



Identity Aware Networking Solutions For PCI DSS Compliance

Solution Brief

Document Version 1.0

www.appliedidentity.com

Identity Aware Network Solutions for PCI DSS Compliance

Overview

The PCI Data Security Standard (PCI DSS) was first announced in 2005 as a jointly developed data security standard for the payment card industry in response to the growing costs associated to credit card fraud through data compromise. American Express, Discover, JCB, MasterCard Worldwide and Visa International provided the guidelines to help organizations process card payments to prevent credit card fraud, hacking and various other security issues.

Compliance-ready networks typically require securing stored data, controlling access to data, ensuring availability of data and applications, and monitoring network events. The PCI DSS uses the following control objectives to define the 12 high-level security requirements and can be broken down into the following sections:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

In the latest iteration of the standard (PCI DSS version 1.1), the twelve broad sections of compliance have been broken down for further clarification into 64 primary controls and 143 control enhancements – bringing the total to 207 requirements. These security requirements apply to all system components which are defined as any network component, server, or application that is included in or connected to the cardholder data environment.

Who Must Comply?

Even though PCI DSS is a U.S. standard, it has become a global requirement for all entities handling cardholder data. A company processing, storing, or transmitting credit card numbers must be PCI DSS compliant or they risk losing the ability to process credit card payments. These companies are broken down into two distinct categories;

Merchants are authorized acceptors of cards for the payment of goods and services.

Service Providers are organizations that process, store, or transmit cardholder data on behalf of card members, merchants, or other service providers.

Merchants and Service Providers are typically classified at different levels based on the number of annual transactions processed – although this can differ depending on the credit card issuer. In general, Level 1 Merchants and Level 1 & 2 Service Providers submit the greatest number of transactions and therefore must validate compliance with an audit by a PCI DSS Qualified Security Assessor (QSA) Company. Level 2, 3, & 4 Merchants and Level 3 Service Providers must complete an annual self-assessment questionnaire and quarterly network scans to prove compliance.

MERCHANT LEVELS

Level 1

- Any merchant from whom cardholder data has been compromised
- Merchants with more than 6 million credit card transactions annually
- Annual onsite PCI data security assessment and quarterly network scans

Level 2

- Merchants with between 1 and 6 million credit card transactions annually
- Annual self-assessment and quarterly network scans

Level 3

- Merchants with between 20,000 and 1million credit card e-commerce transactions annually
- Annual self-assessment and quarterly network scans

Level 4

- All other merchants
- Annual self-assessment and annual network scans

SERVICE PROVIDER LEVELS

Level 1

- All payment gateways and processors
- Annual onsite PCI Data Security assessment and quarterly network scans

Level 2

- Any service provider that is not in Level 1 and stores, processes, or transmits more than 1 million credit card accounts/transactions annually
- Annual onsite PCI Data Security assessment and quarterly network scans

Level 3

- Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 credit card accounts/transactions annually
- Annual self-assessment questionnaire and quarterly network scans

The Penalties for Non-Compliance

Due to the financial impact of credit card fraud and the additional cost of card re-issuance, credit card companies are starting to impose fines on non-compliant entities. In 2005 for example, Visa levied fines of \$3.4 million, with an increase to \$4.6 million in 2007. Finally, after the failures of HIPPA and other compliance mandates to improve data security, PCI compliance is beginning to bear its teeth.

Fines are being levied between \$5,000 and \$25,000 for each month Level 1 & 2 merchants who have not met the deadlines of September 30, 2007 and December 31, 2007 respectively. For prohibited data storage, failing to provide confirmation that Level 1 & 2 merchants are not storing full track data, CVV2 or PIN data by March 31, 2007 are eligible for fines up to \$10,000 a month per merchant, subject to escalation in the event material progress toward compliance is not made in a timely manner.

Fines can also be as much as \$500,000 per incident if credit card data is compromised and merchants are found to be non-compliant with the PCI DSS standard. In addition - in the event of a breach and data compromise;

- Level 2, 3 & 4 Merchants and Level 3 Service Providers are automatically given a Level 1 classification and must undergo the annual onsite PCI data security assessment by a QSA and quarterly network scans.
- The cost to fully comply with the QSA audit can be a considerable inconvenience and additional cost – especially for smaller merchants and service providers.
- Remediation costs are estimated at \$90 to \$302 per record.
- Potential customer lawsuits
- Company reputation and brand damage

What solutions does Applied Identity provide to help meet PCI requirements?

Through auditing, monitoring, reporting and network level enforcement based on User Identity, Applied Identity can help you address multiple sections in the 12 PCI requirements. Applied Identity's solutions help organizations meet PCI DSS compliance requirements in the following sections;

Requirement	Requirement Description	Solution Capability
Section 1	Build and Maintain a Secure Network	
1.1.4	Description of groups, roles, and responsibilities for logical management of network components	Applied Identity's ID-Enforce™ solution allows logical grouping of users and groups based on their roles and responsibilities defined within the identity repository (such as Active Directory (AD) to access PCI defined resources and applications.
1.1.5	Documented list of services and ports necessary for business	Applied Identity's ID-Audit™ solution can monitor and report on all user, service and port access to critical PCI assets necessary for business enablement.
1.1.6	Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)	Applied Identity's ID-Enforce solution can identify, track, and enforce network level access policies for exception services and protocols and documented via ID-Audit's reporting capability

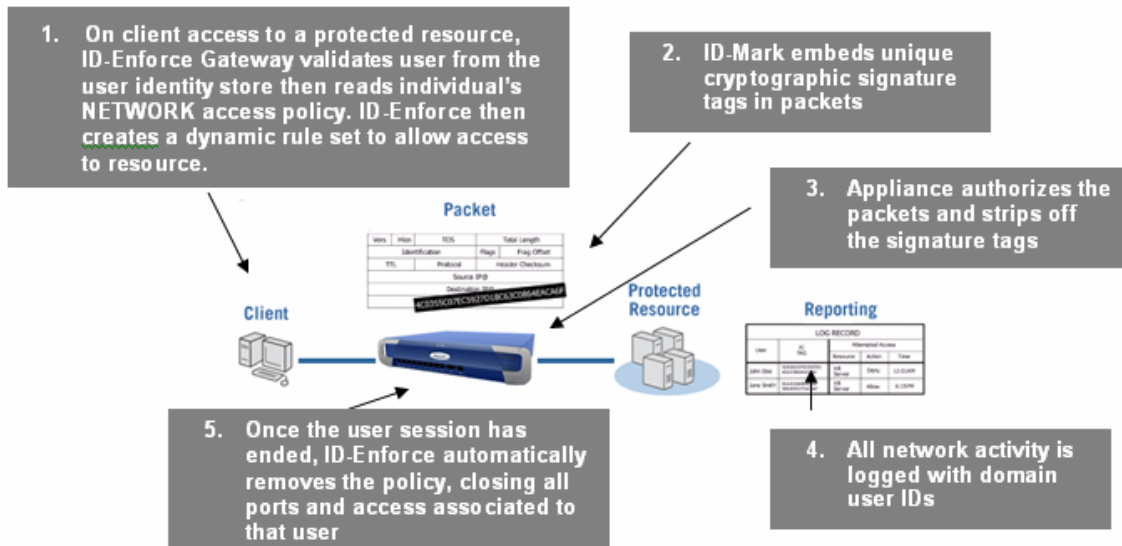
Requirement	Requirement Description	Solution Capability
Section 1		
Build and Maintain a Secure Network		
1.2	Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.	Applied Identity's ID-Enforce solution can enforce access based on user identity and the service/protocols necessary for business to a predefined group of PCI resources and applications, denying all other traffic.
1.3	Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.	ID-Enforce will support user based policy independent of the underlying network topology so that it will implement identity based controls between remote VPN connections and the corporate backbone, between wireless and wired network segments. ID-Enforce can also segment a network virtually - based on identity - when there is no physically separate TCP/IP network segment.
1.3.5	Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment	ID-Enforce can restrict communications to specific IP addresses, ports and applications, completely cloaking resources if denied by policy. In addition, access to PCI resources will be granted only if the ID-Mark client driver is installed on the client.
1.3.7	Denying all other inbound and outbound traffic not specifically allowed	ID-Enforce can restrict communications to specific IP addresses, ports and applications, completely cloaking resources if denied by policy. In addition, access to PCI resources will be granted only if the ID-Mark client driver is installed on the client.
1.4	Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).	ID-Enforce supports bi-directional control of user access to and from the trusted network, based on who the user is, and whether or not they have privileges to use a specific PCI resource.
1.4.2	Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	ID-Enforce can restrict communications to specific IP addresses, ports and applications, completely cloaking resources if denied by policy. In addition, access to PCI resources will be granted only if the ID-Mark client driver is installed on the client.
Section 7		
Implement Strong Access Control Measures		
7.1	Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	ID-Enforce can establish role-based access control by leveraging the user identity in the identity repository to deny access to all but those in a "PCI" role. ID-Enforce integrates policy management with existing LDAP identity management systems such as Microsoft Active Directory, Oracle ID, Sun Java Directory, Novell eDirectory and other LDAP v3 compliant systems.
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.	Before any user session is allowed to pass through an ID-Enforce Gateway, that user must first authenticate based on an existing domain identity. All resources to which the user's policy does not specifically state they have the privilege to use are cloaked from the user.

Requirement	Requirement Description	Solution Capability
Section 8		
Support a unique ID for each computer user.		
8.1	Identify all users with a unique username before allowing them to access system components or cardholder data	ID-Enforce requires authentication before a user is allowed to pass but fully supports the authentication of the directory with which its policy is integrated so that users are not required to login incrementally to the ID-Enforce appliance
8.2	<p>In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> • Password • Token devices (e.g., SecureID, certificates, or public key) • Biometrics 	<p>RSA SecurID and Applied Identity's ID-Enforce together provide organizations with a synergistic identity-based pathway from authentication to network resource access control and tracking of individual user behavior on the network.</p> <p>The RSA SecurID user login is seamlessly embedded within the Applied Identity ID-Mark client driver and provides the user with a consistent experience. ID-Enforce is notified when a user has "passed" SecurID authentication so that it can begin enforcing the up-to-date access policies applicable to that individual - essentially extending the SecurID-validated identity to the network, application, and data access layers.</p>
8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components	ID-Enforce can leverage the existing identity infrastructure already in place without replicating or modifying the identity in any way. Directory identities and the associated authentication and password management are fully supported as part of the ID-Enforce access policy.
8.5.4	Immediately revoke access for any terminated users	As ID-Enforce leverages the existing identity infrastructure, any accounts that are deleted or disabled within the directory will automatically revoke the network level access rights to deny permission through the gateway to the protected PCI resources.
Section 10		
Track and monitor all access to network resources and cardholder data		
10.2.1	Implement automated audit trails to reconstruct [individual user access to cardholder data] events	At the network level, every time a user attempts to open a session to a resource on the trusted side of ID-Enforce the event is recorded in detail, whether allowed or denied. These events can be viewed from ID-Audit and can also be automatically streamed to external log management or compliance monitoring systems via syslog and WELF format protocols.
10.3 – 10.3.6	Record at least the following audit trail entries for all system components for each event: User identification, Type of event, Date and time, Success or failure indication, Origination of event, System component, or resource.	ID-Enforce retains detailed, identity based log information that records User identification, Type of event, Date and time, Success or failure indication, Origination of event, System component, or resource. Each log entry is self contained, including user identity, resource identity and all of the other required parameters so that no post-event correlation is required to establish this information from IP addresses or other data collected on other systems.
10.7	Retain audit trail history for at least one year, with a minimum of three months online availability.	ID-Audit retains recent data within its database and supports archiving to outside database schemes for longer-term retention.

IDENTISPHERE Solution Overview

Applied Identity's Identisphere™ line of identity aware security solutions are purpose-built platforms and can be deployed within the internal network to protect critical resources from unauthorized access. Designed to satisfy demanding small to medium networks and enterprise environments alike, the Identisphere Manager™ provides centralized user identity and role-based policy administration with integrated auditing and reporting across all the ID-Enforce™ devices deployed in the enterprise.

How Identity Aware Enforcement Works

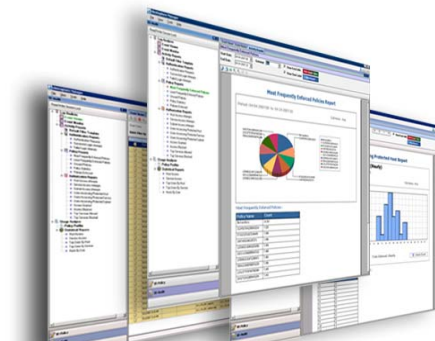


ID-Audit

PCI Section 1.15, 1.16, 10.2.1, 10.3-10.3.6, 10.7

ID-Audit™ is a component of Identisphere Manager effectively replacing the manual correlation of IP address to UserID log data, which is a time and resource intensive requirement for audit reporting. ID-Audit has the ability to audit user behavior & resource usage, which in turn is used to help define access policy and redefines the existing policy implied by other security controls already embedded within the network (such as firewalls, VLAN's and ACL's). This approach provides a much more manageable and granular centralized policy for network level enforcement.

ID-Audit can create real-time views of user access to critical resources and historical reports which can be filtered to provide succinct detail for policy creation and to meet internal and external audit report requirements.



ID-Audit provides over 50 pre-defined reports for both internal and external review

Auditing Network and Resource Access by User Identity

An integral component of Identisphere manager, ID-Audit™ provides IT departments with a powerful window into their network displaying both real-time and historical user and resource activity. ID-Audit allows network and security administrators to visualize a baseline of events that can not only be reported on and used to satisfy internal and external audit requirements, but also acted on to create effective, granular access policies to restrict user access to PCI assets at the network level.

In addition to the improved visibility and the enhanced security provided by identity aware networking solutions, ID-Audit reduces the time and cost associated with audit driven processes, improved accuracy in reporting, and the normalization of information used to define global access policies.

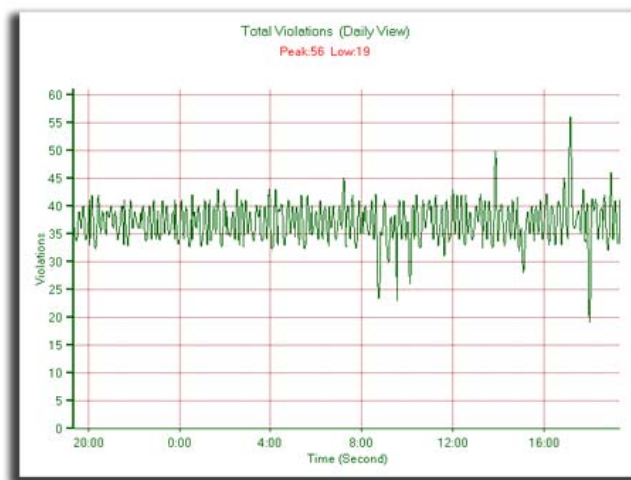
ID-Audit Components and Features

The main features of ID-Audit are the Event Viewer and Event Monitor for viewing both real-time and historical events to create Authentication Reports, Policy Reports, Authorization Reports, and Bandwidth Reports, in addition to the Usage Analyzer that provides the Policy Profiler and Statistical Reports from all of the collected data.

Event Management

Event Viewer: Event Viewer provides both real-time and historical views of collected data generated by the ID-Enforce gateways. Events can be filtered to provide a very granular view of specific events based on a number of different criteria including user name, IP address, service, port, protocol etc.

Event Monitor: Event Monitor generates real-time charts and graphs with tabular detail based on either a daily or weekly summary format. Specific time periods can be selected from the calendar menu to generate historical views beyond the current day or week. These views are predefined and provide a “Top 10” summary of events based on violations, user, resource, service, and networking activity. Filters can be applied to the data set allowing an administrator to drill down further to return the exact information required to troubleshoot issues or view specific events.



Event Monitor has the ability to replay filtered events to highlight the most important and critical information

Event Reporting

PCI Sections 10.2, 10.2.1, 10.3-10.3.6

The following reports allow both network and security administrators to visualize and report on events that may impact the business and operational aspect of the network.

Report Types



Authentication Reports

Authentication reports display the type of authentication used - such as single factor multifactor or Web client, and successful and unsuccessful login attempts.



Policy Reports

Policy reporting allows you to identify the most frequently enforced policies and the least frequently used ones. Policy violations can be identified by source IP, user, and group, and unused policies - policies which can be removed without impacting the user community.



Authorization

The authorization reports section provides 20 predefined templates providing granular detail on host, service, and subnet access attempts - whether granted or denied - and as application and user access attempts.



Bandwidth Reports

Bandwidth reports provide information on access frequency by user and group, the most used and least used protocols, applications, and services. This can benefit capacity planning, load-balancing, and application service separation to further enhance security and application response. Reports can be generated based on the users and groups accessing a specific resource, and the protocols and services utilized.



Statistical Reports

Derived from the user behavior logs, these reports provide insight over long periods of time into how users, hosts, services and subnets interact with your critical resources to help spot trends and enable the prediction of situations leading to network outage.

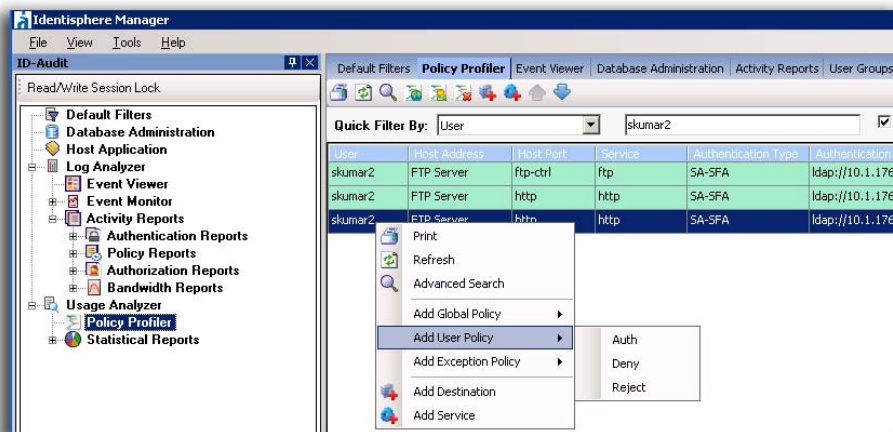
Access Policy Creation

PCI Sections 1.2, 1.3, 1.3.5, 1.3.7, 1.4, 1.4.2, 7.1

Usage Analyzer: ID-Audit is the module in Identisphere responsible for collecting and reporting on the user's, resources, and helps to provide a baseline for the creation and implementation of policy. By passively monitoring the services and protocols used, ID-Audit can quickly build a profile of the protected resources and the services, applications and protocols used - without the need for an active network assessment.

Policy Profiler: Providing a consolidated view of users accessing specific networked resources, administrators can instantly apply a simple "one click" policy template with values extracted from an audited event to either allow or deny network-level access. Global, user, or

exception policies can be applied to the destination resource, the service being utilized, specific users or group of users at the click of a button.



ID-Audit provides “one-click” policy creation from auditable user and resource events

Event Data Storage and Administration

PCI Sections 10.2, 10.3-10.3.6

Zero Administration Database

The large amounts of event data collected does not require the attention of a full-time DBA resource as ID-Audit provides built in utilities to help optimize and manage the database, easing the burden of administration.

Syslog Import

In addition to the industry-standard WELF format, ID-Audit can directly import the Syslog files created by any ID-Enforce Gateway and generate reports from the Syslog data. This may be useful for consolidating reports from remote offices or locations not having a reporting tool of their own.

ID-Enforce

PCI Sections 1.14, 1.2, 1.3, 1.3.5, 1.3.7, 1.4, 1.4.2, 7.1, 7.2

Applied Identity’s ID-Enforce is an identity access gateway solution using firewall-like technology to cost effectively manage the risk associated with inappropriate access to critical PCI resources. ID-Enforce ties access policies with user network identity (via LDAP integration), and network resources, for authorization and audit of network activities. Access policies are created based upon role, group and individual identity, simplifying policy creation and management while ensuring consistent enforcement. ID-Enforce sits inline, close to the resources it protects which ensures that all users must pass through it in order to access data and applications. This approach is significantly more cost effective and easier to manage than solutions architected for distributed enforcement within the network. PCI DSS is the first compliance regulation requiring a unique user identity to audit and control access to PCI resources, which will drive the significance of user identity in future compliance regulations outside of PCI.

ID-Enforce will allow organizations to:

- Identify who is accessing the network
- Audit and control users access rights to resources
- Hide resources a user doesn’t have access to
- Consistently apply global access policies regardless of how a user gains access to the network

Access Control and Authentication

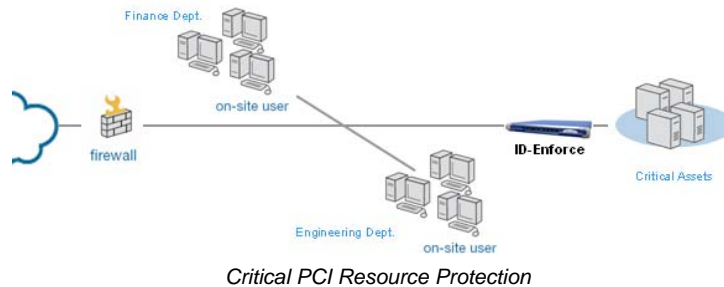
PCI Sec 1.2, 1.3, 1.3.5, 1.4, 1.42, 7.1, 7.2, 8.1, 8.2, 8.5, 8.54

Controlling Access ID-Enforce leverages the internal identity infrastructure so users are authenticated before allowed access to critical PCI resources. If a user is deleted from the identity store or their account disabled, ID-Enforce will not grant access even if an access policy for a user is still valid.

RSA Integration Applied Identity integrates with RSA's two factor authentication to provide both application and network access authentication – strengthening the overall security and integrity of the network.



Critical PCI Asset Protection Adding ID-Enforce to the infrastructure enables administrators to protect specific resources, forcing users to authenticate themselves by UserID as they move from network to network, thereby reducing the risk of unauthorized access to sensitive information.



Application and Resource Segmentation Using ID-Enforce as part of an internal network security solution will provide organizations with additional layers of access control to protect against the organization's sprawling definition of "authorized users," providing attack containment. Users can only "see" the resources they have privileges to see – minimizing the likelihood of attack.

Summary

Merchant and Service Providers are constantly at risk of losing cardholder information. Security incidents involving the loss of such data may result in fines, legal action and bad publicity. This in turn leads to loss of revenue and business disruption. Achieving compliance to the PCI Data Security Standard should be a high priority for organizations carrying out business transactions involving the use of credit cards.

By implementing identity aware network solutions to ensure critical PCI asset protection, in addition to other security solutions (such as vulnerability management, data encryption and two factor authentication) will go a long way towards helping any organization achieve compliance.

Customer Success Story



Boston.com is the fourth most popular media website in the world

- 4 Million Visitors a month with an average of 6 Million hits per day

Challenge:

- IP-based policies were time intensive and difficult to keep maintained for the level of security required
- User auditing for PCI DSS Compliance was a business requirement
- Protection of critical PCI DSS assets

Why they chose Applied Identity:

- Reduced time, resources, cost and effort associated with remote access administration, network segmentation and compliance audit reporting

What they deployed:

- 2 x ID-Enforce in High Availability pairs in front of business critical resources
- Integration with Active Directory and RSA SecureID two-factor authentication