Il ciclo di vita delle identità e dei privilegi per la compliance e la protezione.

Enrico Nasi – Aditinet Consulting

Identita’ = nuovo perimetro

Dal momento in cui i nuovi attacchi informatici bypassano i tradizionali controlli di sicurezza perimetrale, anche il concetto di perimetro sta subendo profondi cambiamenti. Il perimetro e’ determinato non tanto dalla posizione sulla rete, ma dal “**Chi sono**” e “ A quali informazioni posso accedere”.

Oggi e’ fondamentale avere a disposizione gli strumenti e le best practices giuste per il **ciclo di vita di identita' ed accessi** alla velocita’ del cloud e del business di oggi – ma in **modo sostenibile e conforme** agli obiettivi di gestione del rischio.

Cio e’ importante **per tutte le identita’** – siano esse identita’ interne, consulenti, partner o **utenti ad elevati privilegi**.

EU General Data Protection Regulation

La recente approvazione della GDPR:

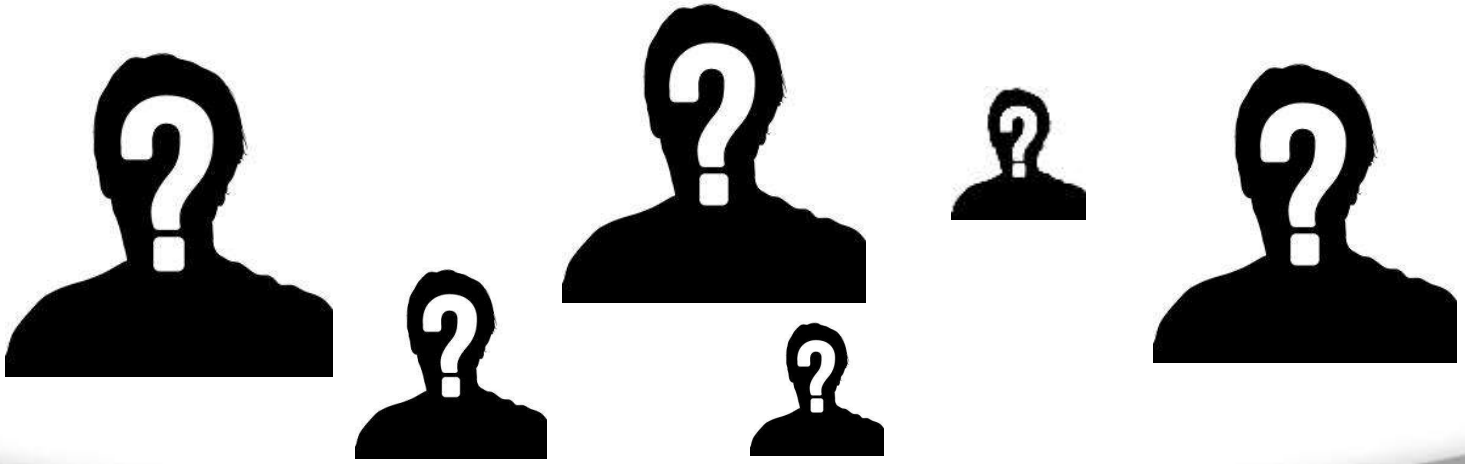
Per le Aziende e' un'opportunita' per rivedere i processi di governo dei dati e delle identita'

aditinet
1st CLASS IT

Si sposta l’attenzione

Oggi e’ accettato il fatto che il perimetro di rete viene bypassato

Il nuovo campo di battaglia e’ all’interno della nostra rete.
Obiettivi = **identita’ e dati**.



Si sposta l'attenzione

Appare una nuova famiglia di tecnologie di contromisura
Un riferimento Gartner:
«Market Guide to User Entity Behavioral Analysis»
Aviva Litah, September 2015

Market Guide for User and Entity Behavior Analytics

Published: 22 September 2015

Analyst(s): Avivah Litan

UEBA successfully detects malicious and abusive activity that otherwise goes unnoticed, and effectively consolidates and prioritizes security alerts sent from other systems.

Tali tecnologie usano tecniche di machine Learning per ridurre la finestra di rischio per il data breach.
Parleremo di Lightcyber nella parte successiva di questo incontro.

aditinet
1st CLASS IT

Identita’ generiche e privilegiate

Identita’ Generiche:

- Piu’ facili da attaccare
- Si arriva direttamente ai Dati
- In gran numero: e’ facile perdere il controllo di cosa succede

Identita’ Privilegiate

- In genere sono protette meglio
- Permettono di arrivare dappertutto

Problemi organizzativi e tecnici differenti,
Strumenti differenti per affrontarli

Strumenti tecnologici per l'Identita'

LEADERS RICONOSCIUTI

tecnologie specializzate, allo stato dell'arte

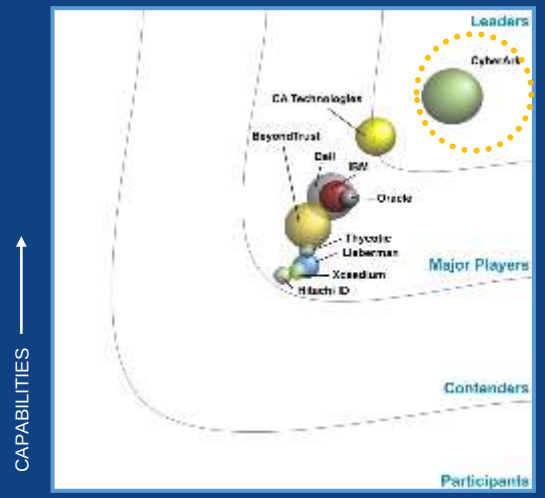
SailPoint

Magic Quadrant for Identity Governance and Administration [February 2016]

SOURCE: GARTNER (FEBRUARY 2016)

CyberArk

IDC MarketScape:
Worldwide Privileged Access Management



SOURCE: IDC 2014

aditinet 1st CLASS IT

aditinet
1st CLASS IT

Sailpoint

Automazione e Conformita’
nella gestione del ciclo di vita
di tutte le identita’

Identity Governance

- Abbiamo una mappa utilizzabile e chiara di CHI ha accesso a COSA ?
- La mappa corrisponde ai reali requisiti di business e gestione del rischio?
- Posso provarlo al mio interno o ad un ente terzo?
- Posso gestire i cambiamenti in modo sostenibile ?

aditinet
1st CLASS IT

Missione Sailpoint

Missione dell'Identity Governance e' rispondere queste domande in modo organico, contribuendo a costruire **un processo aziendale sostenibile ed assistito dall'automazione** per il governo delle identita'.

Tale e' anche la missione di **Sailpoint**,
leader tecnologico nel settore.

SailPoint

aditinet
1st CLASS IT

Missione Sailpoint

La soluzione SailPoint **non si sostituisce ai repository di identità**.

Sailpoint **semplifica ed automatizza i processi IAM** con attenzione alla sicurezza e alle normative, ponendosi come punto di gestione unificato per tutte le identita' e le risorse cui esse hanno necessita' di accesso.

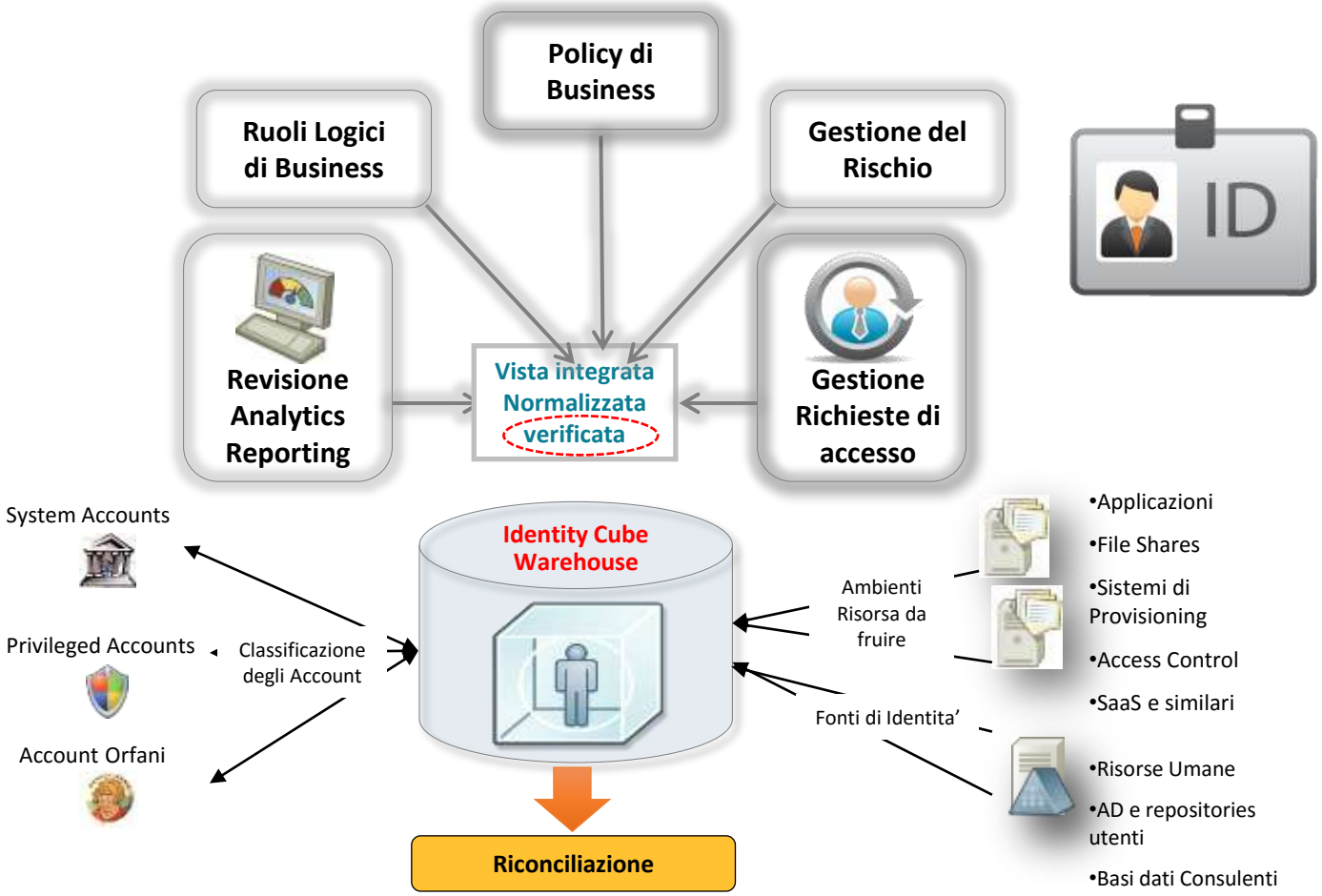
In quest'ottica SailPoint permette di governare in modo efficace e sostenibile il processo di gestione delle identità, con un approccio a fasi:

- **Visibilità** e mappatura dello stato corrente
- **Pianificazione dello stato target**, sulla base degli obiettivi di business e gestione del rischio
- **Gestione continua**, automatizzata, documentata e sostenibile

SailPoint

aditinet
1st CLASS IT

Sailpoint – l'Identity Cube



aditinet
1st CLASS IT

Architettura di Sailpoint Identity IQ

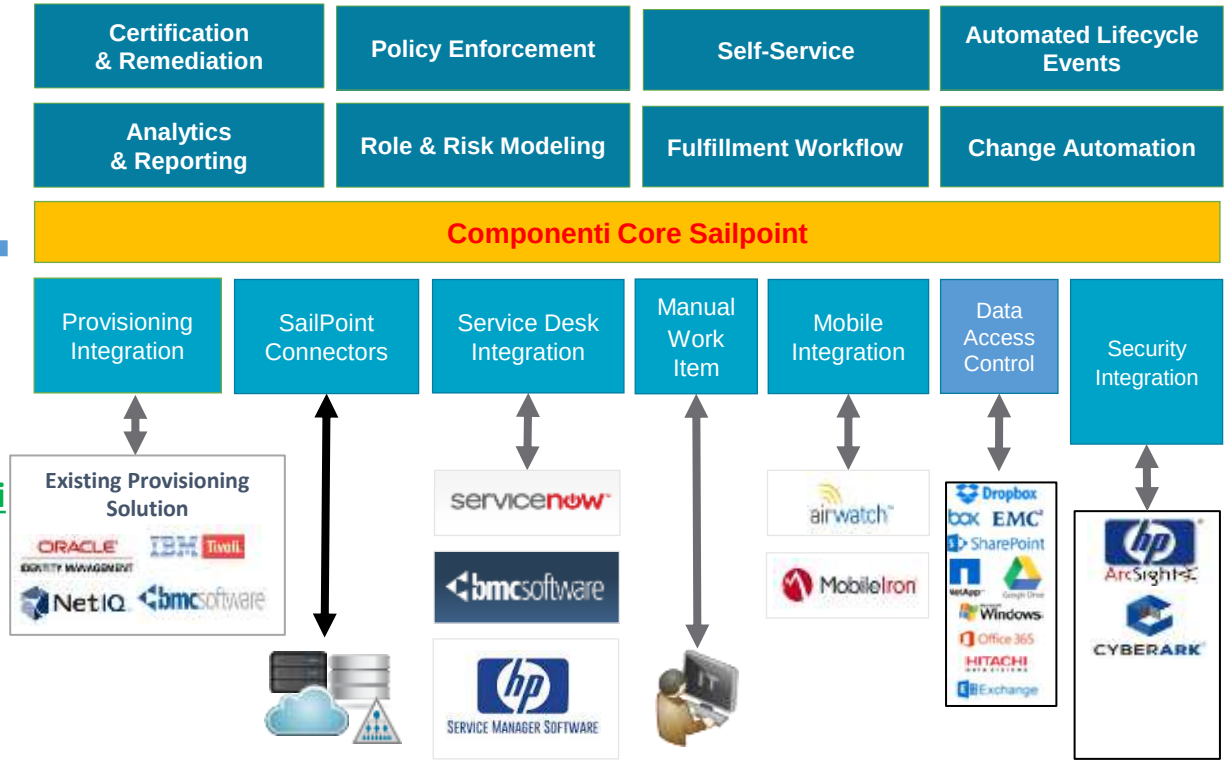
Livello di Business/Automazione

Qui Sailpoint offre due set di funzioni:

- **Lifecycle Manager** per l'automazione
- **Compliance Manager** per il governo e la conformita'

Livello tecnologico

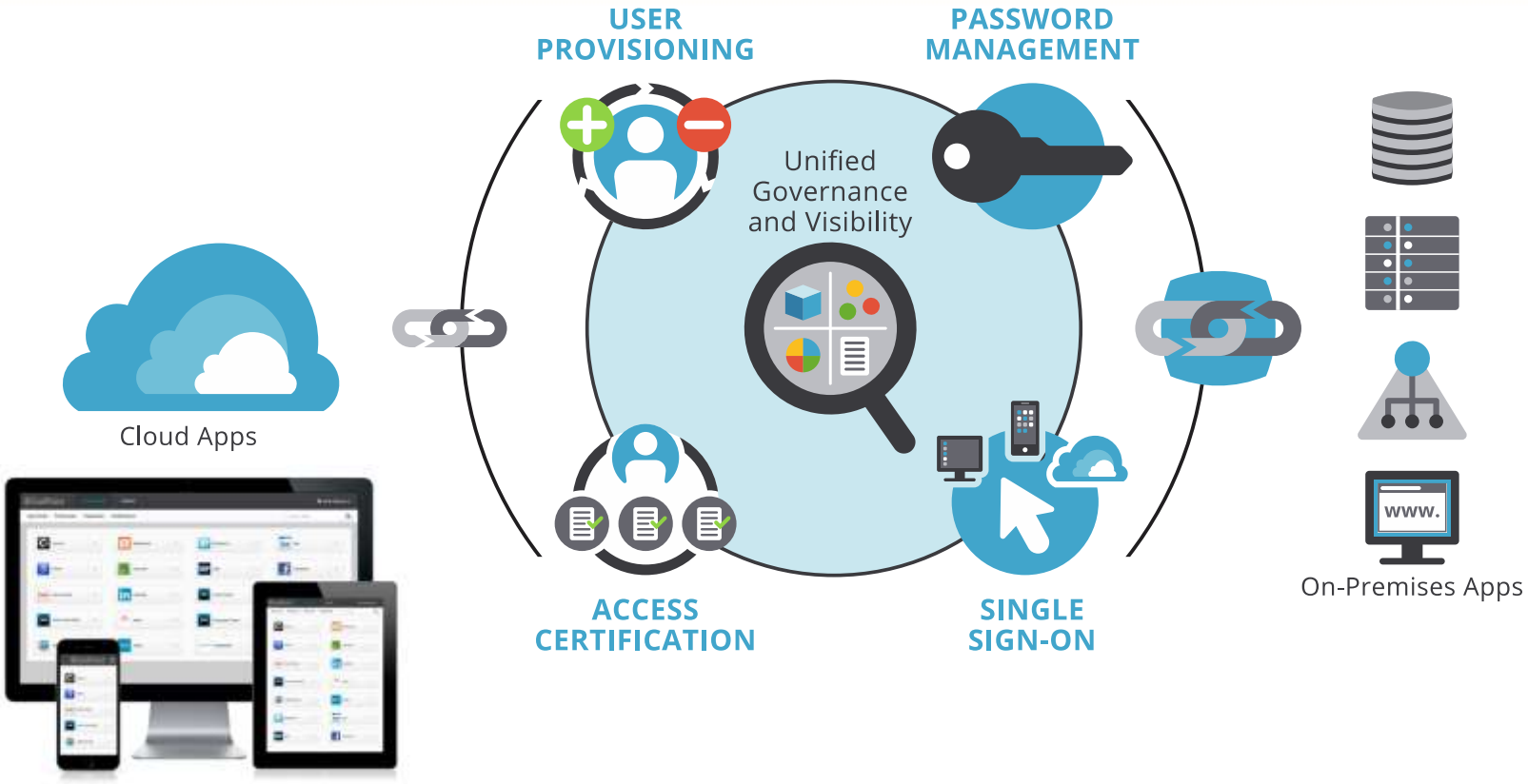
SailPoint e' Leader Gartner nel settore e vanta una larga base di installato in grandi Enterprise, anche grazie al **set completo di connettori** ed alla elevata flessibilità nelle integrazioni.



Alla soluzione «on-premises» (IdentityIQ) si affiancano le soluzioni di IGA su Cloud (IdentityNow) e di controllo accesso ai dati non strutturati(SecurityIQ).

aditinet
1st CLASS IT

IdentityNOW



IdentityNow: la suite cloud-based IDaaS di Sailpoint

aditinet
1st CLASS IT

Dati Non Strutturati

Aumento del volume e dell'importanza dei **dati non strutturati**
Nelle diverse forme: files, NAS, piattaforme di collaboration, cloud storage …

Anche in questo caso e' necessario governo e compliance, attorno al concetto chiave di «Owner di un dato».

Dati Non Strutturati – Sailpoint Security IQ

Visibilita'

- Scoperta e classificazione dei dati sensibili
- Analisi di « Chi » puo' accedere a « Cosa »

Analisi

- Identifica i dati « sovraesposti » oltre le policy di business
- Match tra i diritti di accesso e gli accessi realmente effettuati

Controllo

- Identificazione dei « Data Owners » logici
- Definizione di policy di accesso e di alerting

Remediation

- Normalizzazione dei modelli di accesso
- Identificazione dei gap nascosti
- Riconciliazione

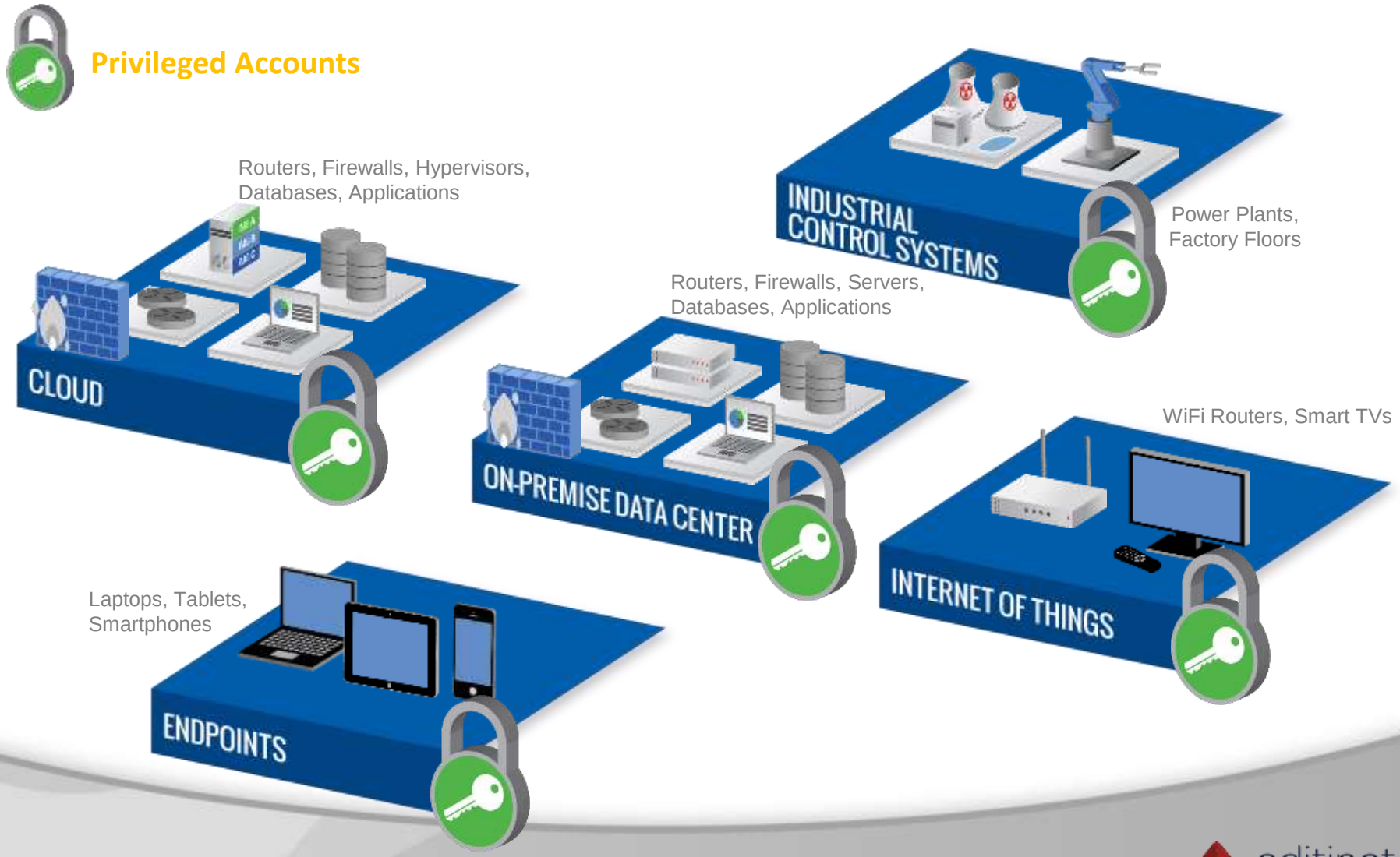
Sailpoint e' presente anche in quest'area – con la soluzione specifica SecurityIQ

aditinet
1st CLASS IT

CyberArk

Protezione completa delle identita’ privilegiate

Le identita’ privilegiate sono ovunque



aditinet
1st CLASS IT

Identita’ privilegiate: un target per gli attacchi

BlackPOS Attacks Retailers

At the end of 2013 and continuing into 2014, several large organizations were attacked using BlackPOS, a type of ma targeting point of sale systems. The malware was transferr at least one of the organizations using **privileged** network credentials assigned to a remote vendor

U.S. Intelligence Agency Breached

A third-party systems administrator abused his insider status and authorized **privileged** credentials to download and make public hundreds of thousands of classified documents.

South Korean TV Stations and Banks Attacked with Data Wiping

According to reports, the devastating attacks carried out on South Korea were precipitated by hackers obtaining a **privileged** admin login to a security vendor’s

Global Energy Firms Targeted by “Flame” Cyber Espionage Worm

Starting in 2009 and reported in 2011, an attack was carried out against a number of energy firms that targeted proprietary operations and project-financing information. Once the initial system was compromised, the attack targeted local **privileged** administrative accounts, providing the attacker with broad access to the energy firms’ systems and confidential intellectual property.

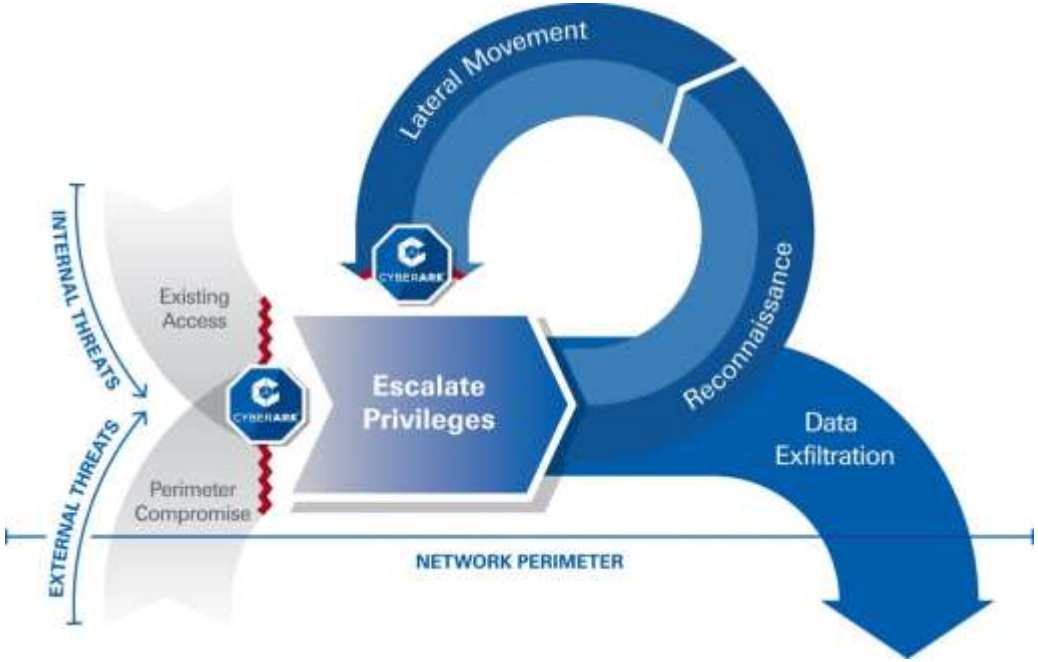
“…once they have privileged credentials, they are pretty much home free.”

Deloitte, 2014

aditinet
1st CLASS IT

Identita’ privilegiate e APT

Negli attacchi di tipo permanente (APT) sono spesso coinvolti gli account ad elevati privilegi.



La suite Cyberark trova applicazione in tutte le fasi della strategia di difesa dagli APT:

Riduzione del rischio: le credenziali sono erogate in modo controllato, con l’enforcement del principio dei minimi privilegi e separation of duty
Rilevamento: con il monitoraggio continuo delle sessioni e degli eventi relativi agli account privilegiati
Risposta: possibilita’ di blocco in tempo reale, disponibilita’ di informazioni di forensica

aditinet
1st CLASS IT

Proteggere le utenze privilegiate in 4 passi

Processo di discovery di tutti gli utenti privilegiati

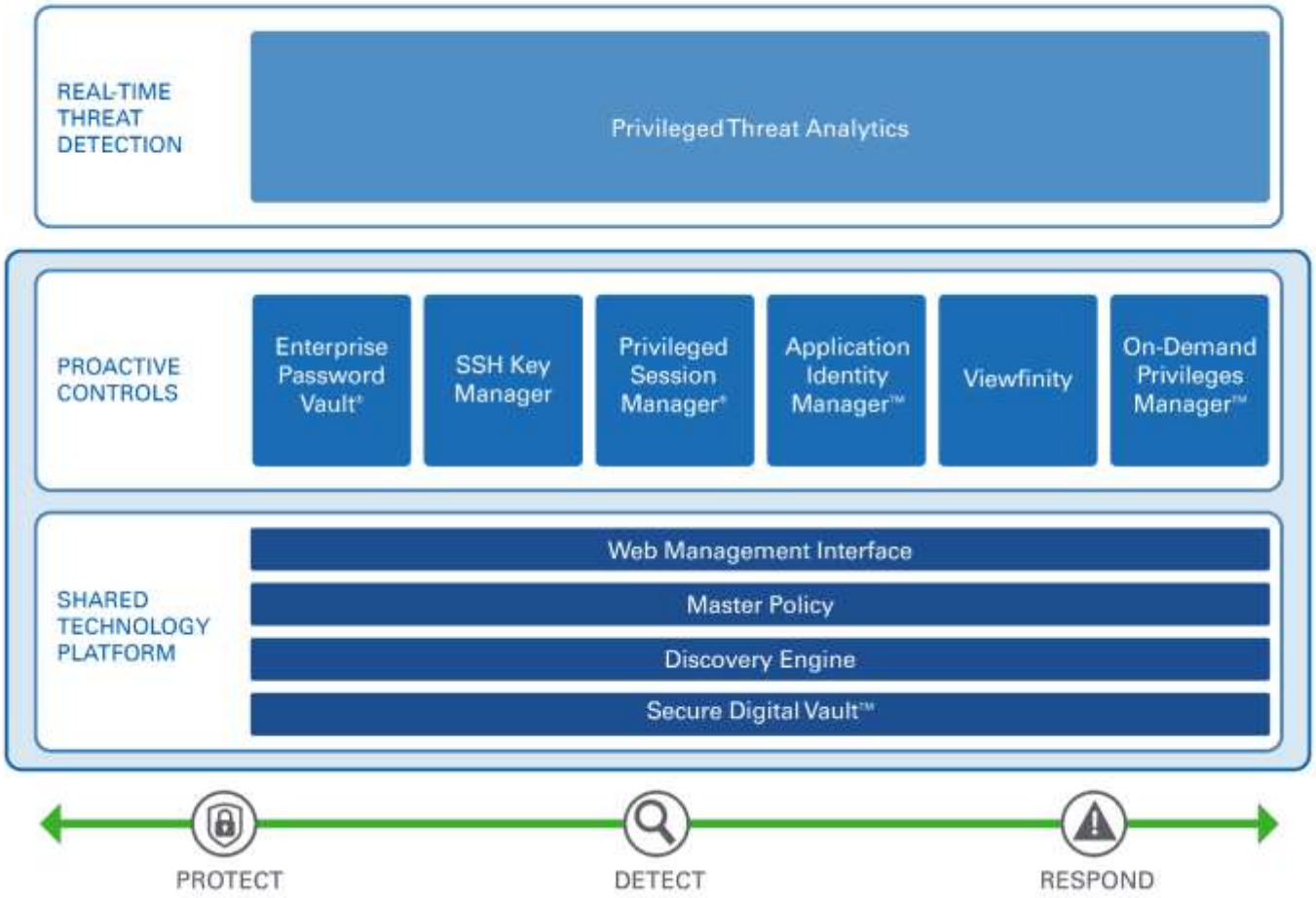
Proteggere e gestire le credenziali

Isolamento e monitoraggio delle session privilegiate

Utilizzare l'analisi real-time sulle attivita' privilegiate per rilevare e rispodere agli attacchi in corso

aditinet
1st CLASS IT

La suite CyberArk



Il diagramma mostra l'architettura della suite CyberArk, con le diverse componenti funzionali che poggiano sul core Shared Technology Platform

aditinet
1st CLASS IT

Discovery

Step 1

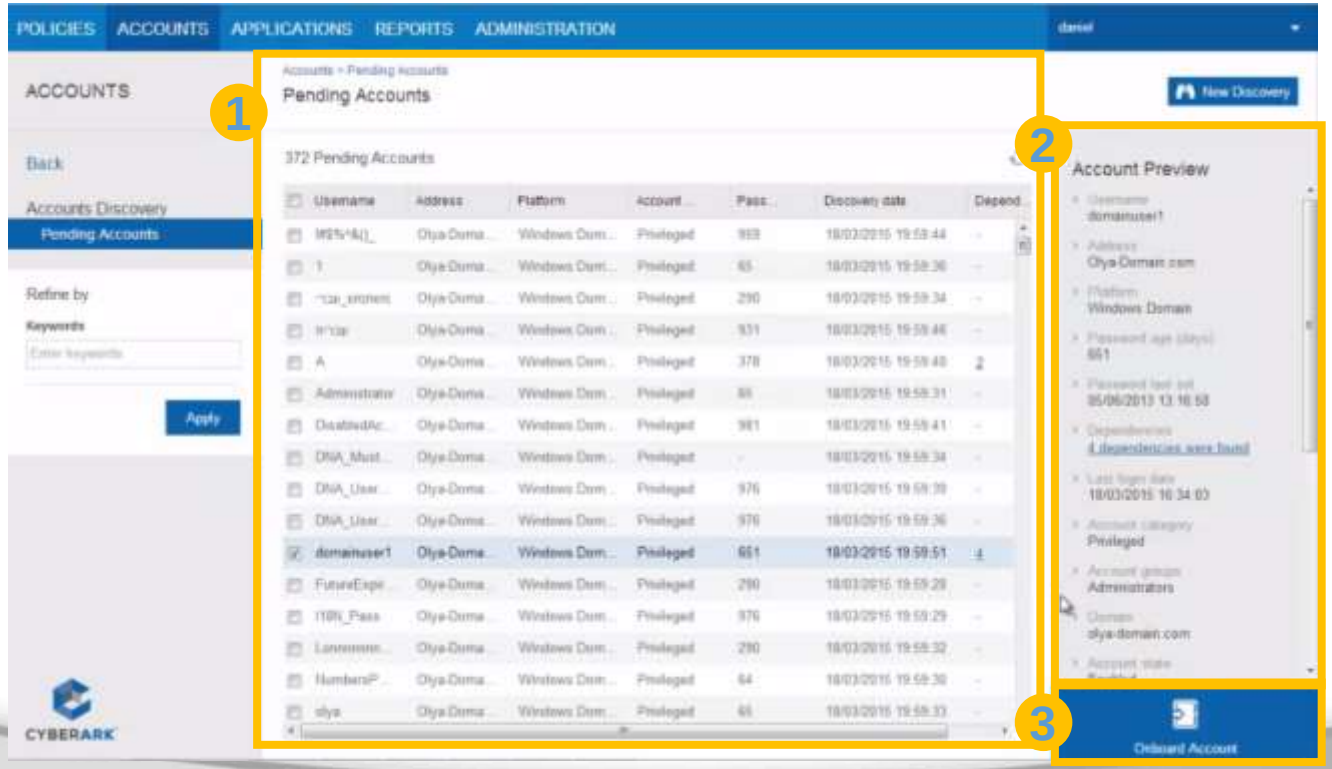
Scan your IT environment for privileged accounts

Step 2

Preview account statuses and dependencies

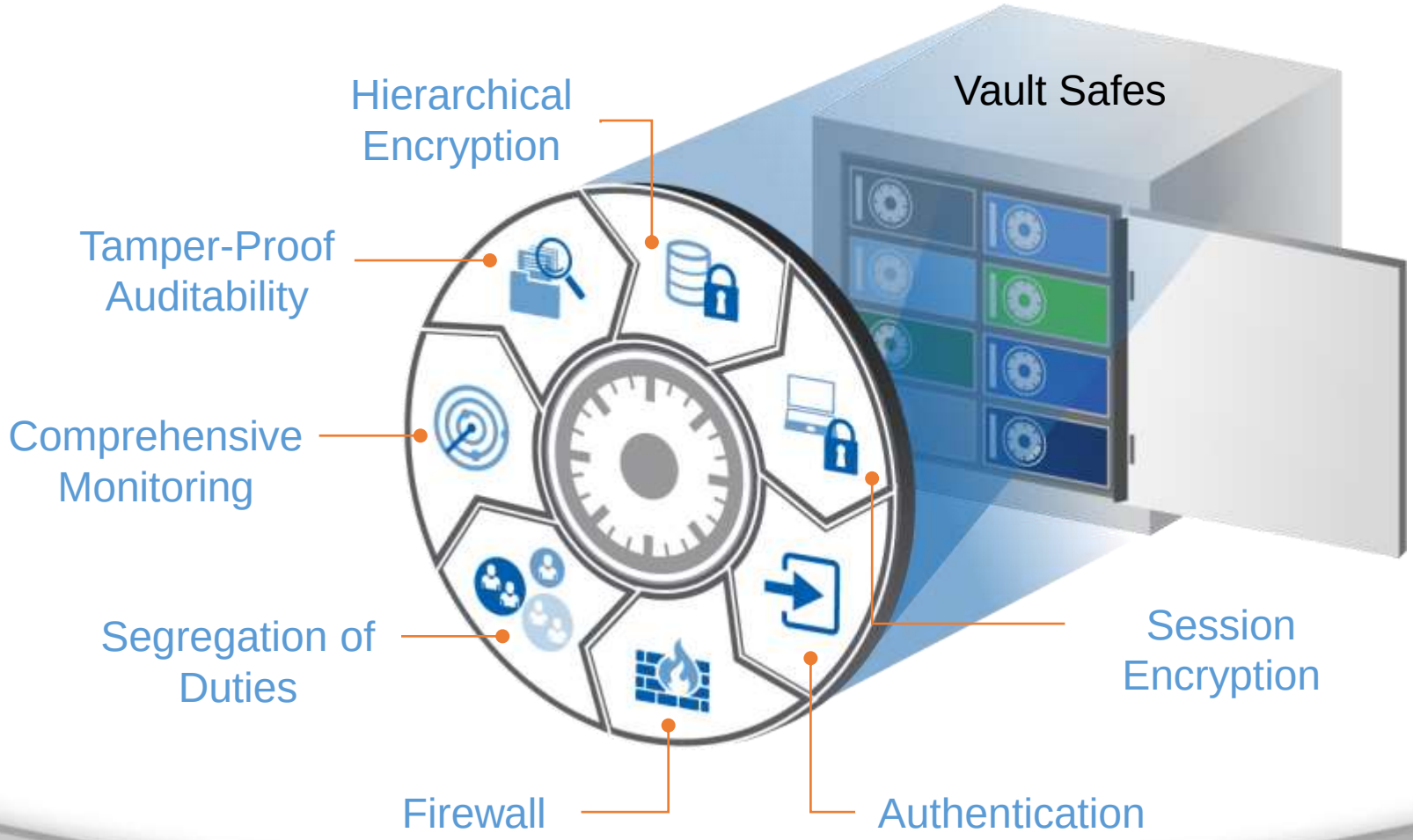
Step 3

Select which accounts to onboard; onboard them to the Digital Vault



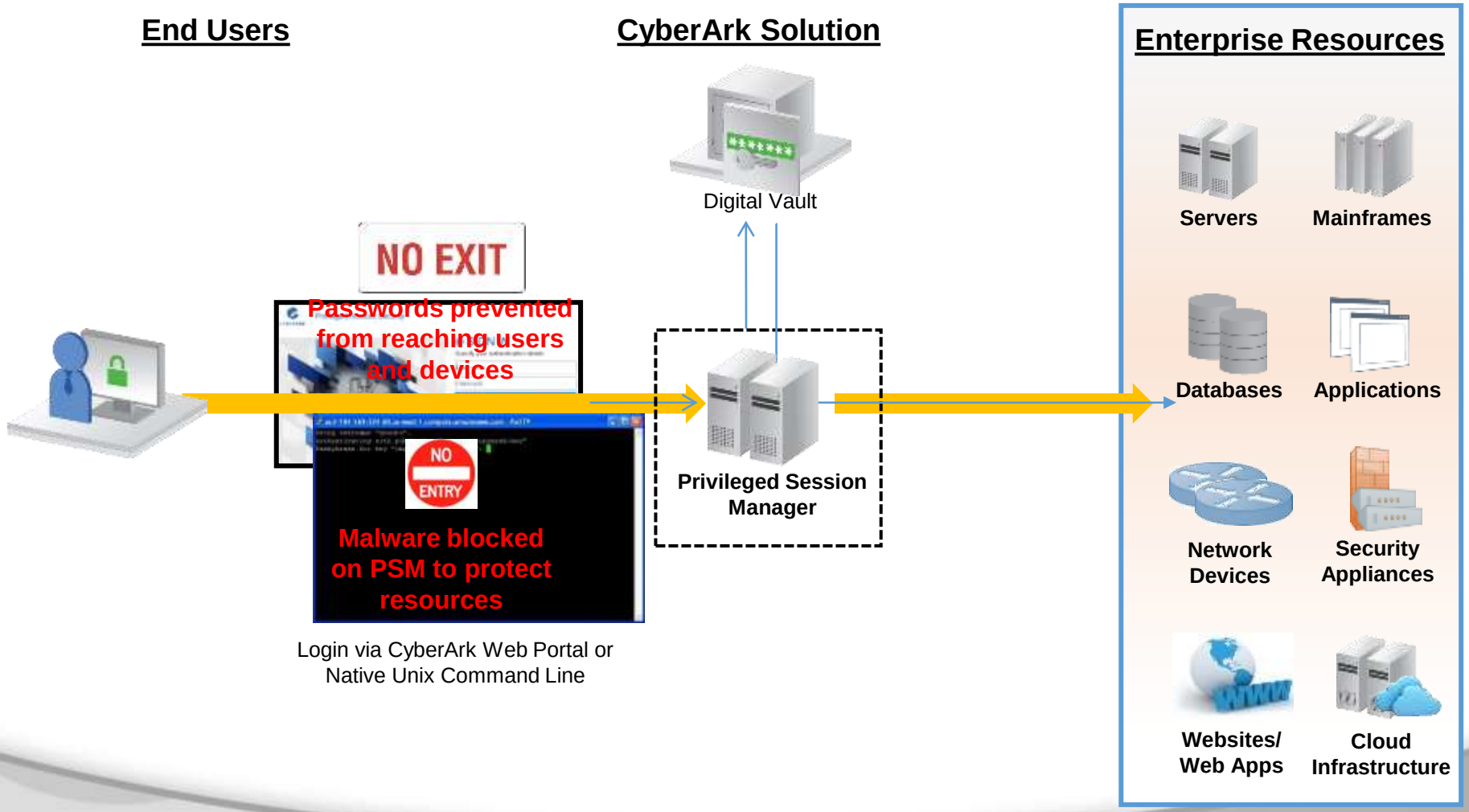
aditinet
1st CLASS IT

CyberArk Digital Vault

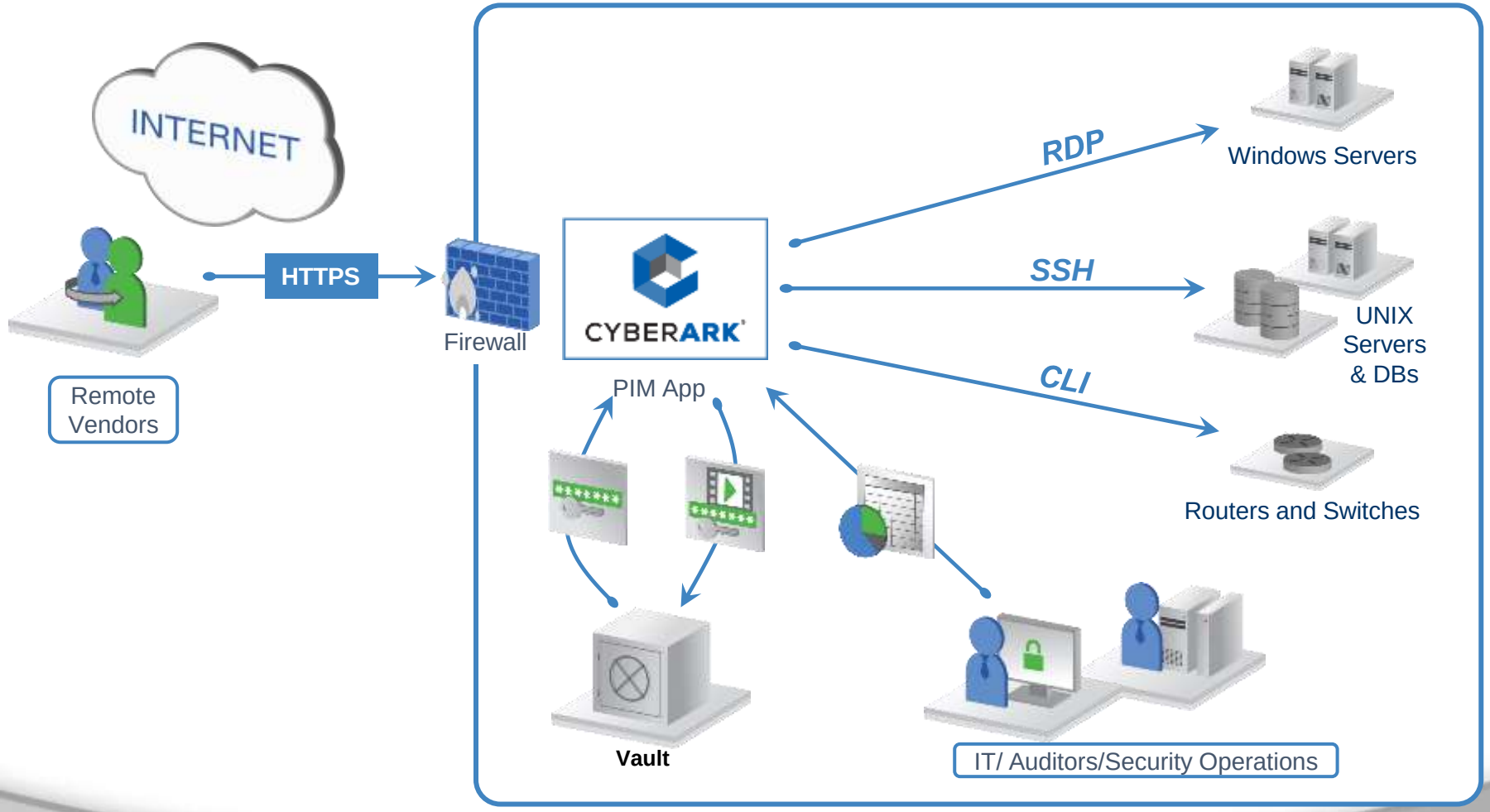


aditinet
1st CLASS IT

CyberArk PSM all'opera:



Un esempio: accesso remoto fornitori



aditinet
1st CLASS IT

CyberArk Suite

In generale, l'adozione di CyberArk e' sempre uno strumento efficace per la riduzione del rischio.

Alcuni casi d'uso:

- **Eliminazione delle utenze impersonali**, con l'introduzione della «accountability»
- Introduzione del principio dei **minimi privilegi**
- Gestione dei **consulenti o fornitori** che richiedono elevati privilegi per l'espletamento dei loro compiti
- Registrazione delle sessioni ai fini della **forensica**
- Contromisura contro le **minacce persistenti APT** all'interno della rete

CYBERARK

aditinet
1st CLASS IT

CyberArk Viewfinity

Il tema dei diritti di amministrazione sulla postazioni Windows: come governarlo?
Come ridurre il rischio e l'impatto sull'operativita' degli utenti?

CyberArk Viewfinity:

- Permette di rimuovere di diritti di admin agli utenti generici Windows, erogando i diritti ad Applicazioni e servizi in modo controllato
- I diritti per le Applicazioni sono controllati da funzioni di Application Whitelisting & Control
- Gli eseguibili non noti possono essere eseguiti con privilegi minimi e privi di accesso alla rete

CyberArk Viewfinity e' utilizzabile per contenere la diffusione di Malware o Ransomware sulle workstation

CYBERARK

aditinet
1st CLASS IT

Il ciclo di vita delle identità e dei privilegi per la compliance e la protezione.

Enrico Nasi – Aditinet Consulting