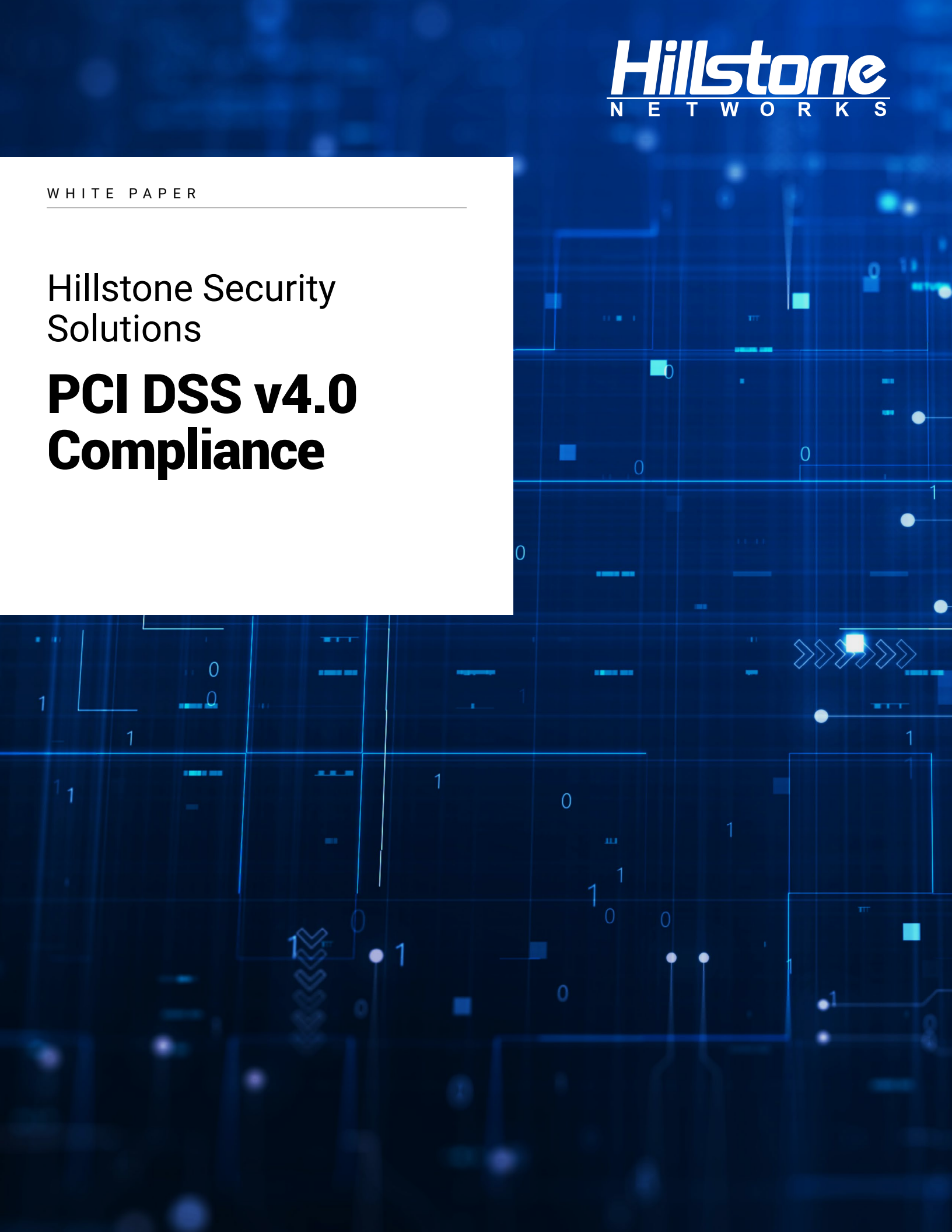


WHITE PAPER

Hillstone Security
Solutions

PCI DSS v4.0 Compliance



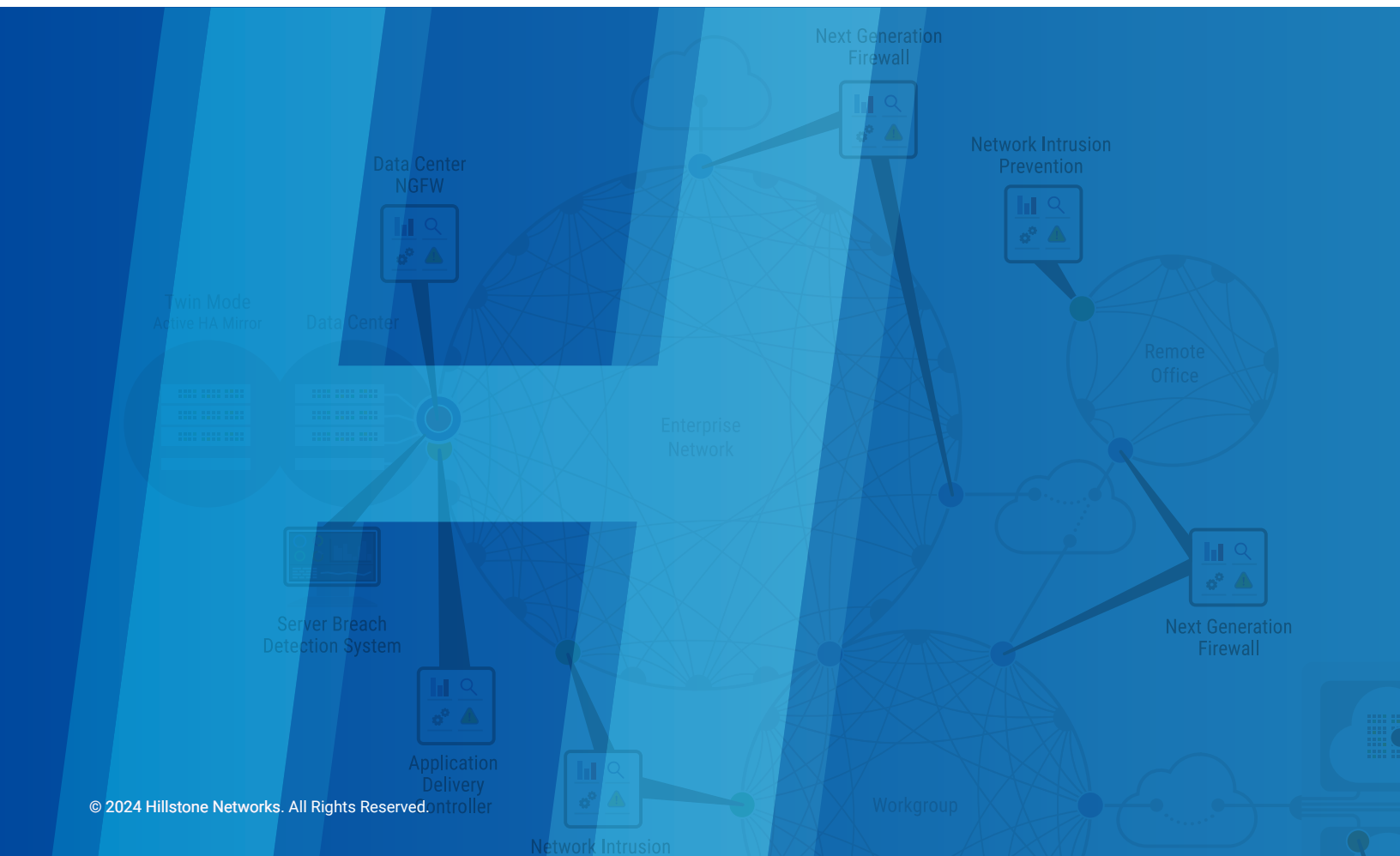
Overview

With the rapid growth of network information technologies and network size, corporate business applications, networks, and data centers are continuously under attack by increasingly creative and sophisticated methods. Standards and requirements such as the Payment Card Industry Data Security Standard (PCI DSS v4.0) strive to improve the overall security of stored and transmitted data and transactions in distributed networks and data centers of enterprises and governments.

The PCI Security Standards Council maintains payment card industry standards for the safety and protection of cardholder data worldwide. The PCI DSS v4.0 standards help merchants and financial institutions understand and implement security policies, technologies, and ongoing processes to protect payment systems from cardholder data breaches and theft. The Hillstone security product line, including solutions for perimeter protection, breach prevention, data center protection, cloud protection, security management, and security services, helps merchants and financial institutions implement features and solutions to meet the PCI DSS v4.0 requirements.

Contents

- PCI DSS v4.0 Requirements 3
 - 3 PCI DSS v4.0 Key Dates and Changes
- Hillstone Security Solution 4
 - 4 Hillstone Firewall Security Features
 - 4 Prevention, Detection, and Reaction Features
 - 8 Encryption Features
 - 9 Access Control Features
 - 10 Vulnerability Management Features
- Hillstone DSS 4 Compliance Summary 10



The PCI DSS v4.0 standards were developed to encourage and enhance cardholder data security and facilitate the global adoption of consistent data security measures.

PCI DSS v4.0 provides a baseline of technical and operational requirements to protect cardholder data.

It applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. Table 1 summarizes the six control objectives and twelve PCI DSS v4.0 compliance requirements.

Control Objective	Requirement
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls.
Build and Maintain a Secure Network and Systems	2. Apply Secure Configurations to All System Components.
Protect Stored Account Data	3. Protect Stored Account Data. 4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software. 6. Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know. 8. Identify Users and Authenticate Access to System Components. 9. Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data. 11. Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	12. Support Information Security with Organizational Policies and Programs.

Table 1: PCI DSS v4.0 Requirements

PCI DSS v4.0 Key Dates and Changes

The PCI Security Standards Council retired v3.2.1 in March 2024 to help organizations transition to PCI DSS v4.0. Some of the v4.0 requirements will be mandatory by March 2024, while some, especially the new ones, will be required by March 2025. For more details, please refer to the [summary of changes](#).

PCI DSS v4.0 changes how payment data security is enforced and operationalized. The new standard highlights the importance of web application firewalls (WAFs) from a recommended security measure to a requirement. The WAF requirement mentioned is critical because it reflects the industry's efforts to prevent web attacks before they can cause harm. Requirement 6.4.2 explicitly states, "Deploy an automated technical solution for public-facing web applications that continually detects and prevents web-based attacks." The WAF provision will be enforced on March 31, 2025.

Hillstone Security Solution

The PCI DSS v4.0 standards provide an actionable framework for developing a robust payment card data security process—including prevention, detection, and appropriate reaction to security incidents.

Hillstone offers a range of sophisticated, high-performance hardware—and software-based intelligent

firewall products, including the E-Series NGFW, the T-Series iNGFW, the X-Series Data Center Firewall (DCFw), and the CloudEdge virtual NGFW. A firewall is a fundamental element in enabling security in any data center or computer network and helping to offer compliance with the PCI DSS v4.0 standard.

Hillstone Firewall Security Features

All traditional firewall features are supported, including (but not limited to)

- Stateful firewall
- Access Control
- Attack Defense
- Intrusion Detection and Protection (IDS/IPS)
- High Availability
- Dynamic Routing
- Security zones and policies
- Quality of Service (QoS) support
- Distributed Denial of Service (DDoS) detection and prevention
- IPv4 and IPv6 support
- Network Address Translation (NAT) support
- Port Address Translation (PAT) support
- Virtual Private Network (VPN) support
- Tunneling technologies
- Application Identification and Signatures
- Security policies based on applications, users, and groups
- Logging and Reporting

Prevention, Detection, and Reaction Features

Hillstone offers numerous features that help you analyze the risk of a configuration or situation, help you detect known as well as previously unseen threats, help with incident investigations via logs and other tools, and allow you to minimize risk when upgrading, or changing the configuration of, your network. Hillstone product features in this category include:

- **Web Application Firewall:** Hillstone W-Series Web Application Firewall (WAF) provides enterprise-class, comprehensive security for web servers, applications, and APIs. It defends against attacks at both the network and application layers, providing protections against DDoS, the OWASP Top 10 threats, and bot attacks, to list a few examples. In addition, the WAF validates APIs against the schema defined in OpenAPI and automatically generates positive security model policies to detect and defend against attacks and misuse. Hillstone's app firewall combines traditional rules-based detection with innovative semantics analysis. This dual-engine approach significantly increases accuracy while minimizing false positives by creating a context-aware analysis engine. Hillstone WAF also leverages machine learning technology to fine-tune security policies and block unknown threats and attacks. Furthermore, logs can be automatically aggregated across multiple dimensions, allowing admins to easily identify suspicious anomalies or locate false positives and then further refine policies as needed.





- **Zero Trust Network Access:** Hillstone ZTNA takes the identity of a user, their role in the enterprise, their location of access, and device state into consideration when granting access to enterprise resources. ZTNA implementations can protect resources anywhere – in branches, in enterprise data centers, or even in the cloud. It has the flexibility of providing different levels of access privileges based on a combination of attributes. For example, companies can limit employees to read-only versus write access if the employee is connecting from an untrusted public WiFi at an airport. This approach ensures that enterprises are minimizing their attack surface without impeding employee productivity.



- **Hillstone iSource:** A data-driven, AI-powered XDR platform that integrates massive security data, correlates and investigates incidents, identifies potential threats, and automatically orchestrates security to respond cohesively across multiple security products and platforms. iSource brings a radical new approach to cybersecurity with unrivaled security operation efficiency. Integration Spanning the Ecosystem iSource can integrate a wide variety of data across the full spectrum of the network, from endpoints to cloud. This data can include NetFlow, Sysmon, Syslogs, metadata, threat information and third-party logs, all of which are then standardized, correlated and analyzed to provide complete visibility and break down security information silos. It not only brings full security visibility with far fewer blind spots, but also improves detection accuracy by minimizing false positives.



- **Abnormal Behavior Analysis:** This unique Hillstone technology offers a cutting-edge method of detecting unknown threats by analyzing user and server traffic, tracking a myriad of traffic parameters, and correlating the gathered data to limit risk and reveal potential new threats. Behavior patterns are baselined, violations against these baselines are deemed abnormal, and the system generates threat warnings. These system warnings enable you to recognize and prevent potential new threats before they impact your network operation or applications.



- **Packet Route Inspection:** Another unique Hillstone capability that allows you to proactively avoid security compromises and reduce the risk of launching new services in your network. This set of features offers advanced tools and firewall self-analysis to verify existing firewall configurations, test planned configuration changes before deployment, and analyze and report on network traffic through the firewall in real-time.



- **Session Limits:** This functionality limits the number of active sessions and the new session ramp-up rate for a source IP address, destination address, a specific IP address, or a service in a security zone of the firewall. It helps mitigate DOS attacks against your network.



- **Managing Network Health and Proactive Detection:** The firewall continuously monitors network health and status and reports on appliance resource utilization, network node connectivity, and business service levels and availability.



- **Connectivity and Business Continuity:** Functionality such as stateful high availability, redundant link and interface configurations, and load balancing configurations offer network safeguards against outages precipitated by a malicious network access breach.



- **Visibility and Monitoring:** Hillstone's security appliances provide monitoring, logging, and notification of incidents or suspicious activity that may indicate an incident. This allows organizations to respond quickly and proactively to new and well-known threats. SNMP (Simple Network Management Protocol) reporting and notification to a remote server are also supported.

Statistics supported by Hillstone devices include:

- **Interface-based statistics:** Traffic passing through an interface.
- **Address-based statistics:** Traffic to or from the specified source or destination address.
- **Application-based statistics:** Traffic that belongs to the specified application.
- **Stat-set:** Data passing through the Hillstone device.

- **Logs:** Hillstone devices support numerous local (on the device) and remote (SNMP) logging facilities for auditing and tracking purposes, including:

- Security logs: System security events, such as attack defense and application security.
- IPS logs: Events related to network intrusion protection.
- Configuration logs: Describe changes in system configuration.
- Network logs: Information on the operation of network services (e.g., PPPoE or DDNS).
- Network Behavior Control (NBC) logs: Information on network behavior controls, e.g., web surfing behavior.
- Traffic logs: Information on traffic flow and policy control.



- **Network Segmentation:** The network can be segmented physically (by port) and virtually (virtual system, VSYS) into security segments. Network segmentation allows a high degree of isolation between different administrators, users, and network traffic and, therefore, imposes strict access control to different aspects of the system.



- **Virtual System (VSYS):** Each VSYS has its own administrators, independent virtual routers, zones, address book, service book, independent physical and logical interfaces, and independent policy rules.
- **Zone and Physical Port Segmentation:** Zones divide the network into multiple segments, usually trusted (Intranet) and untrusted (where security threats exist). Policy rules are applied to control traffic flowing (and therefore access between) between zones. One or more physical interfaces are based on a zone

- **Firewall Policy Controls:** Firewall policy control can be applied by service and by application. A policy is a set of configuration rules to inspect and control traffic flow between security zones or segments. By default, Hillstone devices deny all traffic between security zones or segments. Configured rule policies, if present, identify which traffic is permitted between zones and segments. Security policy rules can be based on application, role, or geo-location. Additional security policy features include redundancy inspection, policy groups, policy configuration rollback, a policy assistant for easy detailed policy deployment, and policy analysis and invalid policy clean-up tools.



- **Intrusion Detection and Prevention (IDS/IPS):** IPS monitors various IPv4 and IPv6 network attacks in real-time and takes appropriate actions (like blocking them) against the attacks. The IPS signature database contains nearly 3000 signatures of known threats and is updated automatically every day. Specific IPS capabilities include protocol anomaly detection, rate-based detection, custom signatures, manual and automatic push or pull signature updates, and an integrated threat encyclopedia.



- **Anti-virus/Malware:** Hillstone devices include a comprehensive, high-speed, high-performance, and low-delay anti-virus solution to detect and defend targeted and advanced persistent threats. Various threats, including worms, Trojans, malware, and malicious websites, are detected and processed according to configured actions. A Kaspersky virus signature database is used, and Hillstone devices are integrated with the Google Safe Browsing database. The virus signature database includes over 10,000 signatures. Daily auto updates and real-time local updates are supported, as well as the ability to scan compressed files.





- **Web or Uniform Resource Locator (URL) Filtering:** This function blocks browsing to, or content from, malicious websites.



- **Default Settings to Block Traffic:** Most configuration parameters in Hillstone devices have a default setting of “disabled” or “deny,” so in the absence of explicit administrator action and configuration, threats and access attempts entering the network (or zones or segments) are blocked. Dynamic web filtering with a cloud-based real-time categorization database is supported.



- **Attack Defense:** Various types of attacks against a network can allow a hacker to gain unlawful entry to the network and, therefore the ability to exploit formation and system configurations. Hillstone devices can defend against these types of attacks, including the following:

- IP Address Spoofing
- Land Attack
- Smurf Attack
- Fraggle Attack
- WinNuke Attack
- ICMP Flood and UDP Flood
- IP Address Sweep and Port Scan
- Ping of Death Attack
- Abnormal Protocol Attack
- Anti-DoS/DDoS, including SYN Flood and DNS Query Flood

Additionally, Hillstone devices offer the following features to strengthen security control and access control to the network:

- Host defense
- Host blacklist
- IP-MAC binding
- DHCP snooping
- ARP inspection
- ARP defense



- **IP Reputation:** Botnet server IP blocking using a global IP reputation database.



- **Application Control:** Over 3,000 applications can be filtered by name, category, subcategory, technology, and risk. Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference.



Encryption Features

Confidentiality of information such as credit card transactions means that data or information is not made available or disclosed to unauthorized persons or processes or access. Encryption is the process of encoding stored or transmitted information so that it is unintelligible until it is decoded by the intended recipient.

- A Virtual Private Network (VPN) is the most common technology to protect and secure a communications channel between two endpoints. A VPN is a generic term and generally include: Tunneling technologies where the packets are encapsulated in an outer header that hides the addressing details of the actual communicating parties.
- Encryption technologies where the packet contents (header and/or payload contents) are encrypted with a key and can only be decrypted by a recipient that also has the key.

Hillstone product features and capabilities in this category include:

- **Secure Remote Access:** Discussed in more detail in the section on “Access Control Features”.
- **Virtual Private Network (VPN):** A VPN builds a private communications channel across a public (untrusted) network segment. A VPN uses a tunnel protocol to encapsulate the transmitted information and usually also a security service (such as encryption, integrity checking, and authentication) to protect the information. Hillstone devices support the following types of VPN technologies:
 - IPsec VPN: IPsec uses 3DES, AES DES, AES128, AES192, AES256 encryption, MD5, SHA1, SHA256, SHA384, SHA512 authentication and is usually deployed as a site-to-site VPN technology. IKEv1 and IKEv2 (RFC 4306) are supported.
 - SSL-based: SSL uses 3DES encryption and provides an encrypted remote user access solution.
 - Secure Connect VPN (SCVPN): An SCVPN provides an encrypted remote user access solution.
 - Plug-and-Play (PnP) VPN: A Hillstone VPN solution that simplifies the configuration of an IPsec VPN.
 - Dial-up VPN: VPN technology that establishes communication with multiple remote clients on an as-needed basis, typically deployed as site-to-site VPN technology.
 - L2TP VPN: VPN tunnels can operate in one of two modes:
 - o Policy-based VPN: Bind VPN tunnels to policy rules to transfer the specified traffic through tunnels.
 - o Route-based VPN: Bind VPN tunnels to tunnel interfaces and then make the tunnel interface the next hop of the static routes. The specified traffic is transmitted through VPN tunnels.
- **Tunneling:** Tunneling technologies encapsulate a data packet in an outer header so that the sender and recipient addresses are hidden, and thereby establish a private communications channel or VPN. Tunneling technologies do not inherently provide security (encryption), but can be used in conjunction with IPsec to provide a secure VPN channel. Hillstone devices support the following types of tunneling technologies:
 - L2TP
 - GRE
 - IPv6 tunneling with DNS64/NAT64

Access Control Features

Hillstone product features and capabilities in this category include:

- **Administrator (User ID) Login and Password Control:** System access is protected by defining user names and passwords required for login. HTTPS (Secure HTTP) and SSH (Secure Shell) and SSL are supported to provide session encryption for user names and password transmitted across the network from remote locations. Privileges (read/write/execute) are defined per username to limit access to system functionality. Maximum session duration and maximum number of failed login retries can be specified. Forced logoff upon session inactivity is supported. Successful and failed user login attempts are logged to system logs.
- **Administrator Authentication:** Administrator logins to the system are authenticated with a user name and password. Additional authentication for remote logins include:
 - Web authentication: All HTTP requests to the system are redirected to a WebAuth login page, where users provide a user name and password. Role-based policies and logins can be established.
 - Single Sign-on (SSO) agent: Users are authenticated by an Active-Directory lookup.
- **Secure Connect VPN (SCVPN) and Digital Certificates:** Hillstone devices provide a secure SSL-based remote access solution via the SCVPN capability. An SCVPN server supports two-factor authentication, requiring a combination of user name/password and digital certificates (a USB Key certificate and a file certificate).
- **Authentication, Authorization and Accounting (AAA):** Hillstone devices support external authentication of users via RADIUS or LDAP servers.
- **User-based Security Policies:** Firewall rules for allowing or denying traffic can be specified based on specific user IDs or user groups.
- **802.1X Network Access Authentication:** Hillstone devices support 802.1X user/device authentication for a layer 2 bound zone, port, or VLAN using MAC or port access control methods.
- **Two-factor Authentication:** Support for 3rd party solutions, an integrated token server with physical or SMS delivery. SMS is used to send a dynamically generated random password or code to the mobile phone which the user must enter during the login.
- **Virtual System (VSYS):** Independent segmentation of administrators, discussed above.
- **Secure Remote Access:** General user access and authentication methods are discussed in the previous section. Additionally, encryption of user access sessions is necessary as remote access is often done from untrusted Internet locations. SSL (Secure Sockets Layer) is an encryption technology (used by Hillstone devices) that is part of the remote client and encrypts communications between the client and the server. A VPN can also be used to encrypt the remote access communications channel.
- **Endpoint Identification and Control:** Support to identify endpoint IP address, endpoint quantity, on-line time, off-line time, and on-line duration. Control policies and status information are available.

Vulnerability Management Features

Hillstone product features and capabilities in this category, already discussed in earlier sections, include:

- Abnormal Behavior Analysis
- Intrusion Detection and Prevention (IDS/IPS)
- Anti-virus/Malware
- Visibility and Monitoring
- Logs



Hillstone DSS 4 Compliance Summary

The PCI Security Standards Council offers robust and comprehensive standards to enhance payment card data security, specifically the [PCI DSS v4.0 standard](#). Table 2 summarizes the Hillstone product features that can help you implement compliance with the PCI DSS v4.0 standard.

Table 2: PCI DSS v4.0 Control Objectives, Requirements and Solutions

Control Objective	Requirement	Hillstone Solution
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls.	The Hillstone firewall allows you to define access control privileges such as denying access to all applications, users, zones, and content as deemed necessary for all networks that contain cardholder data. Hillstone Networks supports all sub-requirements to DMZ implementations that prohibit direct public access between the CDE system and the Internet.
	2. Apply Secure Configurations to All System Components.	Hillstone Networks security platforms require user authentication and use strong encryption for remote administration and all non-console sessions. This includes direct access and through the Hillstone centralized management system HSM. Two-factor authentication is supported for remote access.
Protect Account Data	3. Protect Stored Account Data.	No cardholder data is stored on the Hillstone firewall. The firewall provides anti-virus, anti malware, IPS, IP reputation checking, access rules, user authentication, web filtering, encryption and session logging to protect access to cardholder data stored on a system behind the firewall.
	4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.	IPSec VPNs are supported for secure site-to-site connectivity. Remote access to individual users is provided via IPSec or SSL-protected connections. Hillstone's user, content, and application identification technology is able to detect and control Chat and Messaging applications to the individual user level.

Control Objective	Requirement	Hillstone Solution
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software.	<p>The Hillstone intelligent firewall includes a network-based antivirus solution that complements existing endpoint solutions.</p> <p>The Hillstone platform includes Machine Learning capabilities that allow for the detection of APT's and Zero Day Malware that bypass traditional signature-based anti-virus programs.</p> <p>Mitigation at the Firewall policy level is also available once detection has occurred.</p> <p>Hillstone's Abnormal Behavior Analysis and Abnormal Protocol Attack detection provide additional levels of security against network, system, and application intrusions.</p>
	6. Develop and Maintain Secure Systems and Software.	<p>The Hillstone firewall allows for the detection and security enforcement of applications in your network.</p> <p>Hillstone WAF helps comply with automated technical solutions that continually detect and prevent web-based attacks for public-facing web applications.</p>
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know.	<p>With granular policy-based control over users, content, and applications —regardless of device or location —companies can implement minimum privileges access control to limit access to cardholder data and use a deny-all policy for everything else.</p> <p>Integration with Active Directory and role based access control enables Hillstone Networks to provide enforcement of assigned privileges to users based on classification and function.</p> <p>Virtual System (VSYS), zoning and network segmentation can be deployed to restrict access to need-to-know users.</p>
	8. Identify Users and Authenticate Access to System Components.	<p>Hillstone ZTNA supports multiple authentication schemes and identity stores. Integration with authentication, authorization, and auditing (AAA) systems via RADIUS, TACACS+, and support for multi-factor authentication (MFA) allows rapid deployment into enterprise networks. User identity and role information stored within enterprise directories (Active Directory, LDAP) can be extracted and used as part of intelligent access policies. For instance, user group information can help determine which subsets of employees should have no network reachability at all into sensitive corporate systems, such as engineering, finance and accounting servers.</p> <p>Hillstone Networks provides integration with Active Directory, AAA and other identity stores offering a wide array of authentication policies, including unique user IDs, revocation and terminating users, and locking out user access after failed logins. Multi-factor authentication, including tokens, is also supported.</p>
	9. Restrict Physical Access to Cardholder Data.	<p>No cardholder data is stored on the Hillstone firewall.</p>
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data.	<p>The Hillstone firewall with HD storage can maintain logs/audit information, including system changes, configurations, traffic flow, alarms, threats, data filtering, URL Filtering, and host information. Bundled with HSM, customized reporting capabilities can be provided. Bundled with HSA can provide deep analysis of NAT traffic with both private and public IP look up. The Hillstone intelligent firewall allows for continuous monitoring of all activity of any particular host and can mitigate any unknown or recognized attack.</p>

Control Objective	Requirement	Hillstone Solution
	<p>11. Test Security of Systems and Networks Regularly.</p>	<p>The Hillstone intelligent firewall inspects allowed sessions for threat identification and prevention. The appliance has a native IPS engine that stops and records intrusion.</p> <p>The stream-based anti-virus engine blocks and prevents unapproved data and file types.</p> <p>The intelligent firewall provides machine learning that identifies, notifies and mitigates unknown malware and APTs and provides on the-fly mitigation and policy control.</p> <p>Policy analysis and invalid policy clean-up tools are supported.</p>
<p>Maintain an Information Security Policy</p>	<p>12. Support Information Security with Organizational Policies and Programs.</p>	<p>Hillstone provides interactive reports and investigative capabilities that accelerate incident investigations and inform incident response across endpoint, network, and cloud environments.</p> <p>iSource XDR helps organizations implement an incident response plan by ingesting alerts from various detection sources that streamline incident response plans.</p>

Conclusion

Hillstone’s comprehensive line of security products provide rich prevention, detection and security incidents investigation features. These features help your organization comply with the PCI DSS v4.0 standards to provide a safer and more secure environment to cardholders and cardholder transactions.

Hillstone

NETWORKS

Visit www.hillstonenet.com to learn more
or contact Hillstone at: inquiry@hillstonenet.com

