**WHITE PAPER** | DICEMBRE 2015

# Garantire la compliance PCI

## con Privileged Access Management

# Executive summary

## La sfida

Le aziende che gestiscono transazioni con carte di debito o credito sono soggette a richieste sempre maggiori di soddisfare obblighi normativi in termini di compliance. Nello specifico, devono essere conformi alla versione 3 dello standard PCI DSS (Payment Card Industry Data Security Standard), entrato in vigore nel gennaio del 2015.[1] Tale versione ha definito vari requisiti per la protezione dei sistemi e delle reti aziendali, incluso l'ambiente CDE (Cardholder Data Environment, ambiente dei titolari di carte). I requisiti di strong authentication e controllo degli accessi all'ambiente CDE impongono alle aziende il difficile compito di adottare strumenti o pratiche di autenticazione multifattore, controllo degli accessi e reporting delle attività, in particolare per l'accesso amministrativo o con privilegi a tali sistemi.

## L'opportunità

I requisiti PCI DSS relativi al privileged access management sottolineano il rischio associato all'utilizzo improprio degli account con privilegi, poiché consentono l'accesso ad asset di business strategici. Tutti gli incidenti di sicurezza più recenti indicano come vettore di attacco principale delle violazioni riuscite gli utenti o le credenziali con privilegi. Un approccio efficace al privileged access management consente a un'azienda di limitare, registrare e monitorare tutte le attività eseguite da tali account, ad esempio gli amministratori di rete, sistema e database. Si ottengono così controllo e visibilità maggiori sugli utenti con privilegi e sui loro accessi da "super user" agli elementi strategici del business. Senza questo strumento, molte aziende hanno difficoltà a soddisfare i requisiti di identificazione, autenticazione e controllo degli accessi stabiliti nello standard PCI DSS v3, ma non riescono neanche a ridurre la propria esposizione a violazioni e attacchi.

## Vantaggi

Un sistema di difesa con un approccio granulare al privileged access management e integrato in una soluzione facile da implementare, come CA Privileged Access Manager, può aiutare le aziende a soddisfare i requisiti PCI DSS v3 e a proteggere meglio non solo gli ambienti CDE ma anche l'intera azienda IT ibrida che si estende su ambienti di rete, server, virtuale e cloud. Ne risultano una maggiore sicurezza a fronte delle violazioni e un rischio ridotto di mancata compliance agli standard PCI DSS.

**Sezione 1.**

# L'importanza di Privileged Access Management

Il privileged access management non è mai stato così importante. Numerose ricerche mostrano l'insuccesso sistematico delle tradizionali forme di difesa della sicurezza. Alcune suggeriscono addirittura che ogni azienda registra almeno un tentativo attivo di compromissione in ogni momento.[2] Sui media vengono regolarmente segnalate violazioni di grande portata, come quella subita da Target alla fine del 2013, quella di Home Depot del 2014 e quella dell'agenzia Office of Personnel Management del 2015, che ha visto l'utilizzo da parte di terzi delle credenziali sottratte. Il report Verizon sulle indagini relative alla violazione dei dati nel 2014 cita infatti l'utilizzo delle credenziali sottratte come la minaccia più grande contro le aziende[3], spesso inconsapevoli dei pericoli posti dagli account con privilegi e dall'elevato numero di account di questo tipo presenti nel business. Gli account con privilegi non sono utilizzati solo dai dipendenti dell'azienda, ma anche da terzi come fornitori, appaltatori, operatori che offrono il supporto tecnico per sistemi, device di rete e applicazioni. Una singola impresa può disporre di migliaia o perfino decine di migliaia di account con privilegi, ognuno dei quali implica dei rischi di sicurezza.

Il concetto su cui si fonda privileged access management è quello di fornire maggiore responsabilità e visibilità alle azioni degli amministratori. Nel modello tradizionale viene data completa fiducia a tutti gli amministratori, ma si tratta di un punto di vista ingenuo che trascura due possibili problemi: gli amministratori insoddisfatti che possono trasformarsi in una minaccia interna e le conseguenze di un account amministrativo compromesso da un attacco esterno, soprattutto nel caso in cui l'amministratore in questione sia un fornitore o qualsiasi altra terza parte.

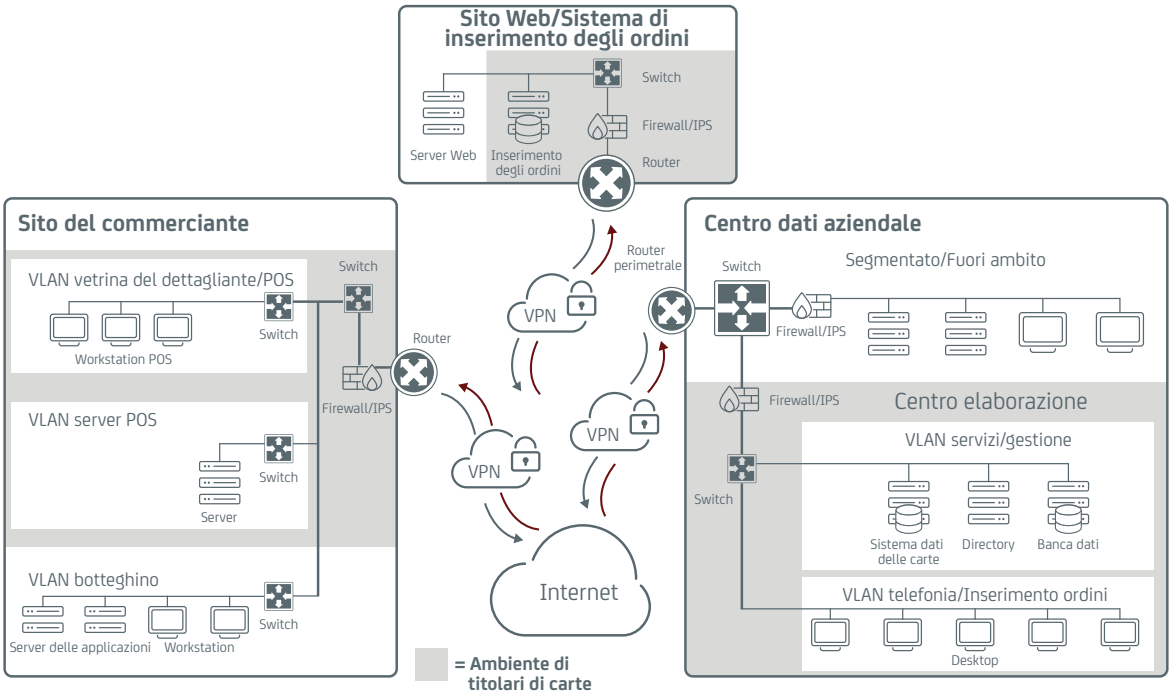
Per superare questa situazione è idonea l'adozione di un modello "zero trust", un approccio che CA Privileged Access Manager (già noto come Xceedium Xsuite), componente chiave delle soluzioni di privileged access management di CA Technologies, impiega quando presuppone che gli amministratori non debbano ricevere piena fiducia. Grazie a questo modello, si riducono il numero di violazioni e la gravità di quelle che potrebbero eventualmente verificarsi. In qualche misura, i requisiti PCI DSS riflettono il modello "zero trust", come nel caso del requisito 7.1.2: "Limitare l'accesso agli ID degli utenti con privilegi ai privilegi minimi indispensabili per l'esecuzione delle attività in funzione delle proprie responsabilità".

Tuttavia, mentre la compliance PCI fornisce una base solida per la protezione degli ambienti CDE, il rispetto dei soli requisiti minimi non è una difesa sufficiente contro le minacce odierne. Privileged access management va oltre i requisiti PCI e consente una migliore protezione degli ambienti CDE.

Oltre alla compliance PCI, altre ragioni rendono necessario privileged access management: interruzione della kill chain, riduzione delle minacce interne, registrazione, monitoraggio ed eliminazione delle password hard-coded.

**Figura A: L'ambito dei requisiti PCI DSS**

PCI DSS v3 richiede misure di salvaguardia dell'ambiente CDE (Cardholder Data Environment)




## Interruzione della kill chain

Il concetto di base di "kill chain", o catena di attacco, è che chi attacca segue uno schema ripetitivo per ottenere o ampliare il proprio accesso a un sistema, per poi conquistare privilegi più elevati, che vengono quindi utilizzati per accedere a un altro sistema o espandere gli accessi esistenti per poi conquistare ulteriori privilegi elevati e continuare con questa catena fino a quando non viene raggiunto l'obiettivo desiderato. Interrompendo la catena in qualsiasi momento del ciclo, l'attacco può essere arrestato prima che raggiunga l'obiettivo prefissato.

Le funzionalità di CA Privileged Access Manager possono aiutare a interrompere la kill chain. Ad esempio, la soluzione supporta l'autenticazione multifattore degli account con privilegi, rendendone più complessa la compromissione, poiché chi sferra l'attacco deve manomettere più credenziali per ogni singolo account. Inoltre, l'impiego dei privilegi minimi per quanto riguarda i comandi effettuabili da ogni account con privilegi su ciascun componente del CDE riduce l'accesso alle informazioni riservate, rendendo più difficile accedere a dati sensibili senza autorizzazione.

Inoltre, CA Privileged Access Manager agevola l'interruzione della kill chain grazie al supporto per la segmentazione di rete, un sistema che limita le subnet a cui può accedere uno specifico account con privilegi e quali sistemi è possibile amministrare su ciascuna subnet. La segmentazione della rete limita inoltre la diffusione degli attacchi da un sistema all'altro e restringe la visibilità degli attaccanti all'interno della rete aziendale. Analogamente, la soluzione è dotata di un agente SFA (Socket Filter Agent) che impedisce all'amministratore di aprire una connessione di rete non autorizzata verso un altro sistema, ad esempio nel tentativo di comunicare tramite SSH o telnet con un host non autorizzato dai criteri di CA Privileged Access Manager.

Queste funzionalità vengono specificamente raccomandate da aziende come Mandiant per la riduzione delle frodi con carta di credito.[4]

### Riduzione delle minacce interne

Sebbene i requisiti PCI si focalizzino sugli attacchi esterni, riconoscono anche l'importanza delle minacce interne che oggi sono una preoccupazione costante per le aziende. Uno studio indica che oltre il 10% dei dipendenti ha sottratto informazioni ai datori di lavoro per trarne profitto o conosce qualcuno che l'ha fatto.[5]

CA Privileged Access Manager limita le minacce interne in vari modi. Innanzitutto, l'implementazione dei principi dei privilegi minimi limita nettamente i comandi che un utente interno può inviare e i componenti dell'ambiente CDE verso il quale tali comandi possono essere inviati, riducendo al minimo i danni che un collaboratore interno può causare. In secondo luogo, la registrazione e il monitoraggio di tutte le attività degli account con privilegi fornisce una registrazione dettagliata di tutti i comandi inviati, che ne garantisce la tracciabilità fino alla persona specifica e non a un generico ID condiviso.

### Registrazione e monitoraggio di comandi

Indipendentemente da quanto sia rigidi i controlli di sicurezza, alcuni punti deboli rimarranno comunque, rendendo qualsiasi ambiente soggetto a violazioni. Poiché CA Privileged Access Manager registra e monitora tutte le attività che coinvolgono account con privilegi, semplifica notevolmente i processi forensi che mirano a stabilire come siano state utilizzate le credenziali amministrative non autorizzate da parte degli autori di attacchi riusciti.

### Rimozione delle password hard-coded

Ormai da tempo sviluppatori e amministratori di software usano le password hard-coded in script, codice sorgente e altro. Si tratta però di una vulnerabilità considerevole, perché a queste password possono accedere sviluppatori software, tester e altri; sono ambite anche dagli autori degli attacchi che sanno dove cercarle quanto si infiltrano nei sistemi e possono utilizzarle per accedere ad altri sistemi, come quelli dei database dei titolari di carte. CA Privileged Access Manager fornisce capacità di autenticazione da applicazione ad applicazione, che eliminano l'esigenza di creare password hard-coded.

---

**Sezione 2.**

## In che modo privileged access management aiuta a garantire la compliance PCI

Come già illustrato, privileged access management è un elemento critico della compliance PCI. È praticamente impossibile soddisfare la moltitudine di requisiti PCI in un tipico ambiente aziendale senza adottare una soluzione di privileged access management. Ad esempio, un leader della vendita al dettaglio era tenuto a versare una sanzione da 100.000 dollari al mese per non aver rispettato i requisiti PCI relativi a identificazione, autenticazione e controllo degli accessi. Aggiungendo CA Privileged Access Manager al proprio portfolio di soluzioni di sicurezza, il rivenditore ha potuto rispettare i requisiti mancanti ed evitare ulteriori sanzioni.

CA Privileged Access Manager consente di soddisfare ognuno dei seguenti requisiti PCI.[6]

### Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di sicurezza.

CA Privileged Access Manager soddisfa questo requisito in due modi. Innanzitutto, se utilizzato durante il deployment del sistema, può prendere il controllo degli account con privilegi predefiniti e reimpostare tutte le password predefinite per tali account. In secondo luogo, limita i protocolli che possono essere utilizzati per l'accesso amministrativo remoto, come SSH o SSL/TLS, impedendo che l'amministrazione del sistema sulle reti venga effettuata mediante protocolli non sicuri.

## Requisito 6: Sviluppare e gestire sistemi e applicazioni protette.

Componente importante di questo requisito è la gestione adeguata delle credenziali e la separazione dei compiti negli ambienti di sviluppo, testing e produzione. In tutti questi ambienti, CA Privileged Access Manager applica il controllo degli accessi basato su ruoli degli account con privilegi, supportando la separazione dei ruoli e facilitando al contempo la rimozione degli account di sviluppo, test e altro, che non sono più necessari una volta completato il deployment di un sistema o applicazione.

## Requisito 7: Consentire l'accesso ai dati dei titolari di carte limitatamente a una specifica esigenza commerciale.

CA Privileged Access Manager consente alle aziende di implementare il principio del privilegio minimo per l'accesso con privilegi, un'area molto spesso trascurata. Nello specifico, il modello "zero-trust" di CA Privileged Access Manager controlla in modo granulare gli accessi dei singoli utenti con privilegi o gruppi di tali utenti (ad esempio gli amministratori di database). Il prodotto limita così i componenti di sistema a cui ogni utente o gruppo con privilegi può accedere, come server, device di rete e applicazioni, e quali comandi possono essere eseguiti da ogni utente o gruppo con privilegi su ciascuno di questi componenti. L'integrazione di CA Privileged Access Manager con Active Directory, LDAP e altre directory aziendali consente di riutilizzarne i ruoli e le definizioni di gruppo.

## Requisito 8: Identificare e autenticare l'accesso ai componenti di sistema.

Quasi tutte le condizioni di questo requisito sono esplicitamente supportate da CA Privileged Access Manager, che richiede infatti un ID univoco per ogni utente con privilegi, offre tutte le funzionalità di gestione delle password standard e supporta numerose tecnologie di autenticazione a fattore multiplo e singolo. Nello specifico, la soluzione supporta il requisito 8 come indicato di seguito.

- **8.1:** CA Privileged Access Management garantisce l'identificazione univoca di ogni utente con privilegi, anche quando vengono utilizzati account condivisi per determinati componenti dell'infrastruttura, come i router. Applica la separazione dei compiti degli utenti con privilegi. Fornisce funzionalità standard per eliminare immediatamente i privilegi degli accessi revocati, disabilitando gli account con privilegi inattivi e applicando criteri di esclusione per i tentativi di autenticazione falliti e i criteri di riautenticazione per le sessioni inattive.
- **8.2:** Integra molti metodi di autenticazione, richiedendo l'autenticazione di tutti gli utenti con privilegi. Archivia password e altre credenziali (ad esempio chiavi crittografiche private) in vault con crittografia robusta e li trasmette esclusivamente su canali crittografati. Adotta criteri standard di lunghezza, sicurezza, età e riutilizzo delle password.
- **8.3:** Supporta numerosi metodi di autenticazione multi fattore, RADIUS, certificati X.509 e smart card.
- **8.5, 8.6:** Consente alle aziende di utilizzare gli account condivisi in background, richiedendo al contempo l'identificazione e l'autenticazione esclusiva di ogni utente con privilegi, incluse eventuali terze parti. Questa identificazione esclusiva prevede anche l'utilizzo di smart card, certificati digitali, token crittografici e altre forme di credenziali diverse dalle password.
- **8.7:** Limita l'accesso diretto al database dei titolari di carte ai soli amministratori di database autorizzati. Offre un supporto da applicazione ad applicazione per garantire che i singoli individui non possano accedere o riutilizzare le credenziali delle applicazioni.

## Requisito 10: Registrare e monitorare tutti gli accessi alle risorse di rete e ai dati dei titolari di carte.

Analogamente al requisito 8, CA Privileged Access Manager supporta quasi tutti gli elementi del requisito 10. Infatti registra e monitora tutte le attività eseguite utilizzando ogni account con privilegi, incluse registrazioni per audit in formato syslog

e registrazioni DVR-like di sessioni amministrative, aggiungendo etichette alle per indicare potenziali violazioni dei criteri e velocizzare la revisione. Nello specifico, CA Privileged Access Manager supporta il requisito 10 come indicato di seguito:

- **10.1:** CA Privileged Access Manager collega ogni istanza di un accesso con privilegi a una persona specifica. Fornisce audit trail per ogni persona per l'accesso con privilegi a tutti i componenti di sistema.
- **10.2:** Utilizza registrazione e syslog nativi per generare audit trail automatici che registrano ogni azione compiuta da ogni utente con privilegi su server, device e data base di rete e altre applicazioni. Include tutte le attività di identificazione e di autenticazione degli account con privilegi. Limita l'accesso agli audit trail in modo che solo gli utenti autorizzati possano revisionarli e accedere a tali revisioni.
- **10.3:** Registra tutti i campi obbligatori PCI per ogni evento registrato, inclusa identificazione degli utenti, tipo di evento, data e ora, esito positivo o negativo, origine dell'evento e identità della risorsa coinvolta (nome host e così via).
- **10.4:** Utilizza la tecnologia di sincronizzazione dell'orario (ad esempio il protocollo NTP, Network Time Protocol) per la sincronizzazione degli orologi.
- **10.5:** Utilizza tecniche di hashing per identificare qualsiasi tentativo di manomissione di log di audit e registrazioni. Consente l'inoltro del syslog per eseguire il backup dei record di audit in un apposito archivio centralizzato.
- **10.7:** Utilizza syslog e supporta l'inoltro di syslog, così da poter conservare i record per il tempo desiderato.

### Requisito 12: Gestire una policy relativa alla sicurezza delle informazioni per tutto il personale.

CA Privileged Access Manager Consente l'acquisizione e l'applicazione di criteri utente con privilegi. Inoltre, registra tutti i tentativi di violazione dei criteri, che sono parte integrante di un processo di valutazione dei rischi.

### Protezione dell'ambiente CDE: dalla prospettiva di controllo del server

La soluzione di privileged access management di CA Technologies include anche requisiti aggiuntivi per il controllo degli accessi localizzati e granulari all'host, al fine di proteggere ulteriormente le risorse più preziose, come l'ambiente CDE. CA Privileged Access Manager Server Control fornisce un ulteriore livello strategico di protezione della sicurezza su piattaforme server, abilitando controllo granulare degli accessi, gestione basata su criteri, e auditing sicuro, fondamentale per proteggere le risorse elettroniche. È possibile progettare policy di accesso che regolamentino l'accesso alle risorse, ai programmi, ai file e ai processi presenti sul server, mediante una vasta gamma di criteri.

---

**Sezione 3.**

## Confronto tra PCI DSS versione 2 e PCI DSS versione 3

L'aggiornamento dalla versione 2 alla versione 3 di PCI DSS ha aggiunto significative protezioni per gli ambienti CDE, come indicato di seguito:

- Implementazione della segmentazione di rete per l'ambiente CDE, al fine di isolarne meglio le diverse aree. Garantisce che tutti i flussi di dati tra i componenti di sistema siano documentati e registra tutte le attività eseguite dagli utenti con privilegi.
- Esegue il testing della penetrazione perimetrale nel CDE.
- Gestisce le credenziali e implementa il controllo e l'auditing degli accessi con privilegi minimi per tutti gli accessi al CDE.
- Rende più rigidi i controlli di sicurezza per i service provider.[7]

Queste forme di protezione enfatizzano la necessità di disporre di una soluzione di privileged access management come CA Privileged Access Manager per proteggere l'ambiente CDE e soddisfare i requisiti di compliance PCI. Nella maggior parte degli ambienti, privileged access management è l'unico modo per implementare in modo efficace sia il principio del privilegio minimo per il controllo degli accessi amministrativi sia la registrazione granulare delle attività amministrative. È inoltre preziosa per l'implementazione della segmentazione della rete e il monitoraggio di tutte le attività che implicano un flusso di dati tra segmenti di rete.

L'aggiornamento dello standard PCI DSS contiene altre modifiche relative a privileged access management. In primo luogo, è stato rielaborato il requisito 8, relativo all'identificazione e all'autenticazione. A un primo esame appare come il requisito che ha subito le maggiori modifiche. Tuttavia, le modifiche fanno principalmente riferimento alla rielaborazione dello stesso requisito.

La modifica più significativa è l'aggiunta del requisito 8.6: "Nell'utilizzo di meccanismi di autenticazione diversi dalle password, quali token crittografici o smart card, il meccanismo di autenticazione deve essere disponibile a un solo utente; non è consentito l'impiego di meccanismi di autenticazione condivisi." Come si è visto nella sezione precedente, CA Privileged Access Manager consente di rispettare questo nuovo requisito.

---

**Sezione 4.**

## Vantaggi

Le aziende che adottano soluzioni di privileged access management ottengono un livello di sicurezza maggiore e riducono i rischi di minacce interne ed esterne, oltre ad aumentare la compliance con le normative e con lo standard PCI DSS.

Più in dettaglio, CA Privileged Access Manager consente alle aziende non solo di soddisfare i requisiti di compliance di PCI DSS, ma anche di migliorare la condizione complessiva di sicurezza nel modo più conveniente dal punto di vista economico.

- **Riduzione dei costi.** CA Privileged Access Manager aiuta a ridurre significativamente il costo degli audit PCI DSS, fornendo una modalità semplice e conveniente di segmentare in modo logico la rete aziendale. Si tratta infatti di un device simile a un proxy che funziona sul livello applicativo della rete e controlla gli utenti con privilegi che possono accedere ai sistemi. La segmentazione logica del livello di gestione consente di conservare le esistenti topologie della rete fisica, segregando al contempo i sistemi con i dati di titolari di carte in punti isolati, il cui accesso è rigidamente controllato. Con questo approccio, CA Privileged Access Manager consente alle aziende di isolare logicamente i sistemi dove risiedono i dati dei titolari di carte, restringendo l'ambito degli audit PCI senza incorrere nei notevoli costi necessari a segmentare fisicamente le reti.
- **Sicurezza migliorata.** Il granulare approccio difensivo di CA Privileged Access Manager alla sicurezza consente alle aziende di implementare un set di controlli completo che riduce i rischi impliciti degli utenti con privilegi e fornisce una più ampia protezione contro le minacce esterne, prevenendo il verificarsi delle violazioni o minimizzandone l'impatto.
- **Time-to-protection e gestione più rapidi.** La facilità di deployment e gestione da una singola piattaforma consente di accelerare e migliorare il controllo degli accessi con privilegi e la protezione delle credenziali dei sistemi nell'intera azienda ibrida, dai tradizionali data center agli ambienti virtualizzati, ai cloud pubblici o a qualsiasi loro combinazione, senza il necessario sovraccarico associato ad approcci alternativi.

**Sezione 5.**

# Conclusioni

Privileged access management è un imperativo per ottenere soddisfare i requisiti di compliance PCI. Il suo valore supera però questo obiettivo, poiché consente a un'azienda di migliorare la propria sicurezza complessiva rispetto alle odierne minacce perpetrate dall'interno e dall'esterno. CA Privileged Access Manager offre modalità efficaci per adottare privileged access management a sostegno della compliance PCI e di altre esigenze di protezione.

Adottando CA Privileged Access Manager le aziende possono:

- Ridurre i costi della compliance PCI soddisfando i molti requisiti dello standard grazie a una soluzione completa completamente integrabile con le soluzioni aziendali già esistenti.
- Risparmiare sui costi correlati alle violazioni e salvaguardare la reputazione dell'azienda prevenendo gli attacchi ai dati e minimizzando gli effetti di quelli che possono eventualmente verificarsi.



1 PCI DSS versione 3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

2 Report annuale di cisco sulla sicurezza nel 2014, http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

3 Report Verizon sulle indagini relative alla violazione dei dati nel 2014, http://www.verizonenterprise.com/DBIR/2014/?utm_source=earlyaccess&utm_medium=redirect&utm_campaign=DBIR

4 M-trends 2014: oltre la violazione, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

5 Fughe di dati a livello mondiale: l'elevato costo delle minacce interne, http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.pdf

6 PCI DSS versione 3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

7 PCI DSS: riassunto delle modifiche apportate nell'aggiornamento dalla versione 2.0 alla versione 3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids



CS200-163851_1215