Trusted Audit
Part of the HP SecureSolutions portfolio

Are you confident that your sensitive information is not being accessed inappropriately?

Are you compliant with the regulatory standards applicable to your industry?

HP SecureSolutions Trusted Audit allows audit data to be collected and stored in such a way that its integrity is assured.

Material such as financial records and computer system logs are collected, digitally notarised and securely stored in original form. This information can then be put to use for compliance purposes or behavioural analysis.
Trusted Audit collects log information from machines in one or more source networks and delivers these to a central location, enabling you to be confident about the integrity of the data. Once centralised, the data can be used for regulatory compliance, behavioural analysis or some other purpose if required.

Key features

- Collect audit material from any data source
- Store audit material in its original form in a storage facility of your choice
- Analyse audit material using an analysis tool of your choice
- Determine whether audit material has been modified since collection
- Collect audit material from devices when running off-line
- Transmit audit material between domains using a protocol of your choice. Standard options are data diode, Web service, HTTPS and SMTP
- Sign audit material (optionally) using the Digital Signature Algorithm, RFC3161 timestamps or a signature provider of your choice

Why Trusted Audit?

Within many computer environments there is typically a wealth of information available in log files that is difficult to make sense of; information from Windows® event logs, database logs, application specific logs etc.

Now consider a highly complex environment containing several networks where information can flow between these in only one direction via a data diode or firewall, where segregation of data is of paramount importance and making sense of the information needs to happen in an isolated network. This raises some obvious questions:

- How can the audit tools be configured to transport information between networks where each transport may require customisation unique to that environment?
- Can the integrity of the information be validated once submitted for analysis?
- Can the original log information be retained and forwarded to multiple locations to be used in different ways?
- If a person has an account in several networks, how can events from these networks be correlated to that person?

Once these questions become important, Trusted Audit becomes an obvious choice as it is intended to collect audit material from within complex multi-network environments, and deliver it to a standard location where it can be put to its intended use. Typically, the data is stored in a long-term storage archive and imported into an analysis engine for behavioural analysis purposes.
Secure Data Tunnel

Trusted Audit is one of several HP SecureSolutions that is built up on the Secure Data Tunnel; an extensible framework for collecting and distributing information in a secure and tamper-evident way.

Organisations that protectively mark data often use multiple networks to maintain separation between the different classifications of data. For the majority of day-to-day business scenarios, this is suitable but there are occasions when data needs to be transferred between different networks. While separate networks with data of different classifications satisfy the security information risk officer, efficiency and productivity of the organisation can decrease due to manual processes put in place to move data around.

Secure Data Tunnel provides a framework for transferring data from point A to point B. What separates A and B is dependent on each organisation’s security needs. Data diodes provide one-way data transfer across an air gap which facilitates complete network separation. For those not requiring physical separation, Web services across firewalls can be used. Simple Mail Transfer Protocol (SMTP) is a further option with integration with virus and content checkers. Secure Data Tunnel is a flexible and scalable framework from which organisations can implement a solution that is tailored for their specific needs.

Once a piece of data is collected, Secure Data Tunnel routes it as per the centrally defined configuration. This could be a simple one-source-to-one-destination transfer or it could be more complicated, i.e. a file is picked up from domain A for transfer to domain B with another copy sent to an archive for auditing purposes.

The integrity of the data being transferred is protected with the Tamper Evident Store built into Secure Data Tunnel. Any modifications to the data in-transit are reported. Further protection can be enforced up on the data with the use of digital signing or RFC3161 time stamping.

With Secure Data Tunnel the configuration combinations are many. Different transports, different destinations, different protection and different solutions, it’s all about picking the right combination for your organisation.
The HP SecureSolutions portfolio is specifically designed to help you meet the requirements of your business and user communities, while maintaining the highest levels of security.

**HP SecureSolutions File Courier**
Enables users to transfer files between networks of different classifications according to a set of configurable rules, maintaining a log of the sender, the type of file and the location it was sent to.

**HP SecureSolutions Secure Multiple Network Access**
Enables users to access applications and information on networks at different classifications from a single desktop without compromising data integrity or confidentiality.

**HP SecureSolutions Secure Multiple Network Printing**
Enables multiple-user networks at different classifications to share a common print infrastructure, without compromising data integrity or confidentiality.

**HP SecureSolutions One-way Transfer Gateways**
Allow files and folders, email, data streams or clipboard data to be transferred between networks across a hardware-enforced one-way connection evaluated to ITSEC E6 and Common Criteria EAL7.

**HP Secure Collaboration**
Brings together disparate individuals and organisations, as well as the processes needed to integrate people, information, systems and devices.

By aligning agencies for integrated service delivery, processes become faster, services become seamless for the customer, and a greater return on IT, people and business investments can be realised.

**HP NetTop™**
Simplifies multi-network access and high-assurance, multi-domain computing. It supports multiple security domains on one machine, non-secure software on a secure OS and data isolation.

Transforms a single workstation into a high-assurance platform running multiple operating systems concurrently – with total domain isolation between each OS and its attached network.

HP SecureSolutions Trusted Audit includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit ([http://www.openssl.org/](http://www.openssl.org/))

---

HP SecureSolutions Trusted Audit is just one of a range of security solutions.
For further information; Tel: +44(0) 1925 841881 or Email: securesolutions@hp.com
To learn more visit [www.hp.com/services/securesolutions](http://www.hp.com/services/securesolutions)