# Automate PCI Compliance Monitoring, Investigation & Reporting

**Reducing Business Risk**

Standards and compliance are all about implementing procedures and technologies that reduce business risk and efficiently validate that controls are working according to stated policy expectations and mandated requisites. The question then becomes finding the right technologies that best automate control verification and documentation, as well as those that streamline audit and investigation processes. Compliance considerations for data center management and security management tools should include the means to:

- Validate a broad set of information security policies across infrastructure technologies
- Understand asset and identity relationships and be able to associate objects with compliance and audit requisites
- Produce reports that adapt to existing security, governance and auditing processes and frameworks
- Normalize compliance-relevant data across disparate systems
- Address complex and rapidly changing environments
- Meet auditing and data management standards leveraging out-of-the-box and user customizable controls
- Maintain log management integrity and data retention: data capture consistency, audit records and availability
- Facilitate investigations such as identity access control patterns and violations to accurately track identity, location and action
- Reduce control gaps and incident response lag time (MTTR)
- Diminish compliance liabilities and audit duration

AccelOps satisfies these compliance considerations with built-in dashboards, analytics and reports mapped to leading standards and compliance best practices, such as PCI-DSS.

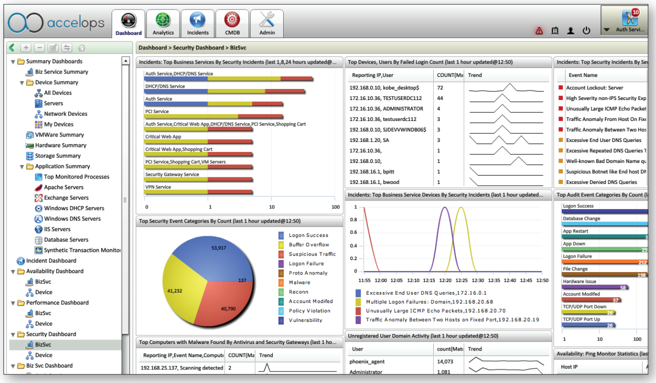
**Payment Card Industry Data Security Standards**

PCI DSS (Payment Card Industry Data Security Standards), created by the Payment Card Industry, was designed to reduce cardholder data security issues and facilitate consistent global data protection standards and merchant assessment among payment card processing vendors. PCI applies to any network, server or application that is included in or connected to the cardholder data environment where cardholder data is stored, processed, or transmitted. Applicable merchants and service providers must manage and monitor compliance including that of all associated third parties with access to cardholder data. The PCI standard, outlining requirements and adherence testing, employs common security best practices to safeguard sensitive cardholder identity and transaction data.
*AccelOps' solution supports adhering to the majority of requirements within the current PCI-DSS standard:*

- Monitor configuration changes to maintain appropriate firewall configuration protecting cardholder data
- Monitoring system controls such as password management to negate using vendor-supplied defaults for system passwords
- Monitor the protection of cardholder data storage such as personal identifiable information and respective financial transactions
- Monitor processes that support encrypted transmission of cardholder data across open public networks
- Monitor, track and respond to malware activity supporting use and regular updating of anti-virus / anti-malware software
- Monitor controls regarding the develop and maintenance of secure systems and applications
- Monitor, alert and store log records regarding access to cardholder data by business need-to-know
- Track directory changes and infrastructure access using unique ID to each person with computer access
- Monitor physical access to cardholder data and alert on restriction/ access policy violations
- Monitor all access to network resources and cardholder data and document segregated access to payment processing resources
- Regularly test security systems and processes by way of control monitoring
- Verify monitoring of security controls for employees and contractors regarding network and application access

**AccelOps, Automating PCI Compliance Processes**

AccelOps delivers management and IT staff timely reporting, extensive monitoring and robust controls that can be easily and consistently applied across an infrastructure and dovetail within an organization's existing security, governance and audit processes.




AccelOps provides a single pane of glass for network operation and security operation teams to support compliance mandates while providing end-to-end visibility across performance, availability, security and change management.

The integrated and service-oriented data center management platform centralizes the collection, monitoring, analysis and detailed reporting on all performance and IT/event log data cutting through networks, systems, applications, virtualization and technology boundaries.

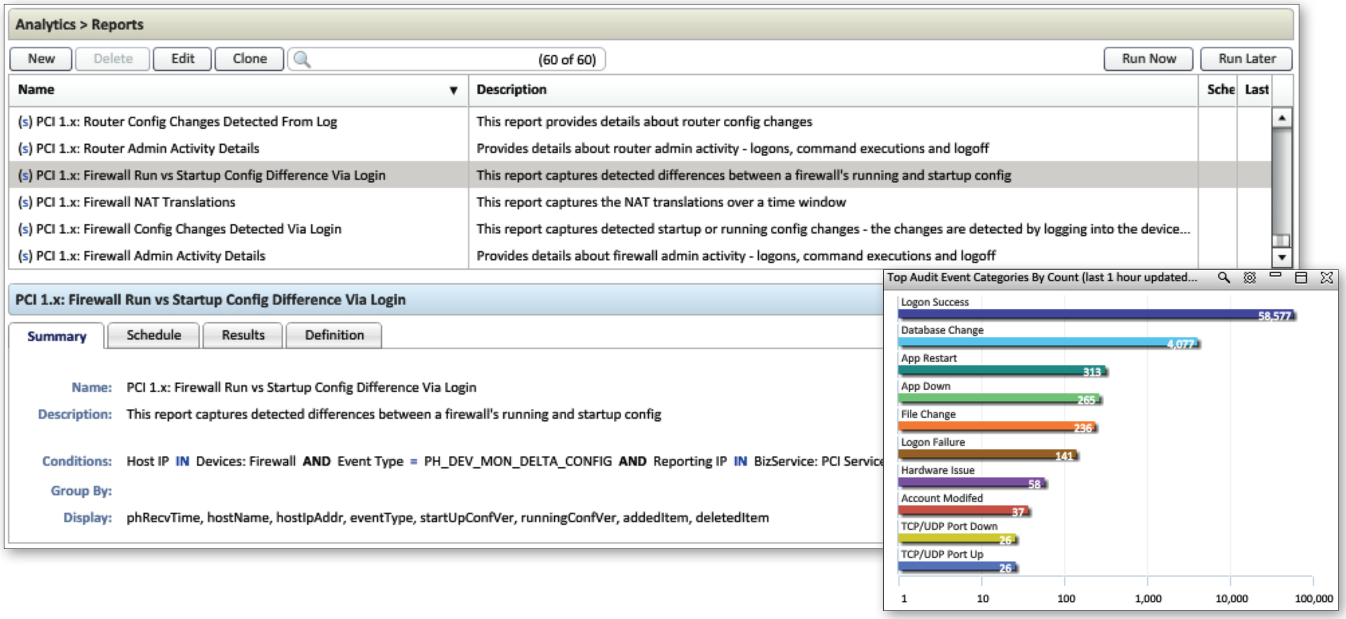
AccelOps puts the "who, what, why, where, how and when" details at the operator's fingertips and enables security/GRC staff to preempt threats and efficiently respond to PCI compliance violations.

2905 Stender Way, Suite 48
Santa Clara, CA 95054, USA
PHONE +1.408.490.0903
FAX +1.408.970.9666
www.accelops.net

# Automate PCI Compliance Monitoring, Investigation & Reporting

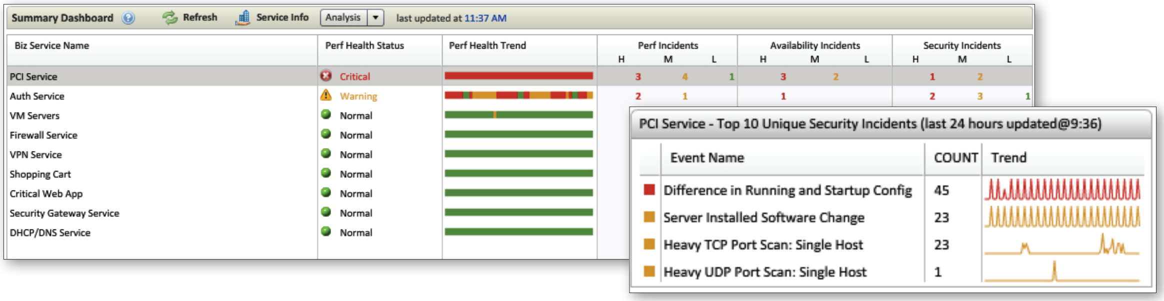
**AccelOps PCI-DSS Monitoring and Auditing Advantages**

Beyond comprehensive security information event management (SIEM) and log management functionality, AccelOps provides broad verification of controls, efficient root-cause analysis, streamlined investigation and PCI-DSS reporting. The solution ships with built-in/ customizable compliance-relevant dashboards, rules and reports leveraging advanced discovery, log normalization and consolidation, cross-correlation, configuration monitoring, pattern profiling, identity access monitoring and object-based compliance grouping.




**Industry-leading Features**

- Fully extensible **compliance management dashboard** with built-in rules, reports and widgets mapped to PCI/compliance standards
- **Auto-populating CMDB** (Configuration Management Database) with versioning and alerting to identify config. change violations
- Interactive Layer-2/3 topology mapping to **instantly document PCI segregated environment** and visually assess incidents
- Auto-discovery and in-depth config. monitoring of **DMZ, NAT, Wireless AP**, as well as hardware, VM, server, and application
- Track and report successful and failed logins, authentication, and location with **network behavior and user behavior profiling**
- Identity Access Management binding IP address to machine, login, user association and event — **capturing TRUE identity behind shared credentials, resource access and activity.**
- **Monitor suspicious activity** ie. terminated or service account use
- **Monitor and document PCI-critical event logs:** vulnerability scanner, application firewall, DLP and MTA encryption activity
- **Filter IDS false positives** with automated patch exception mgmt.
- **Track physical and logical access** and monitor/alert on violations to cardholder data: **user, location and rogue user network access**
- Monitor the performance, availability and security of payment processing systems to **quickly negate non-PCI/security issues**
- Smart network/system behavior rules **pinpoint botnet attacks**
- **Advanced rule engine** and GUI to track & alert **for any scenario**
- **IT business service mapping** for issue prioritization, impact analysis and collaboration as analytics are applied to logical group
- **Expedite incident response** with **alert drill-through** for incident details, object status and config., identity and **trouble-ticketing**
- **Enterprise search** of all real-time and historic raw, normalized and incident details supporting fast keyword and structured search
- **Satisfies secure, long-term data retention requirements**
- **Centralize all event / log management with scale-out architecture for virtually unlimited performance and online data management capacity** — all operation data is readily available with means to expand processing and storage on demand



# AccelOps' PCI-DSS Compliance Support

| 1 | Install and maintain a Firewall configuration to protect cardholder data | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 1.1.1 | Approve/Test external network connections and changes to Firewall and Router configurations. | AccelOps can detect, track and trend Firewall and Router configuration changes.<br>*Report Example:* Firewall Run vs Startup Config Difference<br>*Rule Example:* Firewall Run vs Startup Config Difference |
| 1.1.2 | Maintain a current network diagram depicting connections to cardholder data. | AccelOps' layer 2 and layer 3 topology mapping can illustrate a current PCI-relevant network diagram.<br>*Example:* PCI-Business Service topology map depicting a PCIrelevant connections |
| 1.1.3 | Confirm DMZ Firewall by proving proof of Firewall use at each connection between DMZ and internal network. | AccelOps' layer 2 and layer 3 topology mapping can illustrate a current PCI-relevant network diagram. Users can also drillthrough to obtain Firewall configuration detail.<br>*Example:* Firewall topology map depicting DMZ |
| 1.1.5 | Manage Firewall services: document Firewallprotocols and ports, and justify said use. | AccelOps can monitor and display Firewall configurations and detect/pinpoint configuration changes. |
| 1.1.6 | Review Firewall and router configurations at leastevery 6 months | AcceelOps can detect, version and compare Firewall and Router configurations and changes.<br>*Report Example:* Firewall config changes detected via login |
| 1.2.1 | Firewall should deny traffic from "untrusted networks/hosts" | AccelOps reports can illustrate Firewall traffic rules denying access to cardholder data processing systems.<br>*Report Example:* Top blocked sources, ports |
| 1.2.2 | Secure and sync router configuration. | AccelOps can monitor, alert and track router configuration changes.<br>*Report Example:* Router config changes detected via login |
| 1.2.3 | Firewall configuration should isolate access to cardholder data from public and wireless connections. | AccelOps can display wireless access points connecting through a network Firewall or proxy.<br>*Example:* Topology map of PCI-relevant infrastructure<br>*Report Example:* Wireless logon failure details |
| 1.3.1 | Implement a DMZ limiting inbound and outbound traffic only to necessary protocols | AccelOps' layer 2 and layer 3 topology mapping can illustrate a current PCI-relevant network diagram. AccelOps can provide Firewall configuration rules.<br>*Example:* Topology map of DMZ |
| 1.3.2 | Restrict inbound internet traffic to IP addresses within DMZ | AccelOps can monitor and report on denied inbound traffic.<br>*Report Example:* Top Firewalls by inbound denies |
| 1.3.3 | Prohibit inbound or outbound direct routes for public access to cardholder data | AccelOps can provide rules and reports that identify blocked traffic due violations captured by the Firewall or proxy.<br>*Report Example:* Top blocked internal sources, services and destinations |
| 1.3.4 | Prohibit internal addresses from passing from the Internet into the DMZ | AccelOps can provide rules and reports that identify blocked traffic due attempts to pass internal address into the DMZ.<br>*Report Example:* Top blocked internal sources, services and destinations |
| 1.3.5 | Prohibit direct routes from cardholder data processing systems to external IP addresses | AccelOps can provide rules and reports that identify blocked traffic due attempts to pass internal address into the DMZ.<br>*Report Example:* Top blocked internal sources, services and destinations |
| 1.3.7 | Cardholder processing database and respective systems should be segregated from the Internet | AccelOps' layer 2 and layer 3 topology mapping can illustrate a current network diagram including the segregation of PCIrelevant resources. |
| 1.3.8 | Prevent internal addresses from being revealed on the Internet | AccelOps topology, CMDB and reporting features identify and monitor NAT/PAT implementation details / config. changes.<br>*Report Example:* Firewall NAT translations |

## AccelOps' PCI-DSS Compliance Support

| 2 | Do not use vendor-supplied defaults for system passwords and other security parameters | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 2.1 | Don't use vendor supplied defaults for passwords and other configurations | AccelOps can monitor change information from Active Directory regarding password policy, as well as password changes on systems.<br>*Report Example:* Server password changes |
| 2.1.1 | Change wireless access point default passwords and service settings | AccelOps topology and CMDB features can identify and monitor wireless AP implementation details / config. changes.<br>*Report Example:* WLAN Config changes |
| 2.2.0 | Develop configuration standards for all systems | AccelOps CMBD configuration versioning feature monitors for changes to initial standard settings of systems.<br>*Report Example:* Windows server config modification details |
| 2.2.1 | Implement one primary function per server (or virtual server) | AccelOps CMBD configuration versioning feature monitors for changes to initial standard settings of systems. AccelOps VM dashboard can display VM to guest OS relationship. |
| 2.2.2 | Disable all unnecessary services and protocols | AccelOps CMBD configuration versioning feature can monitor for changes, as well as port activity.<br>*Report Example:* DNS Ports Up/Down |
| 2.2.3 | Configure system security parameters | AccelOps CMBD configuration versioning feature monitors for changes to initial standard settings of systems and security devices.<br>*Report Example:* Windows Audit Policy Changed |
| 2.3 | Encrypt all non-console administrative access | AccelOps can monitor administrative access to systems and accounts, as well as use of non-encrypted protocols.<br>*Report Example:* Non-encrypted protocol resource access |

| 3 | Protect stored cardholder data | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 3.6.7 | Prevent the unauthorized substitution of cryptographic keys | AccelOps can monitor directory or file actions such as writes and potential changes to stored cryptographic keys.<br>*Report Example:* Windows server file modification details |

| 4 | Encrypt transmission of cardholder data across open, public networks | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 4.1 | Encrypt transmission of cardholder data across open, public networks | AccelOps can detect and report the use of non-encrypted protocols communicated to and from PCI-relevant devices.<br>*Report Example:* Non-encrypted protocol use |

| 5 | Use and regularly update anti-virus software or programs | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 5.1 | Deploy and demonstrate anti-virus software on all systems affected by malware | AccelOps monitors and reports on anti-virus solution activity<br>*Report Example:* Total viruses found and remediated by Host antivirus |
| 5.2 | Maintain anti-virus software | AccelOps monitors and reports on leading anti-virus solution patch/update activity<br>*Report Example:* Top IPs with Malware found by Antivirus and Security Gateways |

# AccelOps' PCI-DSS Compliance Support

| 6 | Develop and maintain secure systems and applications | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 6.1 | Verify deployment of current patches | AccelOps monitors and displays patch activity. |
| 6.2 | Identify newly discovered vulnerabilities | AccelOps monitors leading vulnerability management scanner activity and vulnerability notifications<br>*Report Example:* Host vulnerabilities discovered |
| 6.3.2 | Separate development and production environments | AccelOps can display a topology map verifying implementation of network segregation. The system can also monitor activities such as system access between development and production environments to alert and track potential violations. |
| 6.5.1 | Develop secure web applications | AccelOps can monitor for suspicious network and system activity of web applications, and monitor for web security violations as detected by intrusion detection systems and application firewalls.<br>*Report Example:* Host vulnerabilities discovered<br>*Rule Example:* Excessive HTTP client side errors |
| 6.6.1 | Ensure web-facing applications are protected against known attacks. | AccelOps can monitor for suspicious network and system activity of web applications and can monitor for security violations and activity of application firewalls.<br>*Report Example:* Total denied web connections by policy |

| 7 | Restrict access to cardholder data by business need to know | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 7.1.4 | Restrict access to cardholder resources and data | AccelOps can monitor and maintain history, including actual identity regardless of shared credential use, of access to cardholder data processing systems and applications.<br>*Report Example:* Detailed failed login at PCI system |
| 7.2.1 | Ensure access to systems are based on role and that controls are in place | AccelOps can monitor and maintain history, including actual identity regardless of shared credential use, of access to network resources. AccelOps' rules can be implemented to alert on resource access violations based on directory or custom groups. |

| 8 | Assign a unique ID to each person with computer access | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 8.1 | Assign a unique ID to each person with computer access to enable access and use tracking | AccelOps can monitor and maintain history, including actual identity regardless of shared credential use, of access to network resources. |
| 8.2 | Ensure authenticated access to resources | AccelOps can monitor and maintain history, including actual identity regardless of shared credential use, of access to network resources including authentication method. The system can also alert on rogue (not identified in directory services) user or system network access.<br>*Report Example:* Unregistered user domain activity |
| 8.3 | Ensure remote, 2-factor authenticated access to resources | AccelOps can monitor remote access to network resources including authentication method.<br>*Report Example:* Remote desktop connections to Windows servers |
| 8.5.1 | Ensure appropriate authentication and password management | AccelOps can monitor directory service administrative changes and access to network resources.<br>*Report Example:* Global Windows Groups Created, Deleted, Modified |
| 8.5.2 | Revoke access of terminated users | AccelOps can monitor directory service administrative changes and access to network resources, including those accessing resources using terminated account credentials<br>*Report Example:* Users deleted from global groups<br>*Rule Example:* Terminated credential use |
| 8.5.5 | Remove inactive user accounts | AccelOps can monitor directory service administrative changes and access to network resources, including those accessing resources using terminated account credentials<br>*Report Example:* Global Windows Groups Created, Deleted, Modified |

# AccelOps' PCI-DSS Compliance Support

| | | |
|---|---|---|
| 8.5.6 | Monitor vendor and service account access | AccelOps can monitor and maintain history, including actual identity regardless of shared credential use, of access to network resources including authentication method. Custom rules can monitor and maintain history of vendor access and service account access.<br>*Report Example:* Detailed successful login at PCI device |
| 8.5.8 | Do not use shared or generic accounts | AccelOps can monitor and maintain history, including actual identity regardless of shared credential use, of access to network resources including authentication method. The system can indicate the actual user behind shared credentials. |
| 8.5.9 | Change user passwords every 90 days | AccelOps can monitor logs files of systems for password change requests and changes.<br>*Report Example:* Server password changes |
| 8.5.13 | Verify unsuccessful logins and lockout provisions | AccelOps can monitor logs files of systems for failed login attempts and lockout messages.<br>*Report Example:* Windows server account lock/unlock history<br>*Rule Example:* Domain account lockout |
| 8.5.16 | Verify authenticated access to database systems containing cardholder data | AccelOps can monitor log files and alerts regarding database access, and database security system logs and notifications.<br>*Report Example:* Failed database service logon details<br>*Rule Example:* Multiple Logon Failures: Database |

| 10 | Track and monitor all access to network resources and cardholder data | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 10.1 | Verify that audit trails are enabled and active | AccelOps provides reports on those systems being monitored including event capture type, start and anomalies.<br>*Report Example:* Event / Log monitoring |
| 10.2.1 | Implement automated access trails for system components in regards to cardholder data and data processing | AccelOps can monitor and maintain history, including actual identity regardless of shared credential use, of access to systems that are PCI-relevant. AccelOps also monitors administrative changes to directory services.<br>*Report Example:* Detailed successful login at PCI device |
| 10.2.2 | Access actions taken by administrators with privileged system access | AccelOps can monitor and maintain history, including actual identity regardless of shared credential use, of administrative access to systems and respective system config. changes.<br>*Report Example:* Privileged Windows Server Logon Attempts using the Administrator Account |
| 10.2.4 | Monitor invalid access to network resources | AccelOps can monitor and maintain history, including actual identity regardless of shared credential use, of failed access attempts to network resources.<br>*Report Example:* Detailed failed login at PCI system<br>*Rule Exmple:* Suspicious logon failure followed by successful login |
| 10.2.6 | Monitor initialization and failure of logs | AccelOps provides reports on those systems being monitored including event capture type, start and anomalies.<br>*Report Example:* Event / Log monitoring |
| 10.2.7 | Record audit trail attributes | AccelOps captures, maintains and normalizes audit trail attributes.<br>*Report Example:* Detailed failed login at PCI system |
| 10.5.1 | Follow log management best practices | AccelOps follows log management best practices including restricted administrative access to AccelOps system activity logs as well as the ability to provide long-term, online data retention of raw, normalized and incident event log data. |
| 10.6 | Regularly review logs of security functions | AccelOps consolidates, filters and automates the process of reviewing logs and responding to incidents among key security functions such as Firewall, IDS, AAA, etc. |
| 10.7 | Establish Audit Trail Data Retention | AccelOps hybrid flat file and embedded RDBMS data management system allows for efficient and virtually unlimited log data storage with online availability. |

# AccelOps' PCI-DSS Compliance Support

| 11 | Regularly test security systems and processes | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 11.2 | Run vulnerability scans regularly | AccelOps can monitor and record vulnerability scan execution and resulting vulnerability notification.<br>*Report Example:* Detect heavy TCP/UDP host scan on fixed port |
| 11.4 | Employ Intrusion Prevention Systems (IPS) | AccelOps can monitor, alert and report on intrusion detection activity and can automatically filter IPS alerts based on false positives due to attacks on patched or invalid systems.<br>*Report example:* Non-compliance hosts and security software<br>*Rule example:* High severity ISP exploit |
| 11.5 | Employ file integrity monitoring | AccelOps can monitor directory and file changes, system security generated logs, as well as audit data from 3rd party file integrity systems.<br>*Report Example:* Windows server file modification details |

| 12 | Maintain and Information Security Policy | |
|---|---|---|
| | Compliance Requisite | How AccelOps Facilitates Compliance |
| 12.3.2 | Verify usage policies for system resources are authenticated | AccelOps can monitor user access and respective authentication to network resources. |
| 12.3.6 | Verify acceptable network locations for approved technologies | Accelops can monitor and report the location of specified PCI-relevant systems and applications.<br>*Rule Example:* Administrative login from an unauthorized IP |
| 12.3.7 | Develop usage policies for company-approved products | AccelOps CMDB functionality can display installed and running applications. |
| 12.3.9 | Verify the use of remote access devices by vendors in regards to session activation and deactivation | AccelOps can monitor the access to PCI-relevant systems by user or user group as well as record the authentication method. |
| 12.5.2 | Verify the monitoring and analysis of security incidents and information and the means to distribute to appropriate personnel | AccelOps fully monitors and reports on security and PCIrelevant incidents, including configuration changes, access violations, suspicious activity and reported breaches, with the means to create, assign and tra ck the status of trouble tickets.<br>*Report example:* Top business service by security incidents<br>*Report example:* Top security incidents by severity |
| 12.9 | Implement an incident response plan and the means to respond immediately to a system breach. | AccelOps provides an integrated and centralized security information event management to enable efficient real-time and historic event monitoring, correlation, alerting, reporting and investigation of security incidents, suspicious activity, identity access control violations and system breaches. |

**Automate Compliance Controls and Audit Processes**

For more information regarding AccelOps' mapping to PCI mandates and how we can help automate your PCI-DSS compliance monitoring, auditing and reporting processes, please visit www.accelops.net, email sales@accelops.net or call 408.490.0903.