security threats. When you restrict access and strongly authenticate users, you've made a good first start, but the interconnected nature of today's computing world means you must also look beyond hardware to software solutions.

Start using Norton AntiVirus right out of the box

To help you protect personal systems, select HP business notebooks and desktops come installed with a Norton AntiVirus pre-installed with a free 60-day subscription to Live Update. Norton Live update ensures that you have the latest virus Norton AntiVirus, a leading and trusted antivirus application that thousands of businesses count on every day to keep their computers virus-free.

Because the software is pre-installed, all you have to do is start using it. When your trial period is over, you connect quickly and easily with Norton to continue the antivirus protection you already have in place. It's that simple.

Automatically update antivirus programs

Spam and spyware attacks are accelerating and it's difficult to keep up with patches manually. You can better manage your antivirus updates with an easy-to use, single solution:

- Deploy the Trend Micro Client/Server/Messaging Suite for Small and Medium Business on HP ProLiant servers running Microsoft® Small Business Server and have confidence that all of your company's computers and servers have the latest updates for their antivirus software.
- Perform status checks on your virus protection level via a web browser, even from a remote location.

A 90-day full version of Trend Micro Client/Server/Messaging Suite for Small and Medium Business comes pre-installed on all ProLiant ML100 series servers configured with the Microsoft Small Business Server 2003 solution. This version of the suite does not include CSM media, but once you purchase

the software you will have access to all media.

Protect key business applications

The HP ProLiant DL320 Firewall/VPN/Cache Server includes an advanced application layer firewall designed to help defend a network from attacks. It integrates ISA Server 2004, Microsoft's next-generation application layer firewall/VPN/web cache solution, with a hardened version of Windows Server 2003. The HP ProLiant DL320 Firewall/VPN/Cache Server is tightly integrated with Exchange 2003 and Outlook applications, and offers significantly increased security for these applications.

The solution's application-level firewall examines the contents of incoming information to verify that they are destined for a valid purpose. This approach drills deeper than network-level firewalls, which examine only the validity of the surface information coming in and not the true contents within an email, for example.

The HP ProLiant DL320 Firewall/VPN/Cache Server is an ideal solution for businesses that want to protect key business applications, such as Microsoft Exchange Server, Outlook Web Access, Internet Information Services, and SharePoint Portal Server. For simpler, smarter security, this wide-reaching security solution is pre-installed on a set HP ProLiant DL320 server configuration.

HP-UX Bastille: Enhanced security for HP-UX

HP-UX Bastille is a free security hardening/lockdown tool that provides customized lockdown on a system by system basis, addressing a large number of the recommendations from a number of popular security scanning tools and checklists. Bastille was originally developed by the open source community for use on Linux systems, and HP is contributing to the effort by providing HP-UX Bastille.

You can configure Bastille with the help of an interactive interface or using a configuration engine. With Bastille you can:

- Configure daemons and system settings to be more secure
- Turn off unneeded services
- Partially limit the vulnerability of common Internet services such as Web servers and DNS
- Configure Security Patch Check to run automatically
- Configure an IPFilter-based firewall

Bastille is available as a free software download and works well in combination with HP's free Security Patch Check, a tool that analyzes the currency of your system to be sure it is up to date with all security bulletins.

Security solutions - network security

You only have to pick up a paper or hear the daily business news to know that viruses and hackers are a real threat to business networks of all sizes. The question is no longer "Is there a threat to my business?" but instead, "What should I do about it?"

» Deploy a combination firewall and VPN solution
» Proactively update antivirus & antispam protection for your network
» Slow down new and unknown worms
» Store user data at your data center

Deploy a combination firewall and VPN solution

Firewalls and VPNs are two key tools you can use to protect your network and combat the ever-growing range of viruses and would-be hackers who want nothing more than to rampage about your network. The HP ProLiant DL320 Firewall/VPN/Cache Server is an affordable, integrated, easy-to-use, and manageable hardware security and caching solution that you can quickly deploy to help protect key business applications, such as Microsoft Exchange Server, Outlook Web Access, Internet Information Services, and SharePoint® Portal Server.

HP is the first major vendor to offer a product that uses Microsoft's latest Internet Security and Acceleration Server 2004. This server software integrates neatly with Windows® Active Directory® services so you can easily apply group- and user-level policy and authentication across a broad range of scenarios, including firewall policy, VPN authentication, and outbound Web proxy and access control.

To make it easier for your ProLiant servers to handle Secure Socket Layer (SSL) connections on secure Web application servers, HP offers the AXL600L SSL and AXL300 accelerator cards. When you add these cards to your ProLiant servers, you can vastly improve the number of SSL connections your servers can handle by offloading the SSL encryption and decryption onto a dedicated card.

Proactively update antivirus & antispam protection for your network

Trend Micro Client/Server/Messaging Suite for Small and Medium Business provides proactively updated antivirus and anti-spam protection for network environments. HP offers a 90-day, fully functional, trial version of this antivirus/anti-spam/content security solution as a pre-installed security element on HP ProLiant servers that come with an installed version of the Microsoft Small Business Server 2003 solution.

Trend Micro Client/Server/Messaging Suite scans and eliminates recognized viruses within a company's network and blocks identified spam at the email server before it reaches individual PCs. It reduces the risk of malicious attacks by filtering out unwanted email messages and unsafe attachments.

Protect against hackers

In a dynamic Internet environment where new attacks occur daily, HP Firewall/VPN Server - Check Point Edition provides advanced capabilities to help small to midsize businesses defend their networks. This solution includes a pre-installed version of Check Point's SmartDefense technology to actively defend an organization from known and unknown network and application attacks.

The HP Firewall/VPN Server incorporates advanced virtual private network (VPN) technology. This technology allows authorized users to log onto a network over the internet and carry out secure communications. Your employees and clients can be comforted in knowing they have a solid solution that will help shield their words from online spies.

HP backs this solution with a year of free phone support from some of the most experienced security engineers in the business. For safer network security, this solution classifies attacks and rapidly detects, prevents, and responds to potential network intrusions by examining each data packet that tries to enter a network.

Slow down new and unknown worms

Antivirus software is designed to look for virus signatures and trap infiltrators before they can spread through your network. However, when a new worm virus is first released and its signature is unknown,

that virus can potentially run rampant on your company's network. The virus attacks at machine speed and there's simply no way for humans to keep up.

HP Labs has developed Virus Throttle technology designed specifically to slow the spread of new, unknown worms so their damage to your network is as minimal as possible. Virus Throttle technology targets virus behavior instead of the virus signature.

Viruses tend to try to connect to many machines quickly, as opposed to uninfected machines that typically make fewer connections more slowly to fewer machines. When the technology detects rapid connections to many machines, it automatically limits the number of connections the potentially infected system can make and notifies an administrator of the potential problem. The Virus Throttle technology hampers, contains, and mitigates attacks to buy you time to respond.

HP's new Virus Throttle technology is currently available in select HP networking and server products:

- ProCurve Networking Switch 5300xl comes with Virus Throttle technology built in and when used as a router can completely stop routed network traffic from infected network systems from propagating to the rest of the network. Because the ProCurve Switch 5300xl can monitor all ports on the switch for worm virus activity, virus throttling on the ProCurve Switch 5300xl provides a centralized ability at worm control.

- The ProLiant Intelligent Networking Pack with Virus Throttle technology protects the local network environment in case one of your individual ProLiant servers becomes infected with a worm virus. This can help slow the spread of a virus from an infected server to other servers on your network.

Store user data at your data center

A key strategy you can employ to help guard your network from viruses is to store the majority of the data generated by users in your data center instead of on individual computers. User data remains in the data center with the rest of your key company data; because viruses spread with file transfer, they have a harder time propagating when users don't send files to one another via email. Additionally, it is easier for IT staff to manage virus protection at a single data center rather than at every client computer in your office.

HP thin clients can be key components in this strategy because they don't have hard drives, so you are guaranteed that all data resides in the data center. Learn more about this approach to data security in this Thin Client Vulnerability Analysis PDF.

And, because viruses and intruders can also find their way into your network via the unattended thin clients at your data center, HP thin clients allow you to lock down peripheral ports so they won't communicate with outside peripherals, such as USB drives, that can harbor viruses or be a back door opening for data theft.

Security solutions - security management

Keeping pace with the constant influx of new information on IT security threats and require software updates can seem impossible. Manual and semi-automated processes just won't do the job, but there is a better solution.

HP ProLiant Essentials Vulnerability and Patch Management Pack

The HP ProLiant Essentials Vulnerability and Patch Management Pack is an all-in-one tool that is built

into HP Systems Insight Manager.

Vulnerability and Patch Management Pack actively monitors ProLiant servers (and other x-86 servers) and helps protect them from security gaps. This HP offering assesses and identifies known threats and the patches that repair these vulnerabilities. This solution automatically gathers vulnerability data, enables scheduled scans to identify problem areas, automates patch downloads, correlates patches with the problem areas, deploys patches and fixes, and provides assurance that patches remain installed on an ongoing basis.

Working together, HP Systems Insight Manager and HP ProLiant Essentials Vulnerability and Patch Management Pack provide a single-pane status view, which includes information on hardware faults, system performance, system software, and vulnerability status. This integrated approach helps administrators identify and resolve system issues and vulnerabilities quickly, efficiently, and reliably.

HP ProtectTools Security Manager

The HP ProtectTools Security Manager provides a single console that serves as the foundation for existing and future HP ProtectTools client security solutions on select HP desktop and notebook business PCs. The HP ProtectTools Security Manager is a software application that adds an easy-to-use interface into the Microsoft® Windows® control panel so you can easily access the full breadth of HP security capabilities designed to help protect against unauthorized access to PCs, networks, and business-critical data.

HP's latest featured addition to the HP ProtectTools Security Manager suite is Credential Manager. Credential Manager for ProtectTools increases network security by providing a secured password solution so that users do not have to remember more complex passwords. The users credentials are automatically retrieved for them when necessary, and multiple users can set up their own credentials for quick and safe access to shared PC resources. Credential Manager password can be strongly protected via the TPM Embedded Security chip. Credential Manager is available on business PCs, Workstations and Notebooks configured with TPM and select notebooks.

Once Credential Manager is installed, users can login into their identity and gain access the network. Credential Manager also provides fast single sign on to all your business applications, regardless of whether they are web or PC applications or in-house developed or off-the-shelf packages.