The HP Security Handbook

Protecting Your Business

Governance and Compliance
Proactive Security Management
Identity Management
Trusted Infrastructure
Innovation in Information Security

The HP Security Handbook

Vice President, HP Security Office
Tony Redmond

HP Security Handbook Lead
Jan De Clercq

Layout, Illustrations, Graphics and Production Lead
Killian McHugh

Primary Content Editors and Strategists
Governance and Compliance: Stuart Hotchkiss (Lead)
Proactive Security Management: Keith Millar (Lead)
Identity Management: Jan De Clercq (Lead), Mark Crosbie
Trusted Infrastructure: Boris Balacheff (Lead), Iver Band, Archie Reed, Mark Schiller, Bill Wear
Innovation in Security: Simon Shiu (Lead), Joe Pato

Additional Content Contributors

Governance and Compliance:
Lois Boliek, John Carchide, Frederic Gittler, David Graves, Jim Hoover, Cheryl Jackson, Paul Jeffries, Bill Kowaleski, Tari Schreider, Saida Wulteputte, Mike Yearworth

Proactive Security Management:
Hayden Brown, John Carchide, Tracy DeDore, Paul Jeffries, Montserrat Mane, Jim O'Shea, Christopher Peltz, Sarah Porten, Yann Vermast, Brian Volkoff, Doug Young

Identity Management:
Sai Allavarpu, Jean-Michel Argenville, Carolyn Bosco, Pete Bramhall, Christian Fischer, Ronald Luman, Marco Casassa Mont, Robert Neal-Joslin, Jason Rouault, Scott Swist, Ibrahim Wael, Manny Novoa

Trusted Infrastructure:
Enrico Albertin, Shivaun Albright, Sunil Amanna, Mike Balma, Ron Carelli, Lynne Christofanelli, Paul Congdon, Joanne Eames, Janusz Gebusia, Gary Lefkowitz, Shab Madina, Sunil Marolia, John Rhoton, Steve Scott, Rick Supplee, Tom Welsh, Chris Whitener

Innovation in Security:
Adrian Baldwin, Richard Brown, Chris Dalton, Bill Horne, Ed McDonnell, David Pym, Martin Sadler, Steve Simske, Richard Smith

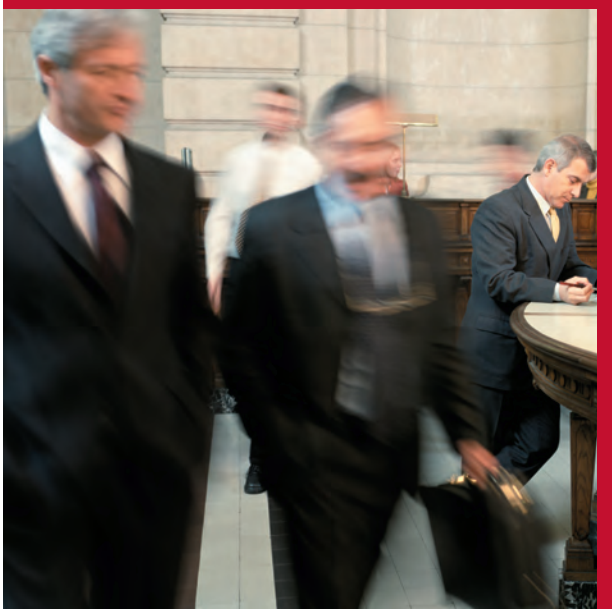
The HP Security Handbook is available online at www.hp.com/go/security/securityhandbook.
For feedback, please e-mail hpsecurityhandbookfeedback@hp.com.
For additional printed copies, please see your HP Sales Representative.

About HP

HP is a technology company that operates in more than 170 countries around the world. We explore how technology and services can help people and companies address their problems and challenges, and realize their possibilities, aspirations, and dreams. We apply new thinking and ideas to create more simple, valuable, and trusted experiences with technology, continuously improving the way our customers live and work.

No other company offers as complete a technology product portfolio as HP. We provide infrastructure and business offerings that span from handheld devices to some of the world's most powerful supercomputer installations. We offer consumers a wide range of products and services from digital photography to digital entertainment and from computing to home printing. This comprehensive portfolio helps us match the right products, services, and solutions to our customers' specific needs.

HP focuses on simplifying technology experiences for all of its customers - from individual consumers to the largest businesses. With a portfolio that spans printing, personal computing, software, services and IT infrastructure, HP is among the world's largest IT companies, with revenue totaling $104.3 billion for the four fiscal quarters ended Oct. 31, 2007. More information about HP is available at **www.hp.com**.



Fast facts

• HP was incorporated in 1939.
• Corporate headquarters are in Palo Alto, California.
• Mark Hurd is president and CEO.
• HP is a US Fortune 14 and a Global Fortune 41 company, with revenue totaling $104.3 billion for the fiscal year ended Oct. 31, 2007.
• HP has 150,000 employees doing business in more than 170 countries around the world.

Technology leadership

HP's three business groups drive industry leadership in core technology areas:

• The Personal Systems Group: Business and consumer PCs, mobile computing devices, and workstations
• The Imaging and Printing Group: Inkjet, LaserJet and commercial printing, printing supplies, digital photography, and entertainment
• The Technology Solutions Group: Business products including storage and servers, managed services, and software

Contribution

HP strives to be an economic, intellectual, and social asset to each country and community in which we do business. Key areas of contribution are electronic waste, raising standards in our global supply chain and increasing access to information technology.

Growth

HP is focused on three technology shifts that have the power to transform our customers' lives and businesses:

• Next-generation data center
• Always on, always connected mobile computing
• Ubiquitous printing and imaging

For more information, visit **www.hp.com**.

About HP's Security Practice

HP takes a holistic approach to security that includes the people, process and technology to ensure the effectiveness of the security solution. HP Services assists in defining a security strategy specifically tailored to the customer's environment and business processes. As a leader in IT management, and more specifically IT service management, HP Services brings tremendous breadth and depth of management expertise to every consulting engagement. Our expert security staff includes Certified Information Systems Security Professionals (CISSPs) and certified Sysadmin, Audit, Network, Security (SANS) individuals who bring extensive experience in multi-vendor platforms including HP-UX, IBM AIX, Sun Solaris, OpenVMS, Microsoft Windows, and Linux. As a member of the Information Technology Information Sharing and Analysis Center (IT-ISAC), HP's security services team stays abreast of the latest information on cyber security issues and utilizes proven best practices and methodologies such as BS 7799/ISO 17799.

Table of contents

Chapter One: Governance and Compliance

Chapter Two: Proactive Security Management

Chapter Three: Identity Management

Chapter Four: Trusted Infrastructure

Chapter Five: Innovation in Information Security

"The HP Security Framework covers the range of security, governance and risk management subjects required of a truly professional security programme. Security is not just a technology issue, neither is it just a single-point problem. Only by stepping back and seeing the whole risk picture can good security be made to work, and I applaud the authors of the Security Handbook in getting this message across."
-Dr Paul Dorey, CISO, BP plc, and Chairman of the Institute of Information Security Professionals (IISP)

Introduction Note

Tony Redmond

Apart from being the world's largest IT company, in many other ways, HP is a unique IT company. No other company develops the same breadth and depth of technology across all market segments - from consumer to enterprise, from small and midsize businesses to the public sector - spanning so many types of computing devices, protocols, standards, and applications. Security is and will remain a prime focus for HP across our complete portfolio because customers expect that everything that they buy from HP is secure.

The HP Security Handbook provides a view of all the different threads of security in which HP works. We plan to update the content regularly; the handbook is an evolving document that tracks new developments, adds new information as it becomes available, and presents industry standards and initiatives important to security as they mature. Much of the content focuses on the three pillars of HP's security strategy - identity management, proactive security management, and trusted infrastructures. These are all "big plays", places where HP believes that we can make a real difference in the way that people use technology.

I cannot think of a bigger challenge than building truly trustworthy infrastructures composed of new hardware architectures, new operating systems, and new applications. Federated identity management will help to liberate users from the tyranny and insecurity of multiple user name and password pairs. And proactive security management is HP's way of declaring to the security industry that it's time to stop reacting to threats and begin building intelligence in servers and other network components to better resist unauthorized intrusions. Because HP is such a large company, we have a special responsibility and role within the IT industry to help chart the future, and that's what the HP security strategy sets out to do. Big plays don't happen overnight - but these plays form the core of our strategy because they are worthwhile and will make a difference.

In addition to describing HP's security strategy, this handbook illustrates the broad sweep of security activity across the range of the company's offerings, from services to the fundamental security features incorporated in HP operating systems. It also describes the work of the Trusted Systems Laboratory and how HP researchers look at future security challenges. Commentators often say that the only guarantee regarding technology is change; this is especially true for security technology. HP's investment in research has already provided great benefits, and we expect this trend to continue.

Tony Redmond
Vice President, HP Security Office

Introduction

Information security is a fundamental necessity and enabler for modern business. Because information technology infrastructures provide the ability for enterprises to automate, adapt, and accelerate their business strategies, information security is essential for safeguarding business continuity. Whether enabling secure sharing and collaboration with partners, preventing or detecting insider attacks, or defending against indiscriminant vandalism by unseen and random network attackers - information security is a key element of any IT infrastructure.

Security, however, is not a simple commodity that can be ordered by weight and bolted on to an IT infrastructure. Security considerations should permeate every aspect of IT - from the design of applications and infrastructure to the mechanisms for managing their deployment; from discrete components that protect specific functions to the design of business objectives and the governance of corporate policy; from the management of technology to the management of people.

Measuring security is also difficult - how safe are we at any point? Unlike processor speed or storage capacity, we do not measure security in simple units - except after an incident when we can objectively demonstrate that the deployed security mechanisms are inadequate. As a result, enterprise security is traditionally mired in a cycle of reactive crises.

The Security Landscape

Enterprises face a rapidly changing environment that demands a proactive stance for information security. Key factors driving this change include:

- Unrelenting presence of security incidents through out the industry
- Ever-increasing sophistication of attack
- Government regulation
- Changes in IT infrastructure to accommodate changing business

Continuing presence of security incidents

High-profile security breaches have made network security one of the most important concerns for corporate and government networks. In the recent past, the rate of security incidents grew at a tremendous rate. More recently, the rate of attacks has leveled off, but many attacks now target specific victims or resources rather than the indiscriminate attacks prevalent earlier in the decade. As reported in the 2007 edition of CSI Computer Crime and Security Survey, the average reported annual loss from security incidents doubled from the previous year.

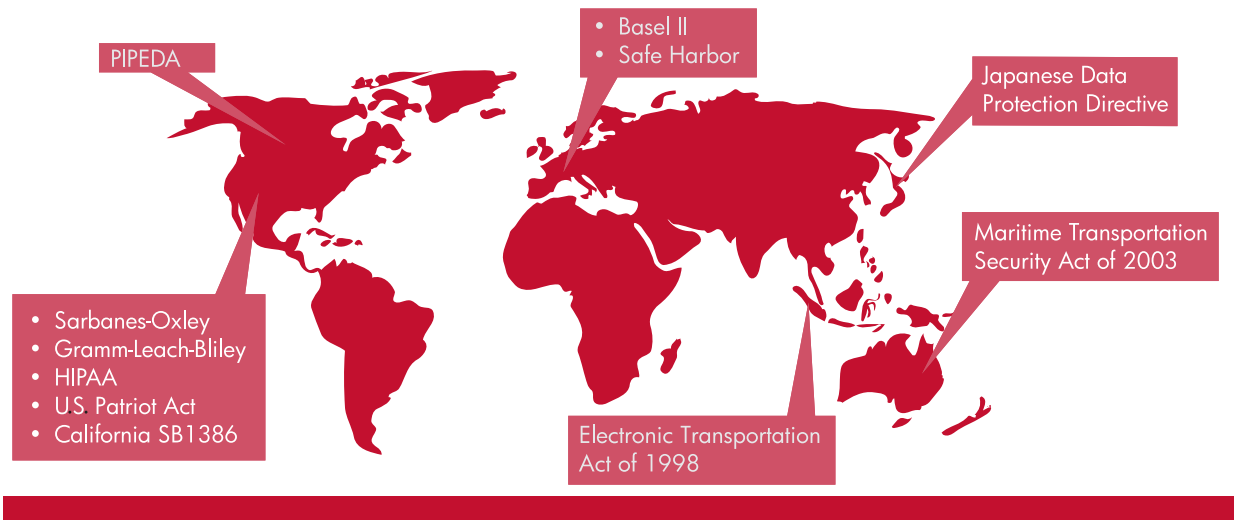
Increasing sophistication of attacks

The emergence of targeted attacks is coupled with an increase in sophistication of attack. Not only are specific victims selected for attack, but unrelated organizations or individuals are also selected for attack to serve as staging points for stealthy attacks. An underground economy has emerged for access to compromised systems for direct exploitation or for use to stage subsequent attacks.

Government response through regulation

Governments have not ignored the increasing threat to commerce. Many governmental entities have enacted or are preparing legislation to require business attention to information security issues.

Figure i-1
Sample regulations affecting security



Regulatory mandates such as the Sarbanes-Oxley Act of 2002, the California Database Protection Act of 2001, the Gramm-Leach-Bliley Act (GLB), the Health Insurance Portability and Accountability Act (HIPAA), and the Basel II Accord are an additional catalyst for applying due diligence in the security decision and implementation process. These laws impose strict requirements on enterprises to establish, identify, document, test, and monitor necessary internal control processes. Because information technology supports most, if not all, of these processes, these laws significantly affect companies' security strategies. These new regulations drive security designers and architects to impose and maintain the proper security controls throughout their enterprise.

Changing business objectives and streamlining processes

The need for business agility is driving the development of proactive security capabilities. Ad-hoc security implementations often interlock the various components of a business application, which limits the overall ability to adapt, increases the cost to operate, and often leads to diminishing protection through an application's lifetime. Enabling rapid flexibility requires an overall process for managing and evolving an organization's IT security.

HP's Security Framework

Delivering a safer enterprise IT environment aligned to defined levels of security and risk requires a framework for rapid and effective response to threats and corporate business objective changes. HP's security framework, shown in Figure i-2, enables a holistic way to proactively define and deliver security across the enterprise.

The key areas represented in this model include the three areas in which HP is investing to create innovation and differentiation: identity management, proactive security management, and trusted infrastructure. The fourth area, governance, includes the supporting services and tools that HP delivers to ensure that IT security solutions meet business objectives.

Business Context

The top level of the security framework consists of the key drivers, including business objectives, operational risk, and regulatory and legal compliance. Businesses and organizations have a set of major objectives or missions that drive their existence. In addition, they must manage operational risk and meet regulatory and legal compliance. All of these factors have direct security implications that drive the overall security strategy of a business or organization.

Figure i-2
HP's security framework

From the security perspective, examples of threats that directly affect the highest levels of a company or an organization include:

- Theft of intellectual property or digital assets
- Disruption of critical services or infrastructure that leads to lost revenues, contractual breaches, or regulatory violations
- Public disclosure of sensitive information, which negatively impacts brand identity or competitive advantage

Governance and Compliance

Governance refers to the controls and policies that translate high-level business objectives, operational risks, and regulatory needs into the directives, objectives, and policies that drive security mechanisms. Governance is a strategic component of every technology optimization initiative. It includes business logic, business procedures, managerial processes, and operational processes that are all supported by specific, lower-level policies for IT operations and security.




Proactive Security Management

Proactive security management focuses on managing security functions in support of business and organizational goals and processes. The fundamental goal of this area is to ensure that protection mechanisms operate appropriately during setup, operation, and decommissioning of various IT services. Proactive security management:

- Manages the protection of data, applications, systems, and networks, both proactively and reactively
- Supports changing business and organizational models and responds to a changing threat environment
- Maintains the level of security and operational risk defined by a company or organization

Identity Management

Identity management is the ability to identify every user, application, or device across an organization or business. It provides flexible authentication, access control, and auditing while respecting privacy and regulatory controls.

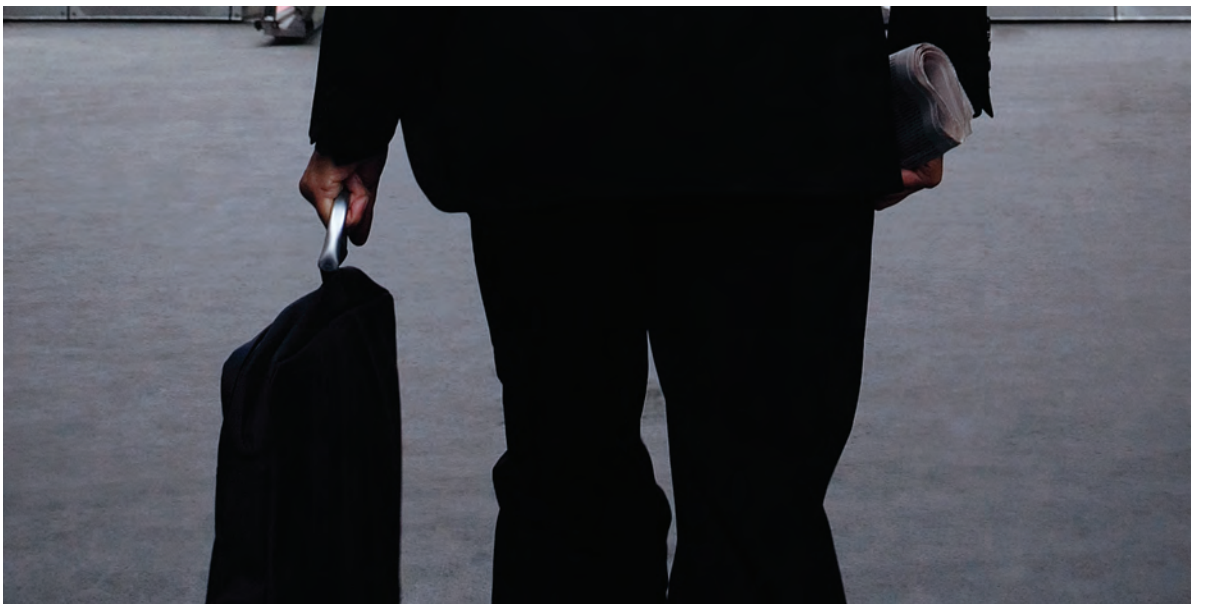
Delivered via a set of processes and tools for creating, maintaining, and terminating a digital identity, identity management allows administrators to manage large populations of users, applications, and systems quickly and easily. The tools permit selective assignment of roles and privileges, which facilitates compliance with regulatory controls and contributes to privacy-sensitive access controls.

Trusted Infrastructure

Trusted infrastructures are composed of hardware platforms, together with their operating environments and applications, which behave in an expected and predictable way for their intended purpose. Trusted infrastructures must support the IT applications underlying the most critical business processes. When IT infrastructure technologies fail to keep pace with emerging threats, we no longer trust them to sustain the applications we depend on in both business and society.

A trusted infrastructure reliably manages and controls access to information assets while delivering the power required for critical business processes. It helps implement appropriate technologies to secure the end-to-end IT infrastructure of a company or organization, worldwide - including data centers, networks, productivity tools, end-user desktops, and wireless devices.

The need for a trusted IT infrastructure flows from our increasing reliance on IT systems to do everything from running our business to running our society's utilities. Just as our dependence on IT permeates all aspects of society, security capabilities must permeate all aspects of IT infrastructure. Security must be built in, not bolted on, at the platform level, at the network level, and in the very processes used for developing systems.



Security Handbook Contents

HP recognizes the complexity of large, distributed IT environments and takes a proactive approach to enterprise security. We secure the Adaptive Enterprise with planning and preparation, rather than simply reacting to changes in the landscape. This handbook outlines HP's strategy for information security and summarizes the products, solutions, and services that address the security needs of enterprise customers. It focuses on the three pillars of HP's security strategy: proactive security management, identity management, and trusted infrastructures. Along with overarching governance considerations, these three areas bring organizations and companies a safer IT environment that can respond to changing threats and business objectives.

This edition of the handbook introduces a section on innovation in information security pursued at HP Laboratories, HP's central research organization. Uncoupled from product and services organizations, HP Labs' mission is to deliver breakthrough technologies that create opportunity beyond HP's current strategies. Some of the work performed at HP Labs has generated new capabilities which are reported throughout the handbook. This chapter addresses aspects of the longer-term challenge in information security and the work pursued by HP Labs to overcome them.

This handbook is intended for CIOs, security administrators, and other staff who are responsible for their organization's IT security and infrastructure. Each chapter begins with the definition and purpose of the topic before moving on to discuss details such as the threat environment, related trends, underlying technologies, and challenges. Each chapter concludes with information about solutions that address the security needs discussed.

Bringing the HP Security Strategy to Market: HP Secure Advantage

Security today is higher on the CIO/CTO agenda than it ever was before. They believe that security is a fundamental necessity and enabler of business outcomes. They want to be able to use HP products and plug them together easily in a secure manner. HP Secure Advantage is the framework under which this will take place. Imagine data protected from desktop to data center, from laptop to printer, throughout the network with no gaps; no places where the data has to be decrypted and re-encrypted to transition to another product. Imagine being able to demonstrate to internal and external auditors that you have a trusted infrastructure and that your data in any form is protected so that you can easily add the people processes to meet your compliance demands; that is the promise of Secure Advantage.

As this Security Handbook illustrates, HP has a unique breadth of products, from laptops to servers and storage and software to printers, using HP network components. This is why HP created the Secure Advantage framework and a portfolio of products and services to meet our customer's needs for secure data and infrastructure protection. Fortunately, HP has a 35 year history in security and is leveraging this expertise to deliver the HP Secure Advantage portfolio. This is especially important today as customers adopt the 24 by 7 next-generation data center model that enables the shift of high-cost IT silos to low-cost, pooled IT assets in order to optimize infrastructures to reduce cost, increase agility, and improve quality of service. Security is a key enabler of HP's Adaptive Infrastructure (AI) offering that provides the platform for the next-generation data center and a linkage of Security to other AI enablers such as IT Systems and Services, Power and Cooling, Management, Virtualization and Automation.

Since security and compliance are an absolute necessity for businesses today the HP Secure Advantage portfolio is designed to enable enterprises to fully automate, optimize and accelerate their IT infrastructures securely with proper validation in order to achieve better business outcomes by mitigating risk. In order to accomplish this goal across the Enterprise, HP is establishing leadership for solutions in information security, key management and compliance.

The HP Secure Advantage vision builds on today's security technologies to create a more manageable way for customers to leverage encryption and key management to protect their resources and data, and validate they are compliant with a growing set of government and industry mandates.

The HP Secure Advantage portfolio takes a layered and integrated approach and helps you extend the value of your enterprise by the following steps - as illustrated in Figure i-3 and explained in the following paragraphs:

Figure i- 3
HP Secure Advantage overview

Protect your resources by improving availability and protecting your networks, systems, applications, software and DBMS using trusted platforms. Minimize IT disruptions due to security breaches with a trusted and hardened infrastructure:

- Multiple OS platforms with the highest level of certification provide maximum proactive protection.
- Configuration and patch management provide continuous protection in changing environment.

Protect your data in all its forms: data at rest, data in transit, and data in use. Use encryption and Identity Management in combination with other proactive security management techniques such as Security Event and Information Management:

- Encryption of critical data at rest, in use or in motion increases protection.
- HP Extends this protection from desktops to servers and printers with focused Key Management.

Provide validation to you by establishing a secure audit trail across the organization as proof for compliance for internal and external auditors with real-time alerts. Utilize encryption and Key Management, working with integrated compliance solutions across organizations.

- Validate at necessary audit points to enable audit trails for compliance to industry regulations.
- Future integration of encryption and Key Management across an organization will provide end-to-end protection.

These elements are more integrated under the Secure Advantage portfolio framework and can be customized to your unique needs by HP Services through our Information Security Service Management (ISSM) Reference Model which establishes a rational basis for security decision-making, ensuring security controls align, and helping optimize business outcomes.

Table i-1 provides a set of examples of key HP Secure Advantage products and services. The table also shows the corresponding HP Security Handbook chapters, sections and pages that provide more detail on these HP Security Advantage offerings.

Table i-1
HP Secure Advantage products and services examples and HP Security Handbook links

HP Secure Advantage Product/Service	HP Security Handbook Link
Protect your Resources	
HP Configuration Management	Chapter 2 - Proactive Security Management: Section 4.2.3.3.1, page 2-23
HP Proliant Essentials Vulnerability and Patch Management Pack	Chapter 2 - Proactive Security Management: Section 4.2.3.3.2, page 2-24
Protect your Data	
HP Compliance Log Warehouse	Chapter 4 - Trusted Infrastructure: Section 7.4.3, page 4-73
HP Secure Print Advantage (SPA)	Chapter 4 - Trusted Infrastructure: Section 8.5, page 4-78
HP StorageWorks Secure Key Manager	Chapter 4 - Trusted Infrastructure: Section 7.4.2, page 4-72
HP ProtectTools	Chapter 3 - Identity Management: Section 8.2.2.1, page 3-16 Chapter 4 - Trusted Infrastructure: Section 5.4.1, page 4-28
HP- UX 11i security	Chapter 4 - Trusted Infrastructure: Section 5.4.3.1, page 4-31
Linux security enhancements	Chapter 4 - Trusted Infrastructure: Section 5.4.3.3, page 4-36
HP NetTop	Chapter 4 - Trusted Infrastructure: Section 5.4.2, page 4-30
HP Application Security Center	Chapter 2 - Proactive Security Management: Section 4.2, page 2-19 Chapter 4 - Trusted Infrastructure: Section 5.4.6, page 4-42
HP ProCurve Identity Driven Manager	Chapter 4 - Trusted Infrastructure: Section 6.8.2.2, page 4-65
HP Trusted Compliance Solution for Energy (TCS/e)	Chapter 4 - Trusted Infrastructure: Section 5.4.5, page 4-42
Provide Validation	
HP Services Information Security Service Management (ISSM)	Chapter 1 - Governance and Compliance: Section 8, page 1-16