Halo Security Overview

July 2007

Overview

The security of the Halo Collaboration Studio and Halo Video Exchange Network (HVEN) system is imperative. Halo customers partner with HP knowing that we are committed to employing only those best practices and proven configurations that meet or exceed our own world-class enterprise network standards. HP gained its network security expertise while running one of the world's largest enterprise networks – the HPQnet.

The HVEN is a private network dedicated to the Halo application – it is not a general purpose network. The HVEN is not intermingled with either HP's corporate enterprise network or the enterprise networks of Halo customers. It does not interoperate with the public internet – it is composed of private leased lines that physically run through secure facilities of bandwidth providers and specifically-contracted secure carrier hotels. The circuits of the HVEN terminate on the campuses of our HCS customers, into their own controlled-access terminals. Equipment closets and racks are locked, and administrative access is logged.

Confidentiality

Network anti-spoofing and access filtering are employed at every Halo connection to the core of the HVEN to protect the overall network and inter-company connectivity from unauthorized activity. Networking devices are configured for intrusion detection and alerting. Access to network devices is via an encrypted channel; authentication occurs via a central authentication server.

No data, video or voice component of the HVEN is wireless (the mouse in the Halo Studio is wireless, though the mouse itself is not a network device and is not on the HVEN). All Halo products with unneeded physical device-ports have those ports administratively shut off. The HVEN networking devices are configured to alert for multiple forms of tampering and attempted intrusion, and all suspicious events are investigated.

HP does not store any customer data, video, or audio on any of the systems used for the Halo Collaboration Studio or the HVEN Service, nor does HP permit the capability for any recording solution to be introduced into the Halo architecture.

Any customer can be voluntarily "unlisted" in the HVEN directory – a directory which allows users to easily connect inside their own company and to partners outside their company with the aid of the HP Concierge. Other Halo customers do not see unlisted Halo customers on their HVEN directory.

In 2007 Halo will introduce a Halo cryptosystem, providing data encryption above and beyond the network and operations-derived security controls providing assurances of confidentiality for Halo customer conversations. Halo encryption will leverage the Advanced Encryption Standard encryption algorithm (AES), chosen in 2001 by the US National Institute of Standards and Technology in cooperation with the US National Security Agency (Advanced Encryption Standard, US FIPS Pub 197).

Halo's own 256-bit AES encryption of meeting content will be backed-up by 2048-bit public-key cryptography for all call signaling and encryption key management.

Integrity

Halo network and server systems on the HVEN are monitored continuously by a team of HP network system experts who monitor only the network traffic statistics, not the content (video, audio, or related meeting content) of the actual Halo events. Similarly, the HP Concierge cannot monitor the content of any Halo event. The Concierge can only access information regarding which Halo Studios are connected.

All Halo server and network devices connected to HVEN undergo standardized build and check-out procedures, and are managed throughout their lifecycles within the Halo business's asset and configuration-management systems. Maintenance, upgrades and trouble-shooting of Halo systems are supported by authenticated and independently audited access controls. Log files of systems and network activity are reviewed for abnormal/suspicious signatures, in addition to failed authorization and access attempts, all of which trigger security investigations. Halo leverages formal operating system and firmware patching procedures, and where applicable installs anti-virus software.

Halo utilizes formal risk-management practices including threat and vulnerability modeling, and evaluation of proper operational controls to mitigate risk across the platform.

Availability

HP confirms the end points engaged in a Halo conference event and will only allow connections between authenticated Halo systems. Accompanying Halo's coming (2007) encryption services, Halo's authentications system will be based on independently issued digital certificates, each verifiably unique to individual Halo hardware.

In coordination with independent network-circuit management performed by bandwidth providers, Halo staff ensures the availability, and swift remediation of the Halo solution against natural and man-made forms of wide-area network interference. In the event of suspicious network anomalies or qualified security events, Halo initializes an incident response process to contain, characterize and eliminate risk to Halo customers. Individual Halo Collaboration Studio customer sites are easily quarantined should any abnormality surface.

Continuous Rigor and Evaluation

Finally, to assure that security and risk management efforts by the Halo team are relevant and meet customer expectations, a thorough security assessment of the entire Halo system has been certified by HP information security experts. Further, HP's objective is to demonstrate Halo's commitment to overall security through ISO-27001 certification of Halo's operations. An organization's certified information security management system (ISMS) informs its partners and customers that the security practices in place are rigorously managed and have been suitably examined by unbiased third parties skilled in information security. HP has begun the process to secure certification of its Halo information security management system. This certification requires extensive analysis and reporting of all domains of security described in the internationally recognized and broadly adopted ISO/IEC-17799:2005. At present, Halo is diligently working toward the certification goal, refining security processes and sustaining an overarching strategy of continuous improvement.

Please visit **www.hp.com/halo/contact_email.html** today and connect with a Halo business specialist to schedule a demonstration, receive additional information about Halo or find out how Halo can help transform your business.

4AA1-1997ENA, 8/2007