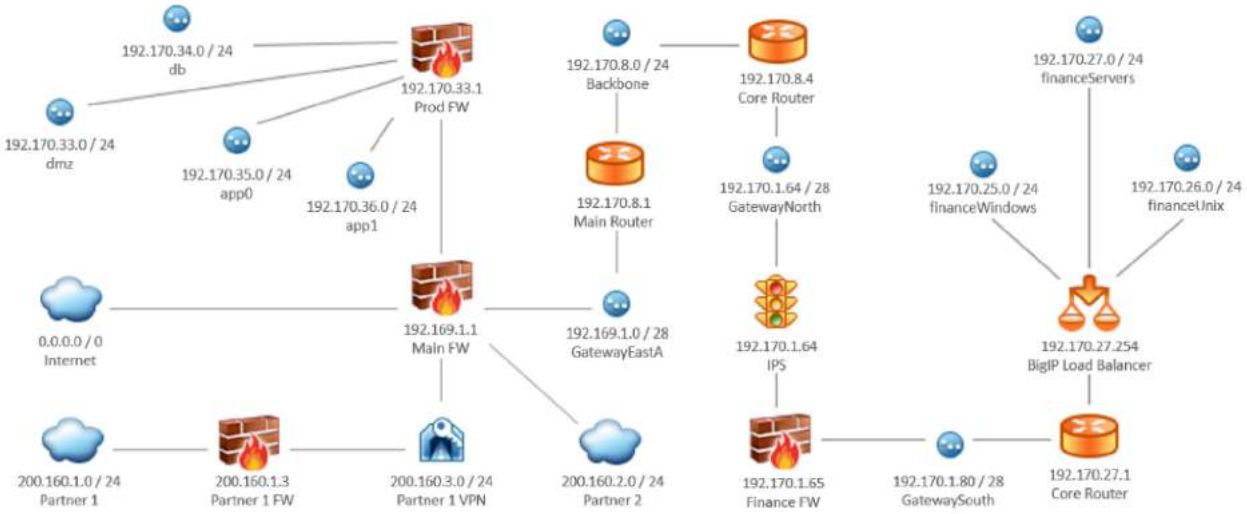
DI.GI. International
Infrastructure Solutions
Information Security
Digital Innovation

SKYBOX SECURITY

SKYBOX VIEW ENTERPRISE SUITE

Prevenire potenziali attacchi informatici richiede il continuo monitoraggio e la valutazione dei livelli di sicurezza di ciascun elemento della rete; attività che è molto onerosa da effettuare manualmente, a causa della enorme quantità di informazioni, parametri di configurazione e cambiamenti continui. Occorrono soluzioni che, invece di aggiungere complessità, semplifichino e riducano il lavoro, aiutando i tecnici a focalizzarsi esclusivamente sui casi critici. Per ridurre al minimo i rischi, è necessario avere una visibilità continua della rete, un aggiornamento costante delle vulnerabilità e delle minacce e un analizzatore automatico ad elevate prestazioni.

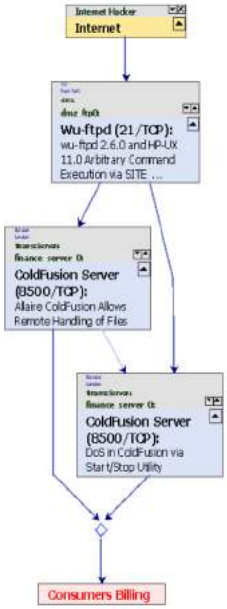
Skybox Security è la soluzione che aiuta le organizzazioni IT ad individuare i percorsi e le vulnerabilità sfruttabili, a dare la giusta priorità ai rischi per la sicurezza e a verificare la reale esposizione per ciascuna vulnerabilità. Skybox Security è la tecnologia che consente di ottimizzare gli investimenti in sicurezza, riducendo il tempo impiegato nei controlli e focalizzando l'attenzione dei responsabili ICT sulle sole vulnerabilità realmente a rischio. La tecnologia Skybox nasce per fare prevenzione, individuando ed evidenziando fra le migliaia di vulnerabilità potenziali che un'infrastruttura può esporre, solo quelle effettivamente sfruttabili.



VULNERABILITY CONTROL (VC)

La migliore soluzione per il governo delle vulnerabilità, che combina le capacità di scoprirne di nuove, attribuirne automaticamente la priorità di gestione di quelle individuate e guidare le attività di remediation:

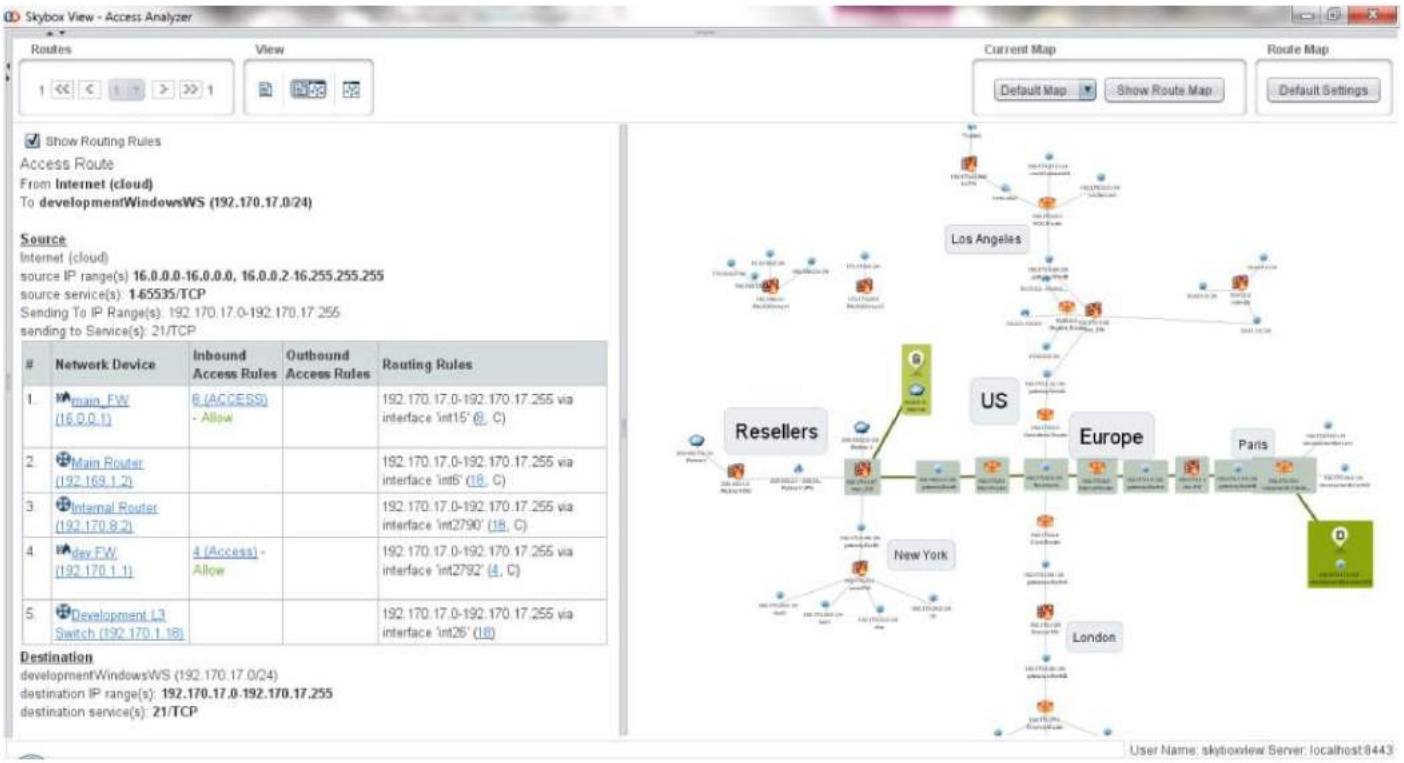
- Integra le vulnerabilità riscontrate da Vulnerability Scanner di terze parti e le posiziona nel modello simulato dell'infrastruttura di rete;
- Tramite la tecnologia esclusiva di Skybox, denominata "Vulnerability Detector", individua le vulnerabilità presenti su host e workstation senza alcuna invasività, a partire dai repository delle configurazioni;
- Utilizza le capacità di modellazione e simulazione, per individuare i path di attacco;
- Simula scenari di attacco da minacce esterne o interne, mettendo in evidenza possibili vie di sfruttamento da parte di hacker, APT, malware e minacce interne, considerando tutti i controlli di sicurezza di rete come firewall, sistemi di prevenzione delle intrusioni e percorsi di routing (Fw rules, ACL, routing, NAT, VPN, Load Balancer, Switch, Proxy, IPS…);
- Tiene conto di apparati IPS e delle signature abilitate per la mitigazione delle vulnerabilità esposte;
- Fornisce una pesatura del rischio sulla base di: CVE, percorso di exploit, classificazione dell'asset software, evidenziando le vulnerabilità più critiche da risolvere con urgenza;
- Favorisce la mitigazione del rischio presentando le possibili alternative di remediation;
- Consente di ridurre drasticamente il numero delle vulnerabilità sulle quali operare perché evidenzia solo quelle effettivamente sfruttabili;
- Calcola indicatori di rischio, analisi del trend, SLA per l'intera infrastruttura o per singoli asset;
- Presenta una console di gestione con ampio uso di grafiche interattive;
- Mette a disposizione un robusto sistema di reporting;
- Consente analisi di tipo "what-if" e "forensic" per simulare i comportamenti e gli impatti sui cambiamenti.



NETWORK ASSURANCE (NA)

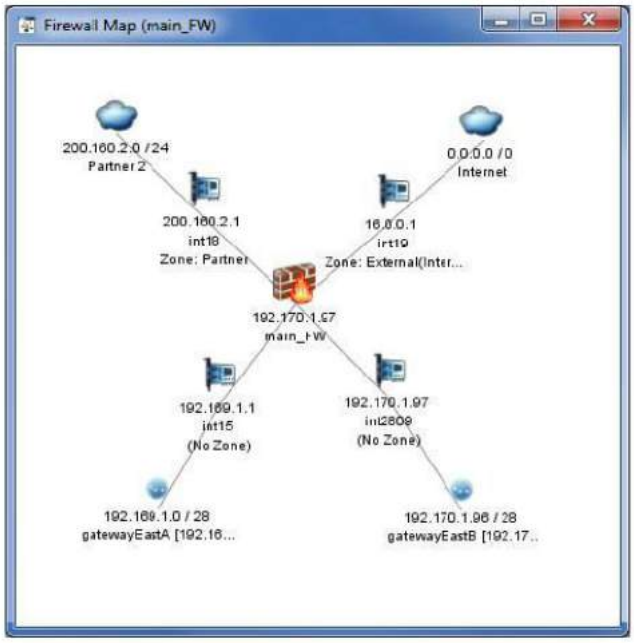
Fornisce una visibilità senza precedenti sulla topologia di rete, la configurazioni dei dispositivi e la conformità alle policy di accesso:

- Realizza una modellazione virtuale della topologia della rete e una simulazione delle logiche di percorrenza tenendo conto di: Fw rules, ACL, routing, NAT, VPN, Load Balancer, Switch, Proxy...;
- Offre una rappresentazione grafica interattiva della topologia della rete con esplorazione tramite drill-down e drill-up;
- Offre visibilità di tutta la struttura di rete, comprese le reti perimetrali e di accesso, evidenziando sia i problemi di sicurezza, che analizzando i problemi di accesso alla rete;
- Analizza i percorsi di rete evidenziando protocolli, porte e indirizzi IP, rispondendo in modo interattivo alle richieste di percorrenze da un qualsiasi elemento sorgente ad un qualsiasi elemento di destinazione;
- Consente la classificazione della rete in zone per ottenere in automatico la Access Compliance;
- Trova eventuali blocchi su rule dei firewall o segmenti non connessi;
- Controlla la compliance delle configurazioni;
- Permette di studiare i percorsi di rete permessi/bloccati per sfruttare le vulnerabilità esposte.

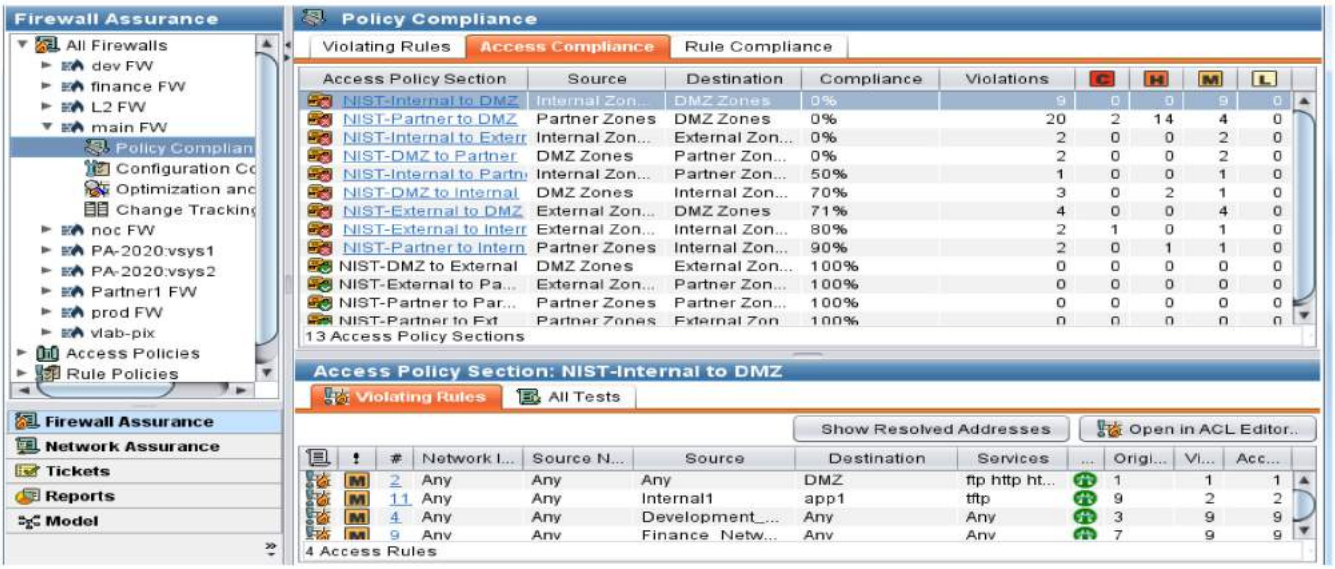


FIREWALL ASSURANCE (FA)

Il modo più efficace per trovare problemi di sicurezza e ottimizzare l'utilizzo dei Firewall esterni e interni. Supporta il più completo elenco di produttori di firewall (compresi i firewall legacy attraverso API del prodotto):



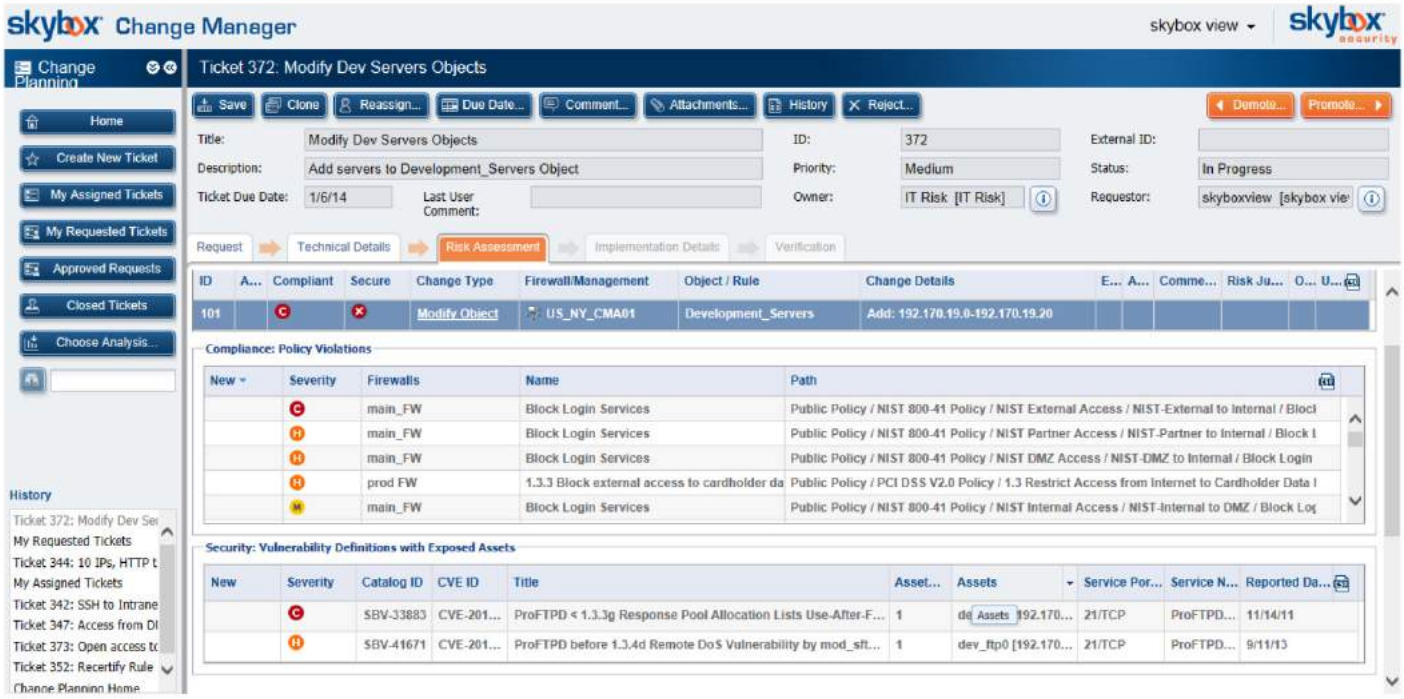
- importa automaticamente i dati di configurazione dei firewall e controlla regole, conflitti e errori di configurazione;
- permette di ottimizzare le rule attive evidenziando sia quelle Shadowed, che quelle ridondanti;
- controlla ed evidenzia le rules che non rispettano le access policy definite;
- Controlla ed evidenzia la compliance rispetto a best practice, regulation e custom policies comprendendo: PCI DSS, NIST, SOX, ISO, NSA, NERC e FISMA con il supporto di un sistema di reporting;
- Access compliance a livello applicativo;
- Fornisce un'analisi comparata fra le firme e le minacce attive sugli apparati IPS supportati;
- Consente la classificazione delle interfacce in zone per ottenere in automatico la Access Compliance;
- Tiene traccia delle modifiche apportate alle regole/oggetti del firewall grazie alla grafica di supporto per comparazioni di configurazioni su base temporale e fra FW diversi;
- È integrato con Skybox Change Manager (tramite API anche con strumenti di terze parti) per una gestione attraverso un processo controllato di workflow controllato;



CHANGE MANAGER (CM)

Skybox Change Manager aggiunge funzionalità di workflow a Skybox Firewall Assurance per gestire, in modo completo e controllato, le attività di modifica delle configurazioni dei firewall.
Change Manager consente agli amministratori dei firewall di monitorare in continuo le configurazioni, valutare i rischi e gestire centralmente tutte le richieste di modifica dei firewall.
Gli utenti finali possono inoltrare richieste di modifica con l'apertura di un ticket, per nuove connessioni o accesso alle applicazioni. La richiesta di modifica segue quindi un ciclo controllato fino a soluzione.
Le principali funzionalità del Change Manager sono:

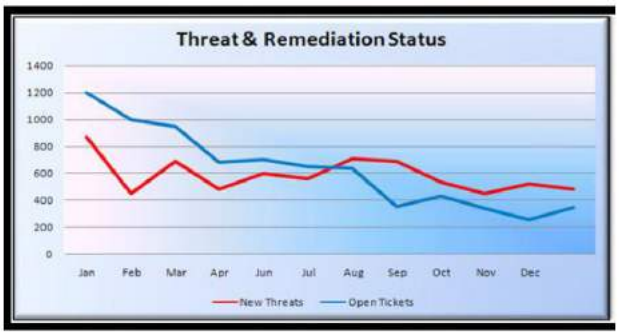
- Presenza di processi di workflow precostituiti su casi di uso generalizzabili;
- Possibilità di personalizzazione dei workflow esistenti e/o realizzazione di nuovi tramite semplice interfaccia grafica;
- Individuazione dei FWs impattati in modalità Network Mode, secondo le reali logiche di percorrenza tenendo conto di: Fw rules, ACL, routing, NAT, VPN, Load Balancer, Switch, Proxy…
- Proposta di modifica e/o creazione di rule nell'ottica di mantenere una adeguata ottimizzazione dei singoli FWs;
- Analisi preventiva della compliance di accesso/segregazione;
- Analisi di sicurezza per evidenziare nuove vulnerabilità che diventerebbero exploitable se fosse applicata la modifica;
- Verifica automatica fra ticket richiesti ed eseguiti con alert per scostamenti di configurazione ed individuazione delle modifiche non autorizzate.



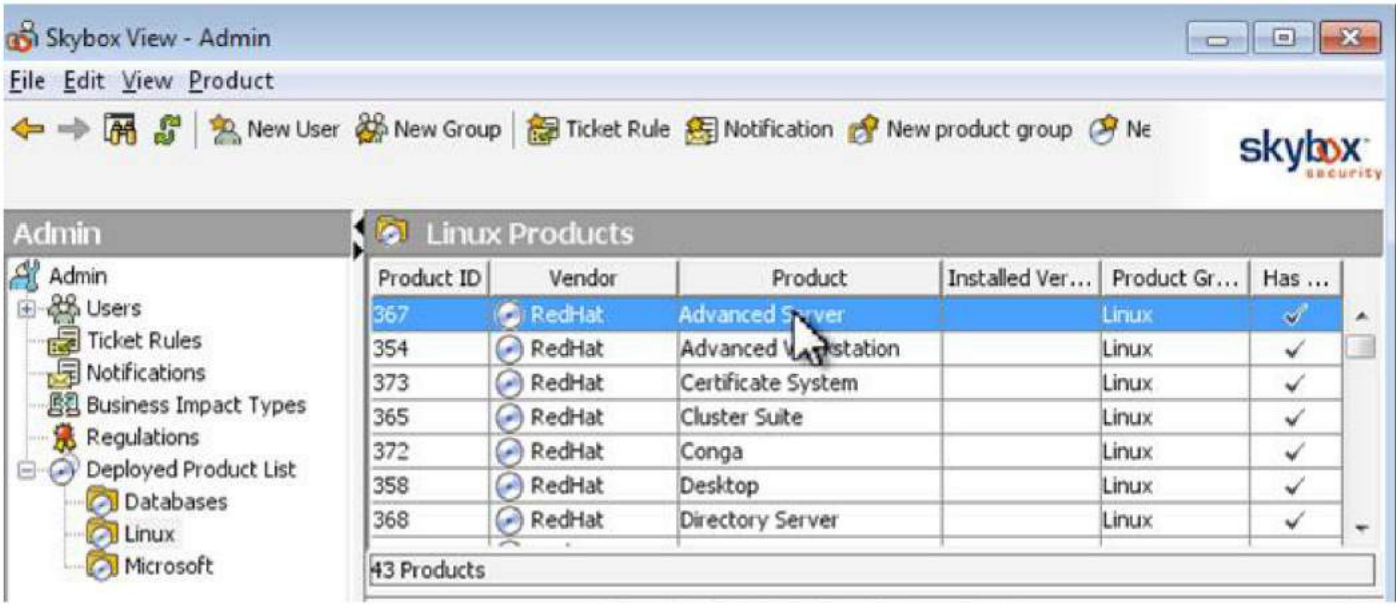
Change Manager assicura che ogni richiesta segua un predefinito processo di approvazione automatizzato, in cui gli amministratori possono valutare la sicurezza, approvare e promuovere una richiesta di cambiamento. Questo flusso di lavoro fornisce ai manager un completo e verificabile controllo su ogni "change request" nella rete e quindi fornisce una dettagliata documentazione per garantire la compliance, risparmiando tempo prezioso.

THREAT MANAGER (TM)

Con Skybox ® Threat Manager è possibile gestire centralmente le minacce acquisite da fonti più disparate, analizzarle in modo tempestivo e avviare rapidamente le più opportune operazioni di remediation.
Skybox Threat Manager è integrato con Skybox Risk Control per gestire facilmente e in continuità, tramite workflow, ciascuna minaccia rilevata da Skybox Risk Control.

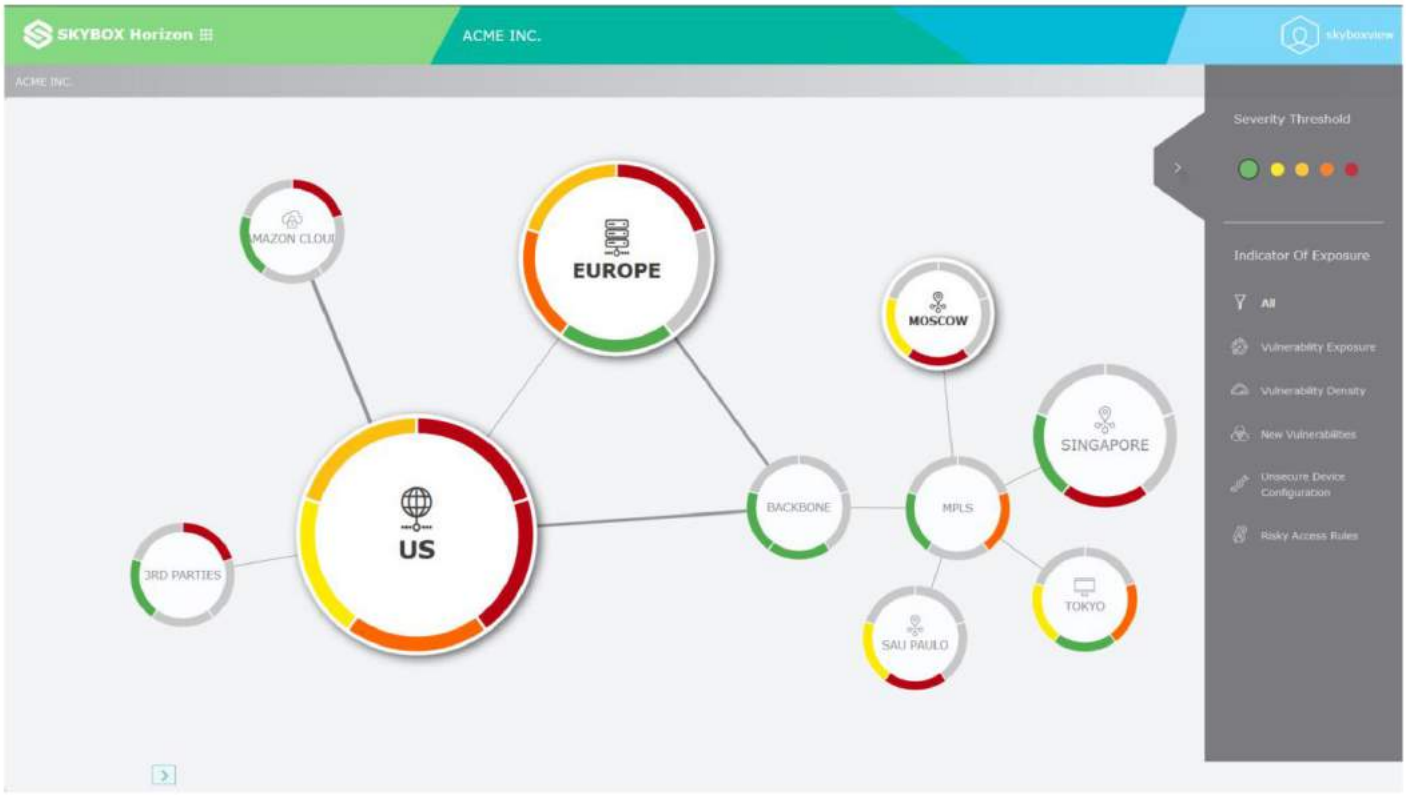


- Gestione in contesto delle nuove minacce (Early Warning);
- Vista esaustiva delle nuove minacce individuate sugli asset aziendali;
- Controllo degli SLA per il Remediation;
- Analisi delle vulnerabilità e dell'impatto sull'infrastruttura;
- Integrazione con fonti di minacce gestite da terze parti - Symantec DeepSight, VeriSign iDefense;
- Gestione del workflow e degli avvisi;
- Classificazione automatizzata della criticità, per ciascuna vulnerabilità, rispetto alle reali minacce per il sistema, in modo che i manager possano rapidamente definire le priorità di intervento;
- Gestione delle minacce tramite un sistema di ticket e workflow integrato;
- Drastica riduzione delle ore uomo spese per attribuire manualmente la priorità alle minacce.



HORIZON

Horizon è un'interfaccia Web che raccoglie e rappresenta in modo intuitivo i dati raccolti dalle analisi dei moduli Skybox; i risultati così presentati sono chiamati Indicators Of Exposure (IOEs). Ogni segmento colorato del singolo nodo rappresenta un IOE.



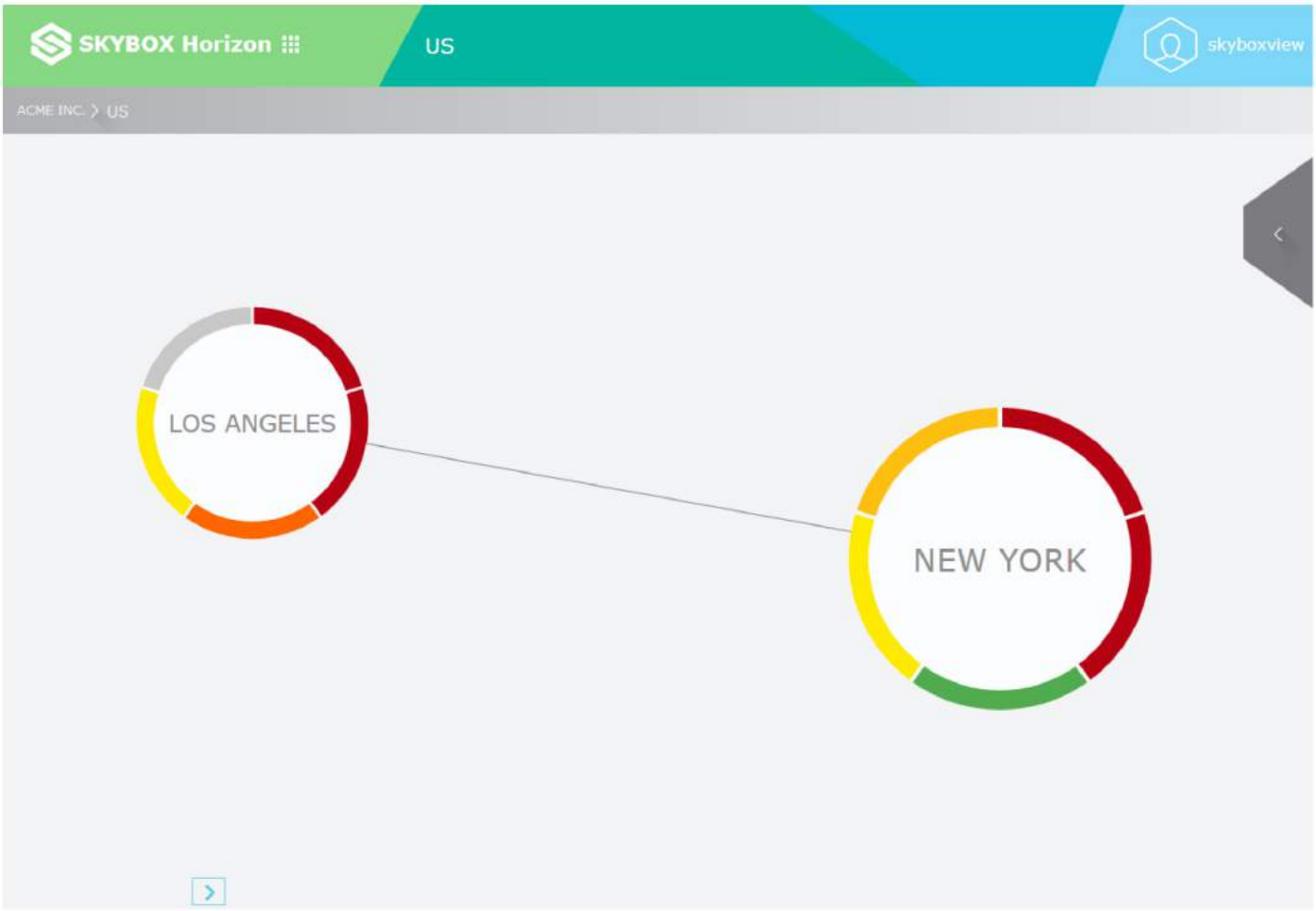
È possibile fare un drill-down facendo click sul singolo nodo:

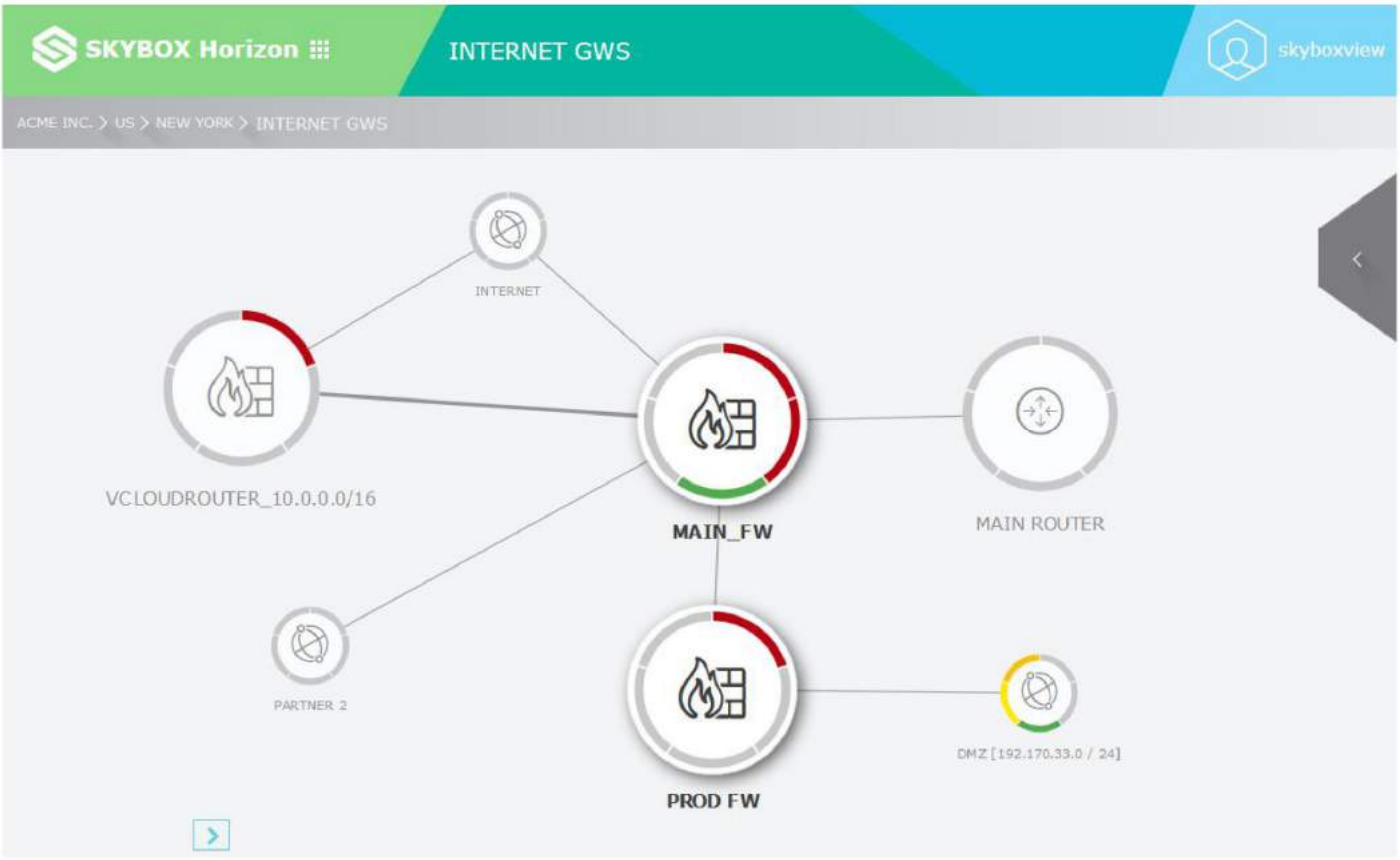
Gli IOS visualizzati rappresentano:

- Risky Access Rules: access rules dei firewall o routers che non sono in linea con la Security Policy dell'azienda;
- Unsecure Device Configurations: problemi di configurazione degli apparati di rete e di sicurezza che non rispettano i requisiti della Configuration Security Policy adottata;
- New vulnerabilities: le nuove vulnerabilità, che sono state riscontrate a carico degli asset e che afferiscono al nodo in esame;
- Vulnerability Density: misura la numerosità delle vulnerabilità che sono state riscontrate a carico degli asset che afferiscono al nodo in esame;
- Vulnerability Exposure: le vulnerabilità che sono state classificate come Exploitable dal modulo VC di Skybox;

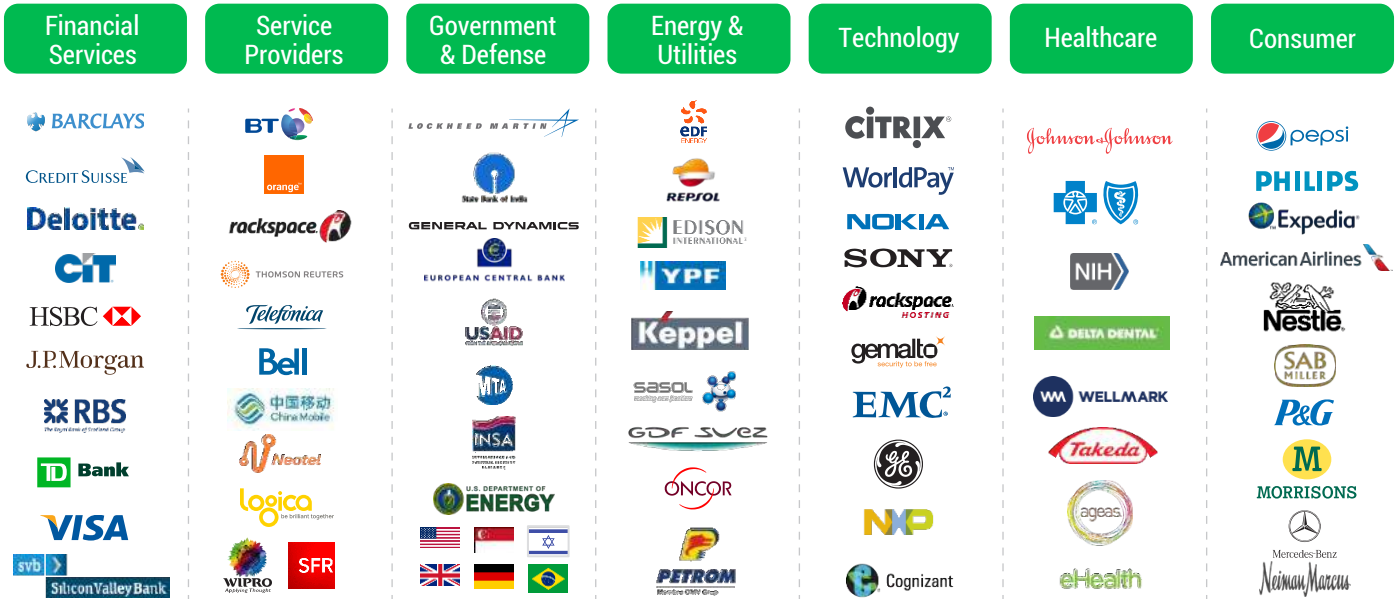
Selezionando ogni singolo segmento colorato è possibile accedere ai dettagli dell'indicatore IOE.

Con facili operazioni di drill-down, selezionando “Site Details”, è possibile percorrere la gerarchia dei nodi navigando fino al singolo asset.





ALCUNI CLIENTI NEL MONDO



LINK UTILI

Skybox Security

http://www.skyboxsecurity.com/

> Skybox Vulnerability Center
http://www.vulnerabilitycenter.com

> Skybox in the news
http://www.skyboxsecurity.com/news

> Skybox Channel on YouTube
http://www.youtube.com/user/SkyboxSecurityVideos

> Skybox supported devices
https://www.skyboxsecurity.com/sites/default/files/Skybox%20Supported%20Devices_0.pdf

DI.GI. International

http://www.digi.it/index.php/information-security

Per ulteriori informazioni o prenotare una dimostrazione:

Carlo Gianini
Country Manager

phone +39 3356171454
carlo.gianini@skyboxsecurity.com
www.skyboxsecurity.com

Francesco Ghezzi
Sales & Marketing - DI.GI. International S.p.A.

phone +39 342 6839661
francesco.ghezzi@digi.it
www.digi.it