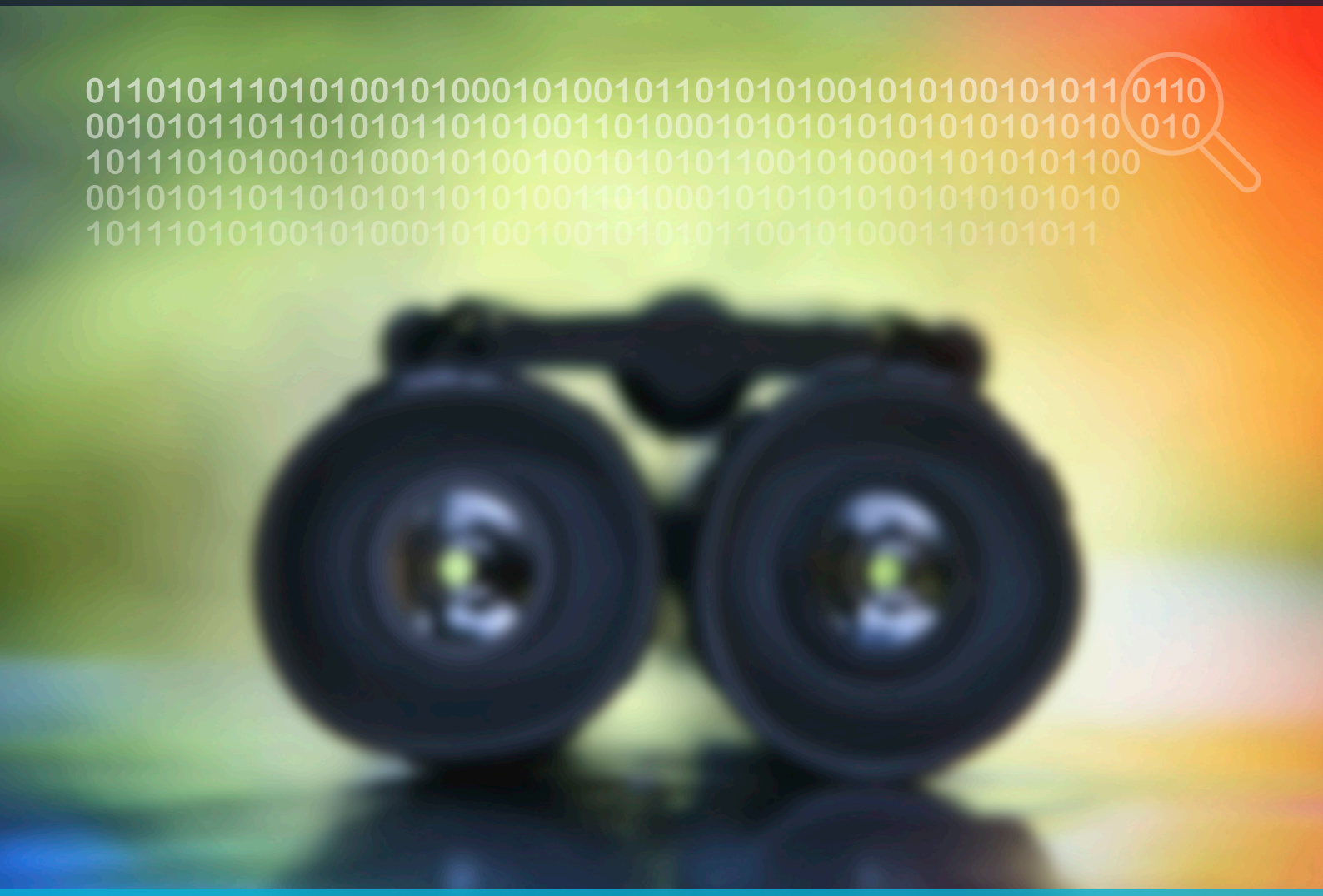
A SECURITY AND COMPLIANCE WHITE PAPER



PREVENTING DATA LOSS THROUGH PRIVILEGED ACCESS CHANNELS

ssh communications security

TABLE OF CONTENTS:

ssh communications security

ABOUT SSH COMMUNICATIONS SECURITY

As the inventor of the SSH protocol, we have a twenty-year history of leading the market in developing advanced security solutions that enable, monitor, and manage encrypted networks. Over 3,000 customers across the globe trust the company's encryption, access control and encrypted channel monitoring solutions to meet complex compliance requirements, improve their security posture and save on operational costs. SSH Communications Security is headquartered in Helsinki and has offices in the Americas, Europe and Asia. The company's shares (SSH1V) are quoted on the NASDAQ OMX Helsinki. For more information, visit www.ssh.com

INTRODUCTION

"Trust is no longer a guessing game: Gain immediate visibility and control on encrypted third-party access within your network."

A basic tenet of security is to apply the strongest safeguards to the highest value targets. Systems and IT administrators comprise a set of privileged users granted access to very high value targets. Their access rights include, to name a few, the ability to create new virtual machines, change operating system configurations, modify applications and databases, install new devices - and most of all, direct access to organization's protected data (let it be financial or health, for example). If misused, the privileges they are granted can have devastating consequences.

Simultaneously the extent of privileged access is expanding to entities outside the enterprise through outsourcing arrangements, business partnerships, supply chain integration, and cloud services. The growing importance and prevalence of third-party access is bringing matters of trust, auditability and data loss prevention to the forefront of security compliance and risk management.

As being compliant against any typical standards and norms mandates privileged access to be secured by encryption, it is opaque to standard layered defenses, such as next generation firewalls and data loss prevention systems. The resulting loss of visibility and control creates a heightened risk for undetected data loss and systems damage as well as an attractive attack vector for malicious activity like stealing information and disrupting operations, while hiding all traces from the system audit logs. Auditors are always thoroughly testing privileged access controls as they are key controls for example for financial and health industry organizations. Lack of visibility into administrator's activities will lead to audit exceptions.

This white paper focuses on how organizations facing these issues of privileged access can effectively balance the challenges of cost, risk and compliance. It describes how privileged access governance can be made minimally invasive, scale to enterprise requirements, and most importantly, prevent costly losses and potential audit exceptions.

THE PRIVILEGE / TRUST RATIO

In corporate governance, trust is normally inversely proportional to privilege. To give a simple example: high trust is given with respect to access to the office supply closet, a low privilege activity. On the other hand, those with access to the corporate bank account are not trusted. Multiple levels of signature and audit are required.

While the SSH protocol ensures the activities of privileged users are well secured from eavesdropping, it also results in their actions being largely unmonitored. This is a fundamental gap in security in terms of both risk management and compliance. A monitoring, audit and control solution is needed to establish the correct privilege to trust ratio. Table 1 summarizes the requirements of such a solution:

Requirements	Cost	Risk	Compliance
Regulations and security standards (e.g. PCI DSS) require encryption of data in transit, but also full auditing of privileged user activity and individual accountability.			X
Centralized visibility of encrypted remote system access, privileged user activities and data transfers.	X	X	
Real-time information, alerts, intrusion or data loss prevention capabilities for encrypted connections - crucial especially for external connections.		X	
Strongest audit capability over administrators (internal/external) who have the biggest operational power over the IT infrastructure and systems: Those with ability to modify logs, shutdown the auditing services and erase or hide their actions.		X	X
Streamline complex, time consuming and error prone processes for reacting to security events. Effective workflow for troubleshooting and forensics.	X	X	
Non-invasive auditing. Limited changes to end-user experience and current workflow processes.	X		
Limited, non-invasive changes to network topology.	X		
Fault tolerance in the system.	X	X	
Effective integration with established layered defenses (NGF, IPS, SIEM, DLP).	X	X	

Table 1: Cost, Risk and Compliance Requirements for Privileged Access Management

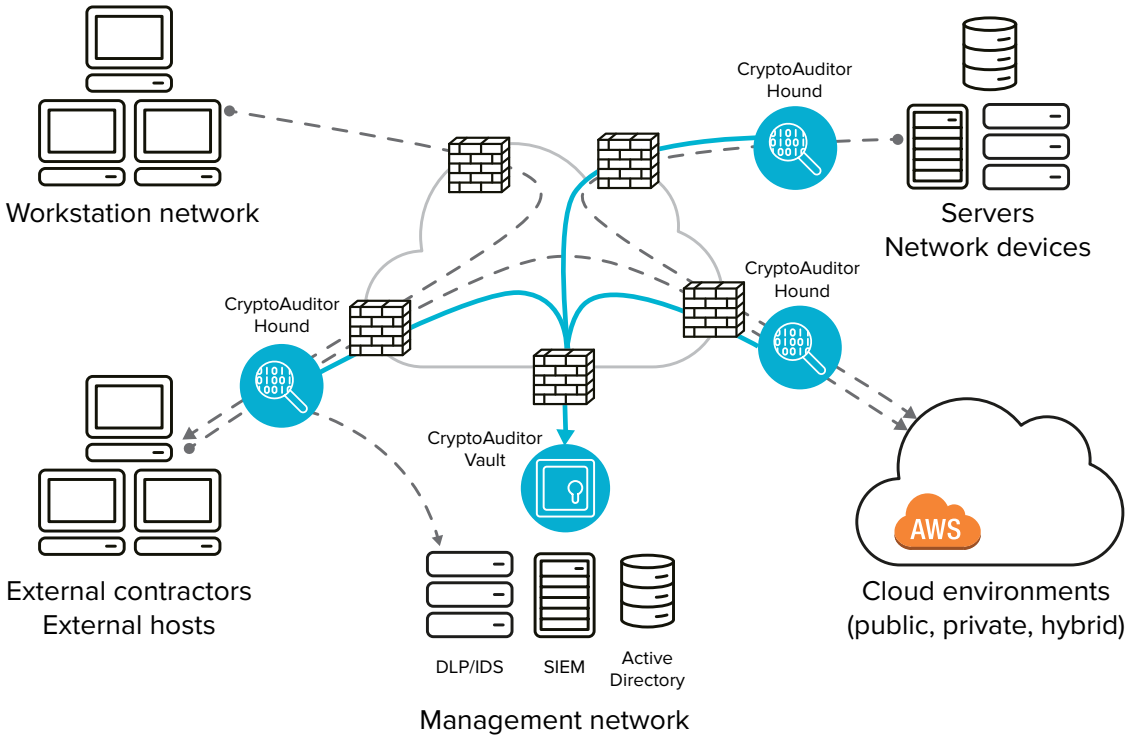
CRYPTOAUDITOR: MINIMALLY INVASIVE PRIVILEGED ACCESS MANAGEMENT SOLUTION

CryptoAuditor is a network-based virtual appliance that has the capability to control, monitor and audit encrypted sessions, as well as file transfers. It is purpose-built to be lightweight for this task and requires no agents to be deployed or access portal to go through, making it fast to implement and having no impact on end-user experience or workflows. CryptoAuditor is available as stand-alone virtual appliance as well as through the AWS Marketplace.

Further Details:

- Accountability and review: Full session recording, search and playback features enforce accountability for privileged user operations within the network. Visual playback of administrator sessions provides fast and powerful review for troubleshooting and incident response, beyond simple log entries.
- Real-time defense: SIEM, DLP and IDS gain real-time visibility into encrypted sessions.
- Fast, easier access: Drop in as transparent inline router or bridge, or as a bastion host, and utilize the user mapping capability for shared accounts to enable fast access to system and application accounts for administration and management purposes, without additional authentication steps – while enforcing full session recording and accountability for privileged users. No changes are required to the end-user tools, workflow or the target host instances, enabling cost-effective access to enhanced security.
- A flexible solution: Distributed architecture designed for virtual and cloud environments enabling flexible deployment and adaptability to changes in cloud or any other networks. No additional software needs to be installed on the user workstations or server instances.

The diagram below presents an example of CryptoAuditor's distributed deployment model.



Distributed Architecture with Central Security

Audit trails are stored and indexed in real-time into the centralized management node (Vault). This provides an enterprise-wide view of all remote system access connections including the actual contents of the encrypted connections. It enables content-based searches and real-time alerting to provide proactive security measures.

High Availability and Scalability

CryptoAuditor provides active/passive fault tolerance to ensure users are not prevented from doing their work in the event of a node failure. Failover to the passive node and bringing it up to active state is automatic. Distributing the network-auditing Hound nodes enable scaling up the capacity and placing those lightweight components to critical points in the network.

User Mapping into Shared Accounts and Enterprise Authentication

Managing separate end-user accounts for server access is not necessary with CryptoAuditor, as it integrates with existing RADIUS, Active Directory and other LDAP-compliant services in use. Individual users can be mapped to a shared account on the server while maintaining exact visibility into the real user identity.

4-Eyes Principle and Support for Strong Multi-factor Authentication

CryptoAuditor has an in-built capability for enforcing 4-eyes principle for audited connections that may involve critical administrator actions. Specific CryptoAuditor administrators can accept or deny new connections, or terminate any on-going session.

Taking advantage of the Tectia MobileID –product integration, CryptoAuditor also supports two-factor authentication over the cost-effective and logistics friendly mobile phone.

Built for the Cloud

Capacity can be adjusted on the fly thanks to the components being virtual appliances, portable to any network from on premise to cloud. CryptoAuditor can be evaluated on AWS Marketplace in less than 15 minutes.

Role-Based Management and Access Control

CryptoAuditor provides role-based access control providing the ability to granularly control what actions the administrators of CryptoAuditor may or may not manage or view in terms of audit trails, connection rules and logs, channel management, host groups, alerting and reporting settings.

Policy-Based Access Control

The CryptoAuditor connection policy engine provides the guidance for connection capturing and auditing rules, as well as full control capabilities over the sub-channels. For example, you can set protocol-level management to allow or deny tunneling, X-11 forwarding, as well as define which of the channels are audited and indexed. This enables not only granular auditing controls but also ability to control what privileged user actions are permitted and from which locations.

Session Playback and Searches

CryptoAuditor can playback sessions as a video stream. Besides the terminal sessions, by utilizing in-built Optical Character Recognition (OCR) engine, CryptoAuditor indexes even graphical sessions to enable free-text searches into the audit trails for identifying commands utilized or specific keywords. You can view the session videos directly through a web browser, retroactively or in real time.

Certified Auditing Capabilities

CryptoAuditor integrates with leading Data Loss Prevention and Enterprise Incident Management Systems and infrastructures, as it has been certified as McAfee, RSA, IBM Security QRadar, Amazon Web Services, and VCE Vblock System compatible.

Real-Time Response

Leveraging DLP integration, CryptoAuditor can stop unauthorized commands or content from executing and prevent malware propagation that would normally be unnoticed because of the encrypted SSH, SFTP or HTTPS channels. SIEM integration via syslog enables real-time alerts to existing enterprise systems.

Integrity of Audit Trails

Audit trails are stored using strong AES encryption.

GAIN COMPLIANCE

CryptoAuditor supports the compliance requirements of the largest enterprises. Table 2 depicts the primary points related to controlling, monitoring and auditing privileged user access in accordance with PCI DSS section 10. Similar compliance requirements exist in Sarbanes-Oxley, HIPAA/HITECH, and other laws, regulations and mandates.

PCI-DSS Requirement		CryptoAuditor Solution:
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	• Additional control to restrict outbound traffic from restricted Cardholder Data Environments (CDE).
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, SFTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	• Acts as additional security feature by providing visibility into encrypted administrative user sessions.
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	• Prevents dev/test systems from connecting to CDE.
6.4.2	Separation of duties between development/test and production environments.	• Additional control used to enforce segregation of duties.
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	• Automatically deny certain usernames (e.g., root) from accessing protected servers. • Control who can use a specific username to access the server.
8.1.5	Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.	• Restricts third-party access and provides visibility and monitoring capabilities of their sessions.
10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	• Automatically deny certain usernames (e.g., root) from accessing protected servers. • Control who can use a specific username to access the server.

Table 2: PCI-DSS requirements for privileged access monitoring

PCI-DSS Requirement	CryptoAuditor Solution:
10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.2 All actions taken by any individual with root or administrative privileges. 10.2.3 Access to all audit trails. 10.2.4 Invalid logical access attempts. 10.2.5 Use of identification and authentication mechanisms. 10.2.7 Creation and deletion of system level objects.	• All actions of privileged users are visible in the connection replay stored at the central Vault. • The contents of the connections can be indexed, and searched based on keywords. • Audit trails are stored encrypted in the central Vault. There can be multiple Audit Storage Zones in the Vault, each with its own set of encryption keys. • Only users with special permissions are allowed to view the audit trails. Multiple role-based access levels can be enforced. • Access to a connection replay is logged in the system log. • Denied connection attempts of both the audited users and the CryptoAuditor administrators are logged in the system log. • Used authentication method is visible in the audit trail. • The connection replay shows the full scope of the privileged user's actions. • All configuration changes made to the CryptoAuditor system itself are logged.
10.3 Record at least the following audit trail entries for all system components for each event: 10.3.1 User identification. 10.3.2 Type of event. 10.3.3 Date and time. 10.3.4 Success or failure indication. 10.3.5 Origination of event. 10.3.6 Identity or name of affected data, system component, or resource.	• The listed data is stored for all audited connections in the central Vault and advanced searches can be used to drill down to the interesting information.

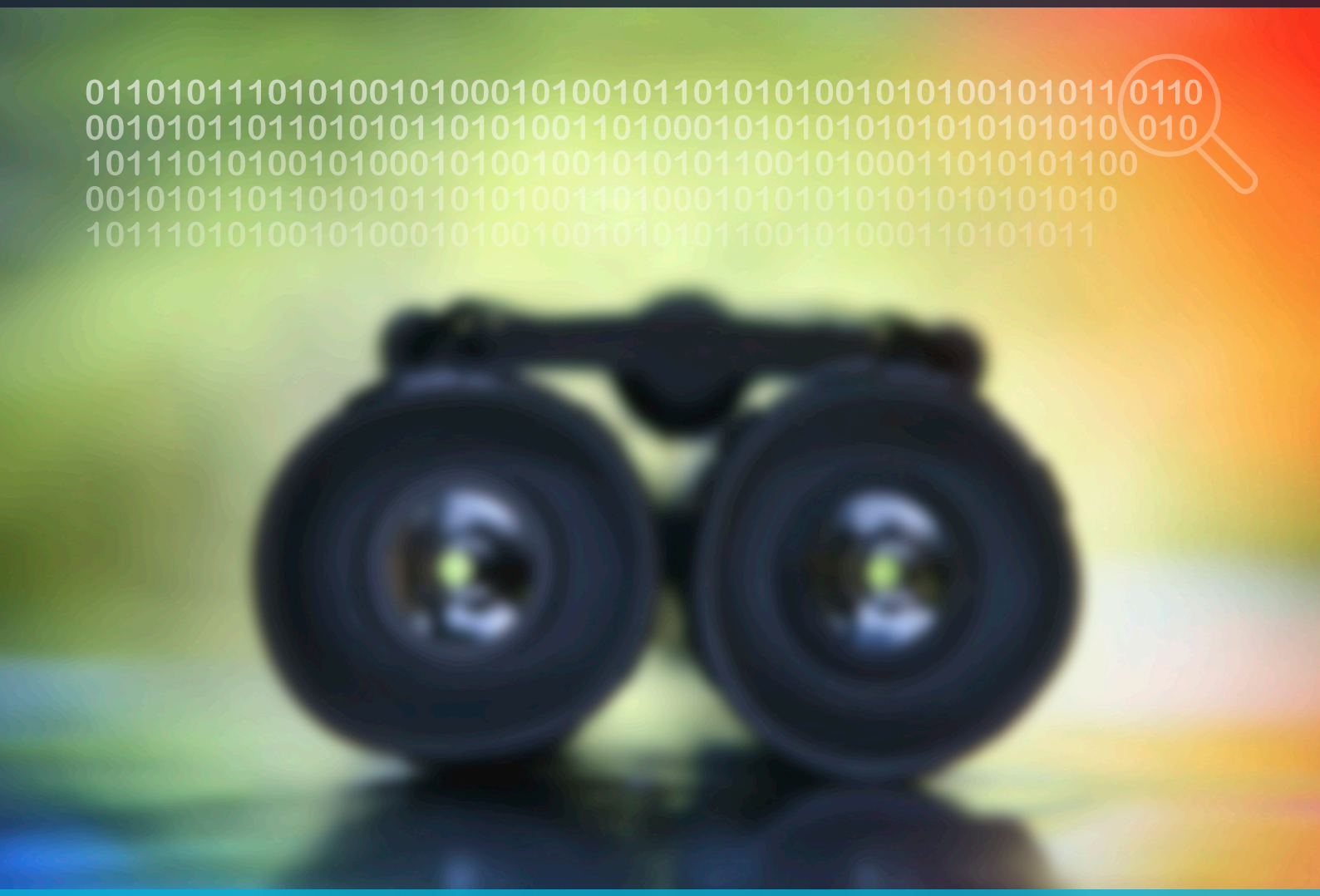
Table 2: PCI-DSS requirements for privileged access monitoring (cont.)

CONCLUSION

Cost effectiveness, risk mitigation and compliance comprise the primary requirements for restoring the correct balance of privilege vs. trust with respect to actions of highly privileged users and processes. In the past this led to unpleasant tradeoffs related to changes in administrator workflows and tools used in their daily work, as well as burdensome changes to network topology. Few tools existed for demonstrating compliance to PCI DSS, Sarbanes-Oxley, HIPAA/HITECH, and other laws, regulations, and mandates.

CryptoAuditor is a powerful monitoring, auditing and forensics tool for privileged, secured connections. It enables enterprises to reach compliance goals, while cost-effectively raising the security level of the operational environment.

For more information on CryptoAuditor, please visit www.ssh.com.



ssh communications security