Versatility 2024

Remote Browser Isolation

VERSA

Agenda

Versatility 2024

VERSA

Agenda

- Problem to solve
- Versa RBI solution
  - Overview
  - How it works
- Demo
- Conclusion

RBI – Problem to Solve

Challenge

- Browser is the first medium between attackers and enterprises under attack
- Common attacks prevalent in recent years-
  - ***Drive-by-downloads*** where malicious content is automatically downloaded to an endpoint
  - ***Drive-by-compromise*** attacks, a common tactic where a victim visits regular websites that are seeded with malicious content
  - ***Squatted domains*** leading to malicious web pages

Why Current Solutions don't work

- Firewalls, VPNs and other security solutions use *Allow* or *Block* rules which are *all or nothing*
- There is no intermediate solution to provide access in a secure manner
- Issues propagated due to 'all or nothing' access-
  - Initial access through compromised web sites, vulnerable browsers
  - Credential theft, exploitation
  - Data exfiltration

48%

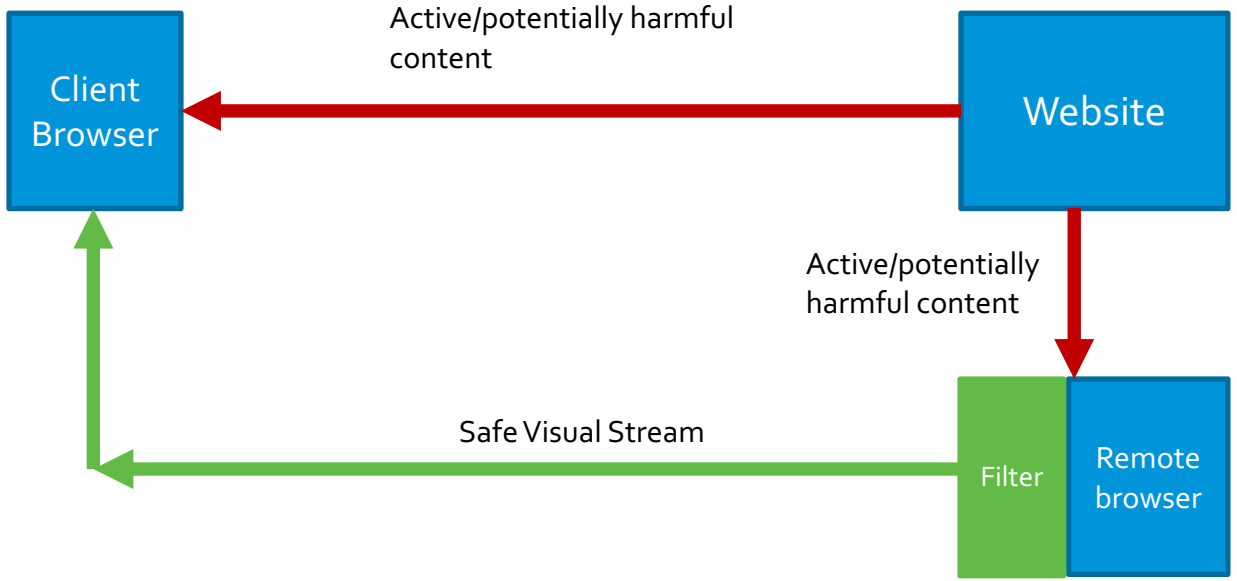
Threats entered the organization by drive-by-downloads, SANS whitepaper

Versa RBI solution

Versatility 2024

Versa RBI solution

- Isolate browsing activity from internal network.
- Browsing activity is executed in a remote, sandboxed environment
- Active content only executes in remote browser
- Only a safe visual stream is relayed to the client browser



VERSA

Versa's RBI solution

Functionality

- Render a visual stream of websites
- Filters harmful content
- Part of the Versa SSE platform
- Tightly integrates with rest of Versa ASC
- Scans client to server and server to client traffic

Actions supported

- Allow/Block uploads and downloads
- Preview downloads: Convert documents to pdf for preview
- Scan uploads and downloads for malware
- Persist first party cookies, block third party ones
- Allow/deny clipboard access

Powered by:

Technology: DOM mirroring

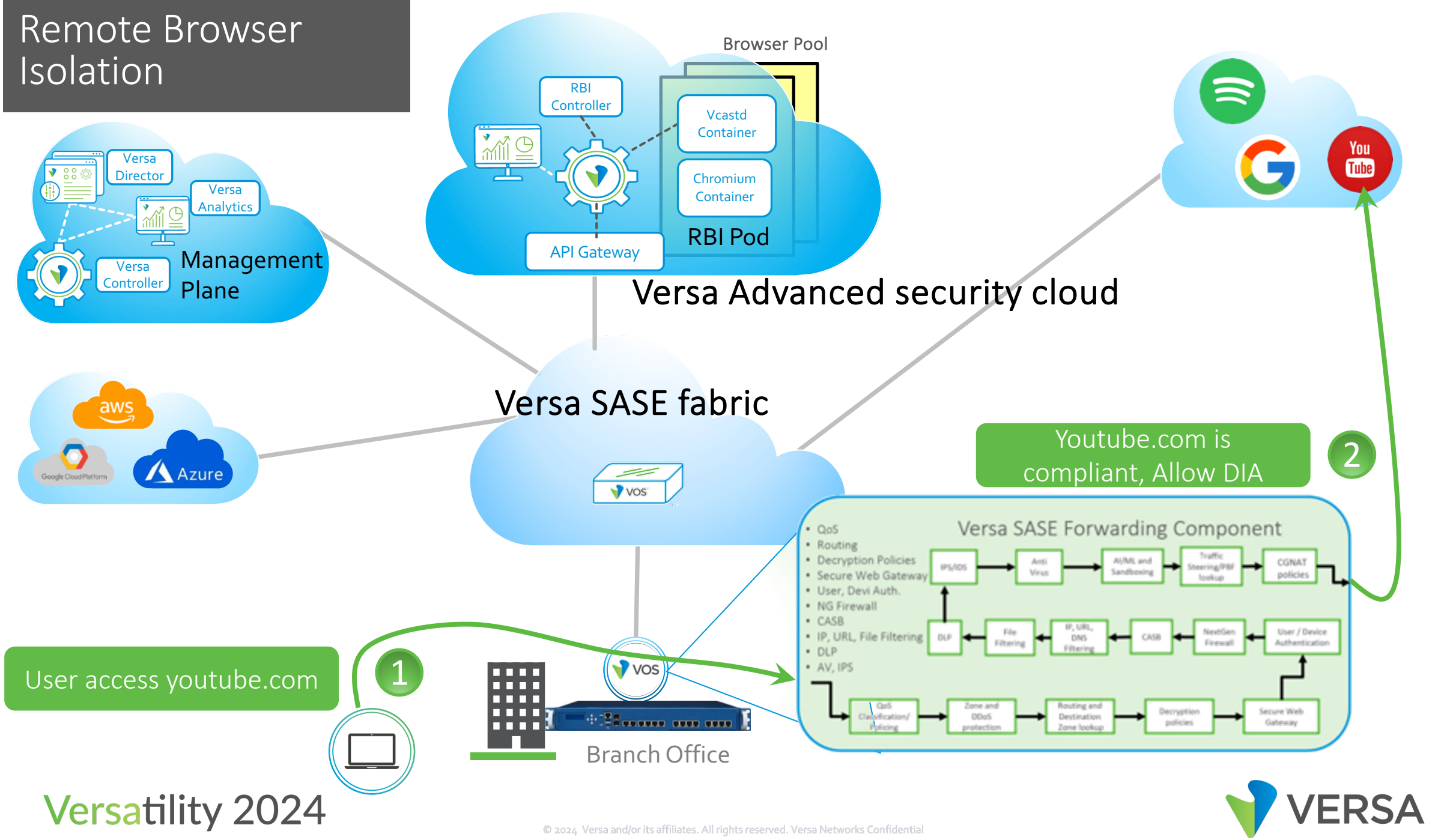
- Remote Browser
- Filters active DOM content
- Streams safe DOM elements to client browser
- Streams audio/video as pixels
- Works with any HTML5 compliant client browser -- Chrome, Edge, Firefox, Safari

Versa RBI: Highly responsive, native experience – the *next best thing* to browsing in real time

Versa RBI - how it works

- Configure real time protection policy on SWG
  - Redirects matching uses browsing sessions to the RBI cluster for secure, isolated access.
  - Same rich policy language used by other security Versa security features.
    - Match based on URL category, reputation
    - Match based on geolocation
    - Match based on user
    - Match based on user and device posture
- Configure RBI data protection rules in Advanced Security Cloud
  - DLP and ATP for files transferred by remote browsers (downloads as well as uploads)

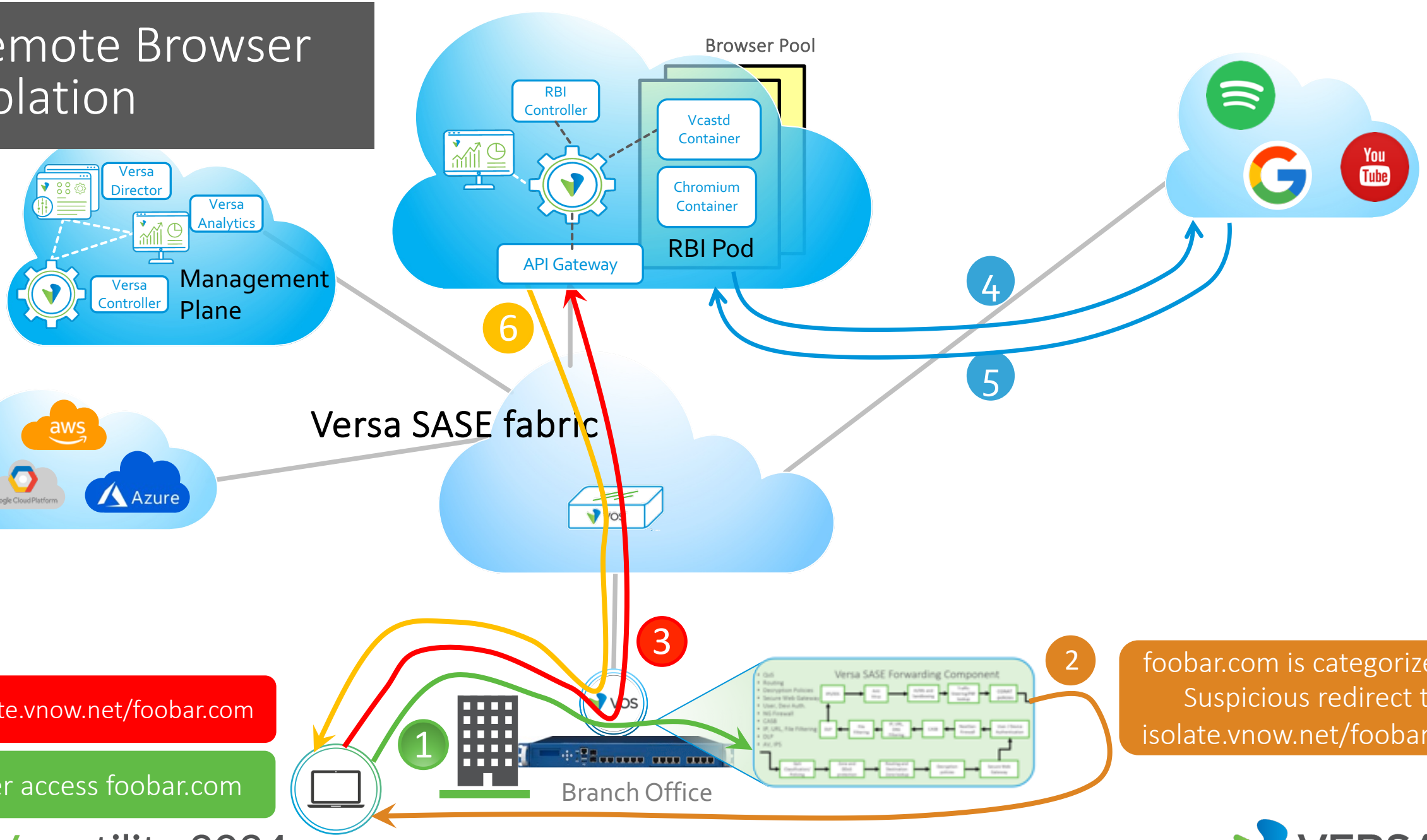
Remote Browser Isolation



Versatility 2024

VERSA

Remote Browser Isolation



Versatility 2024

VERSA

Demo

Versatility 2024

VERSA

Versa RBI - Conclusion

- Improve overall security posture with RBI as a mitigation technique
- Improve productivity with isolation as an intermediate action instead of blocking access.
- Provide differential access to employees and contractors.
- Protect against ransomware attacks.
- Prevent data exfiltration.

Questions

VERSA

Versatility 2024

API-Based Data Protection & Email Protection

VERSA

Agenda

- Why API-Based Data Protection (API-DP)?
- Connectors, SaaS Authorization – Grant Access
- API-DP Policy Rules, Retroactive and Scheduled Scans
- Email Protection – SMTP Proxy
- Monitoring
- Demo

Versatility 2024

VERSA

Why API-Based Data Protection?

Versatility 2024

VERSA

Why API-Based Data Protection (API-DP)?

Challenges

- Inline CASB breaks open TLS and inspect content as a reverse proxy
- However, enterprise SaaS applications are often “certificate pinned”
- Users can access public cloud apps using BYOD or without being behind VPN/corporate firewall
- Need an “out-of-band” mechanism that works directly with SaaS applications through authorized “connectors”

Solution

- Versa’s API-DP, part of the Advanced Security Cloud (ASC) in Secure Service Edge (SSE) platform, secures access from user to application
- Also known as API-Based CASB, out-of-band CASB, offline CASB, etc.

Overview

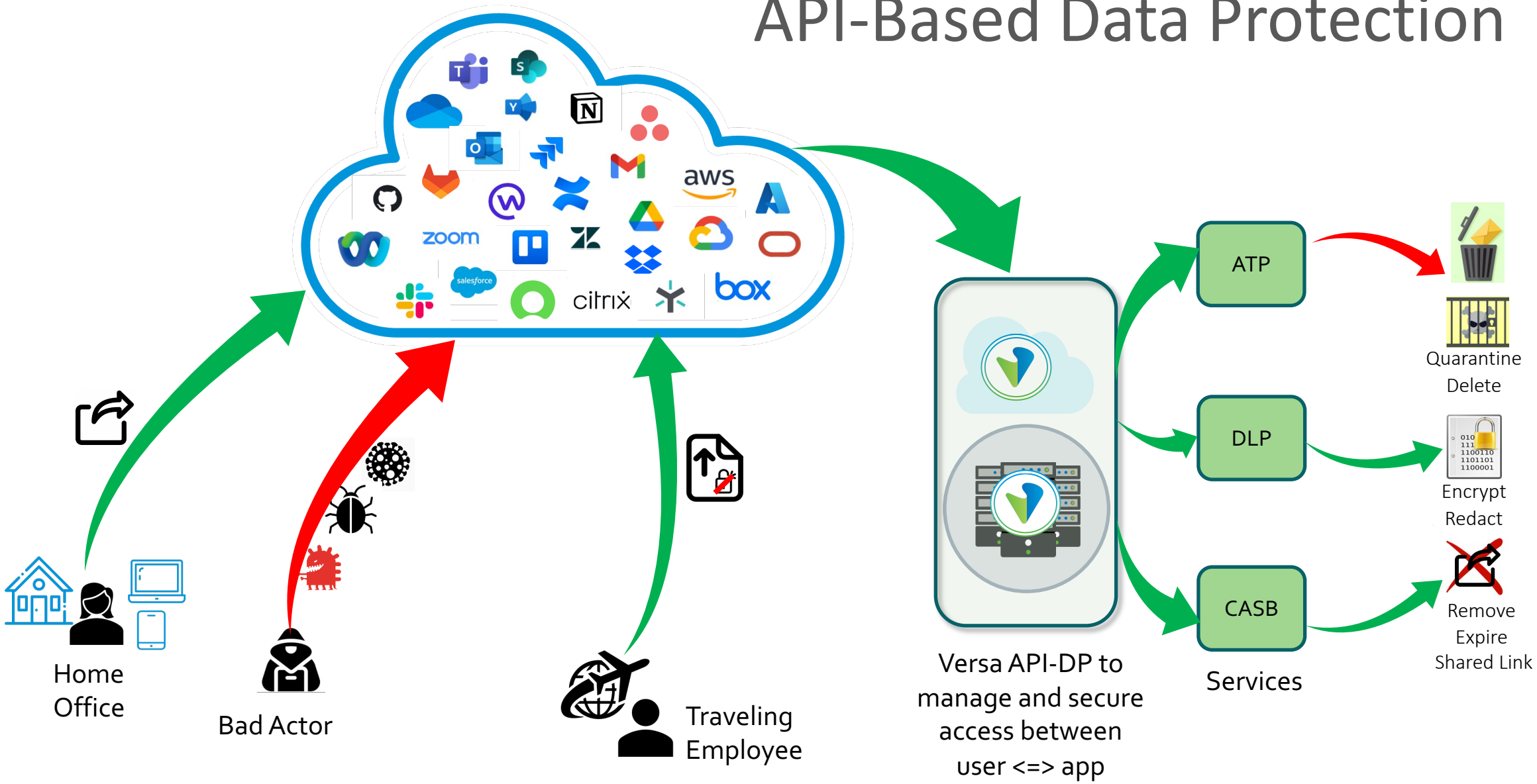
- Protection for File, Email, Instant Messaging, Cloud Infra services
  - Webhooks, Poll Based and Hybrid
  - Retroactive, Scheduled and On-Demand Scan
- Provides policy and access control.
- Run DLP, CASB, Sandbox (Static, Dynamic, AI/ML). Fine-grained control compared to inline CASB
- Encrypt, Redact and other DLP actions
- Quarantine and Legal Hold
- Expire, delete shared links/collaborators. Restrict shared access
- Support for different categories of application like cloud storage, collaboration, email, messaging and source code repositories, CRM, etc.

API-DP Use Cases

Versatility 2024

VERSA

API-Based Data Protection

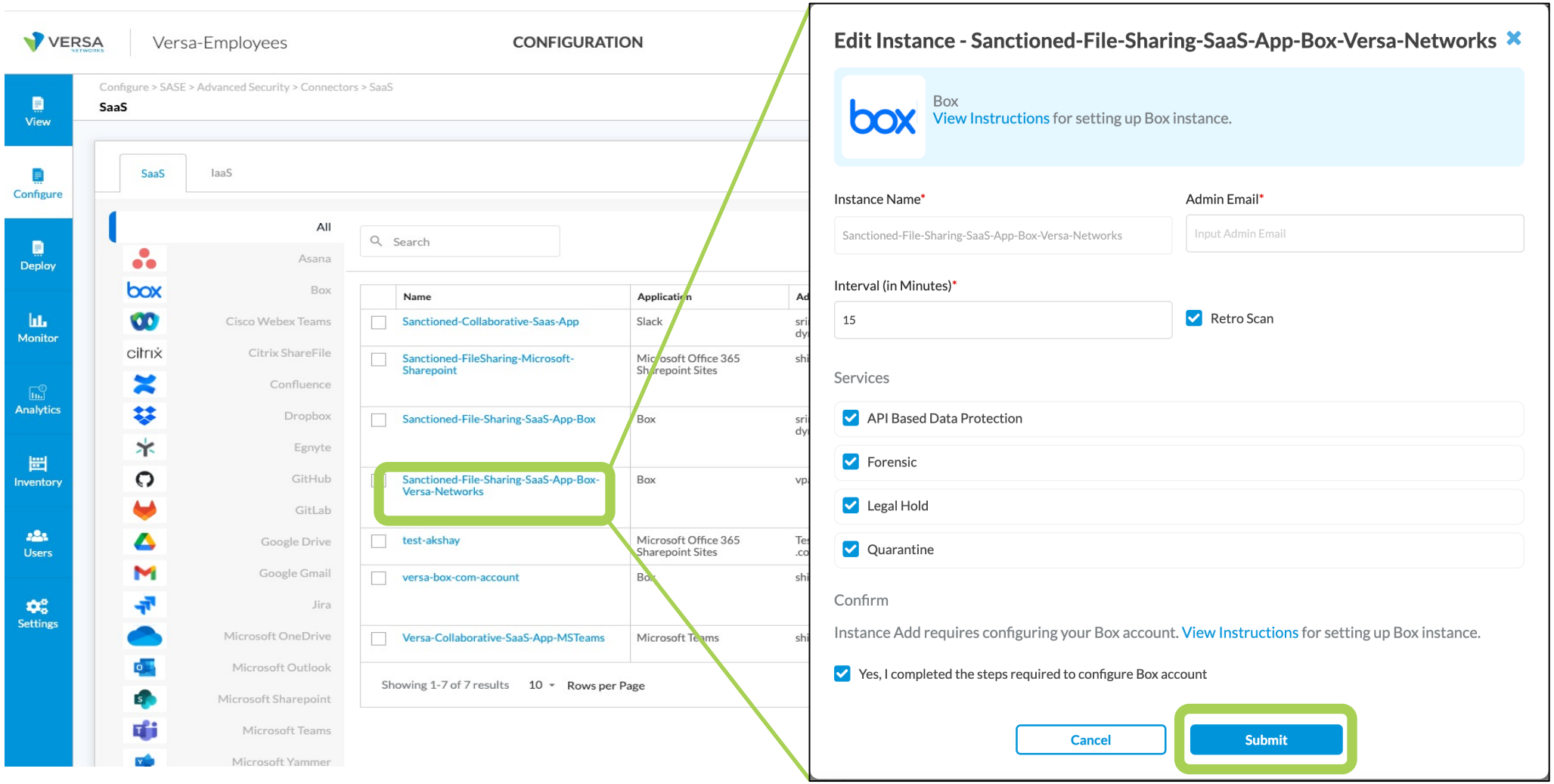


VERSA

Connectors

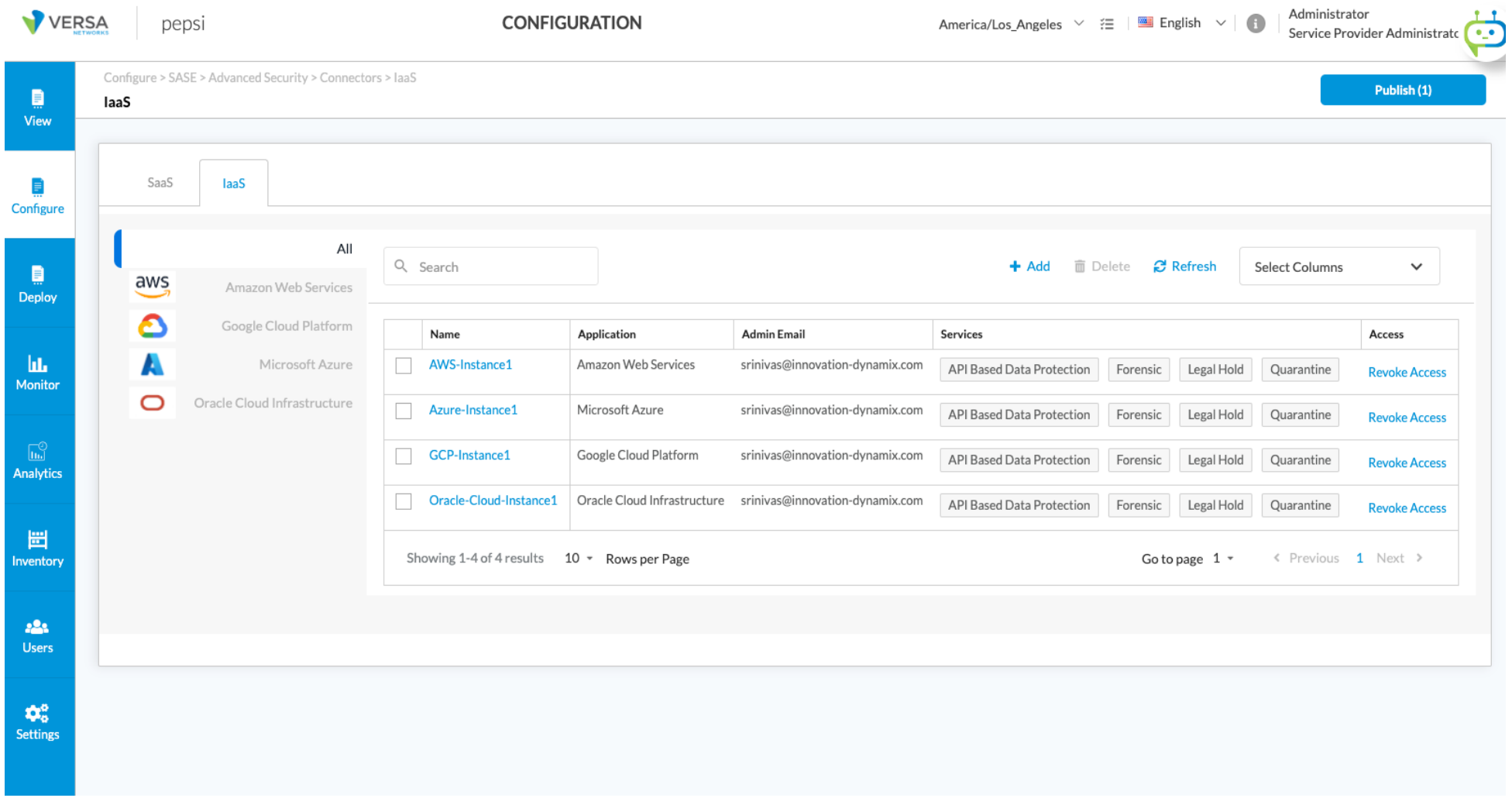
VERSA

SaaS Connectors



VERSA

IaaS Connectors

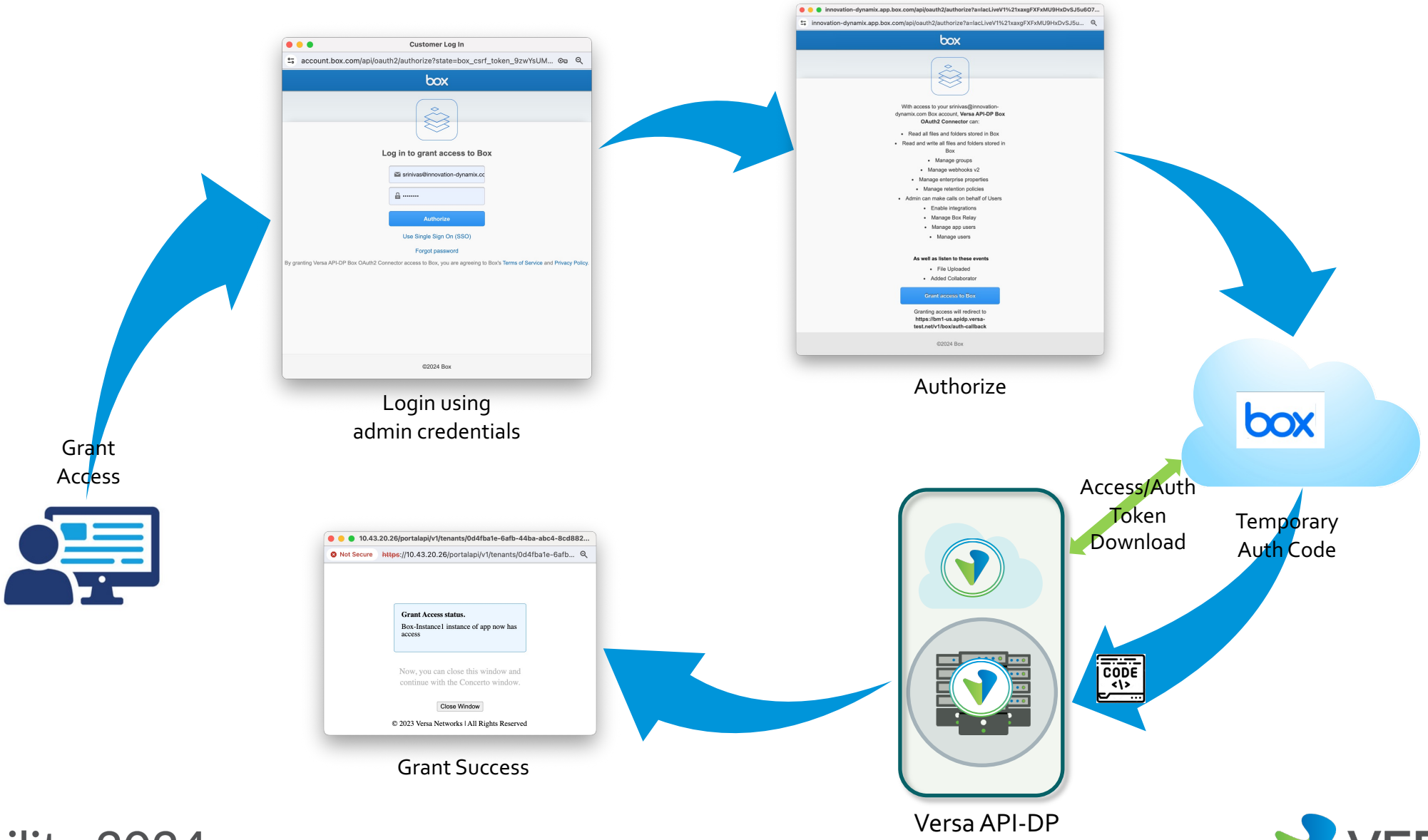


SaaS Authorization

Versatility 2024

VERSA

SaaS OAuth2.0 based Grant Access



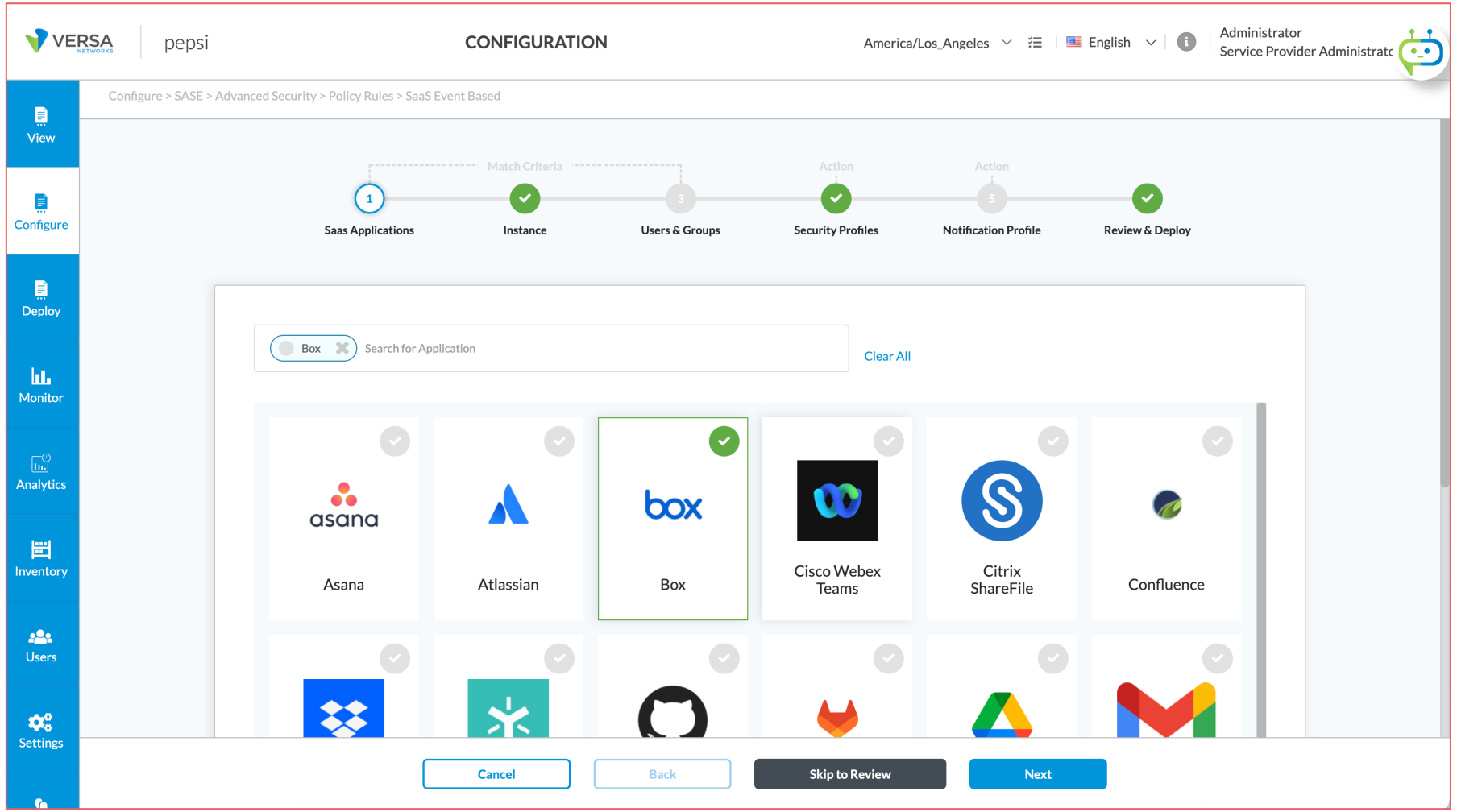
VERSA

Policy Rules

Versatility 2024

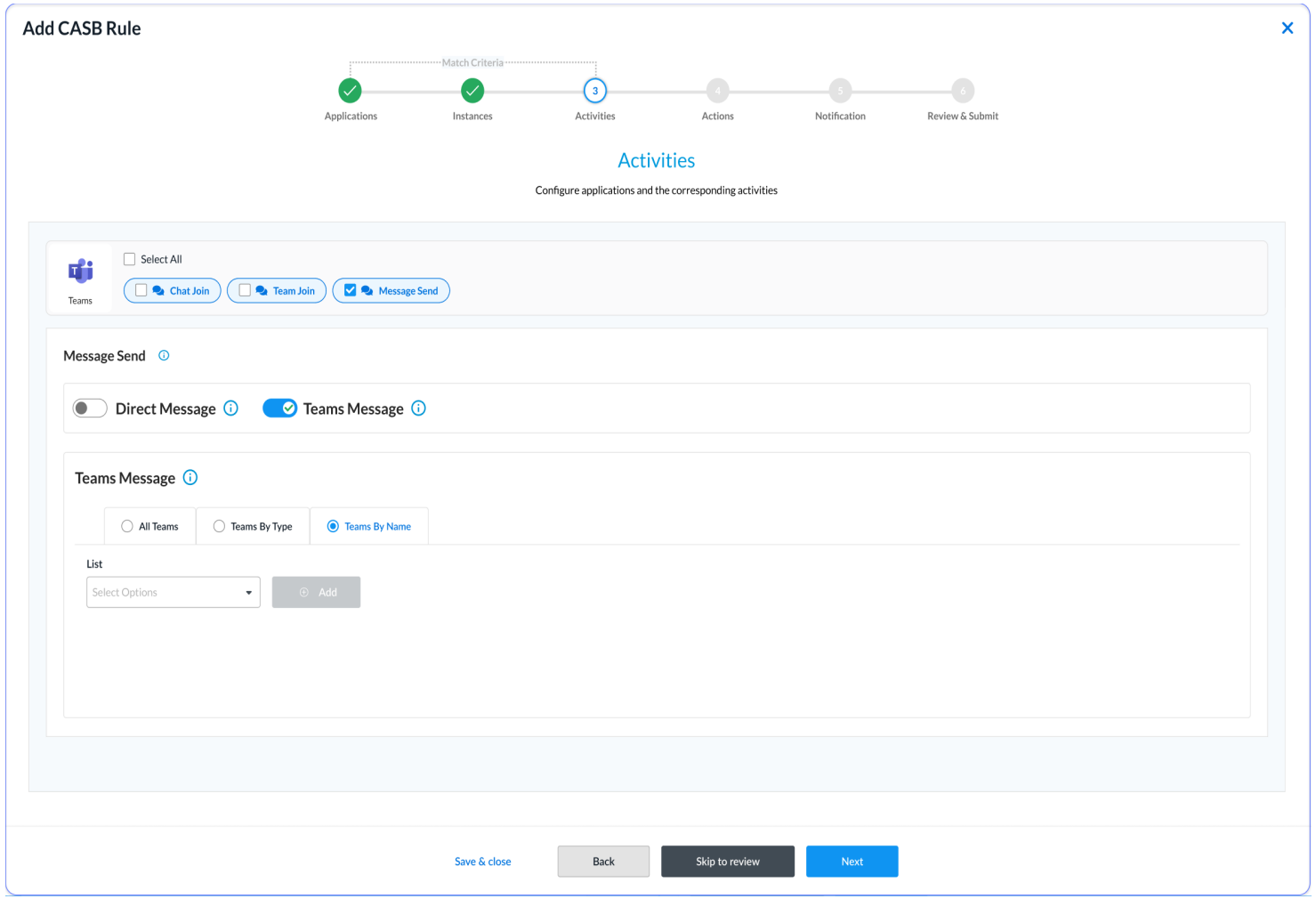
VERSA

API-DP Policy Rule



VERSA

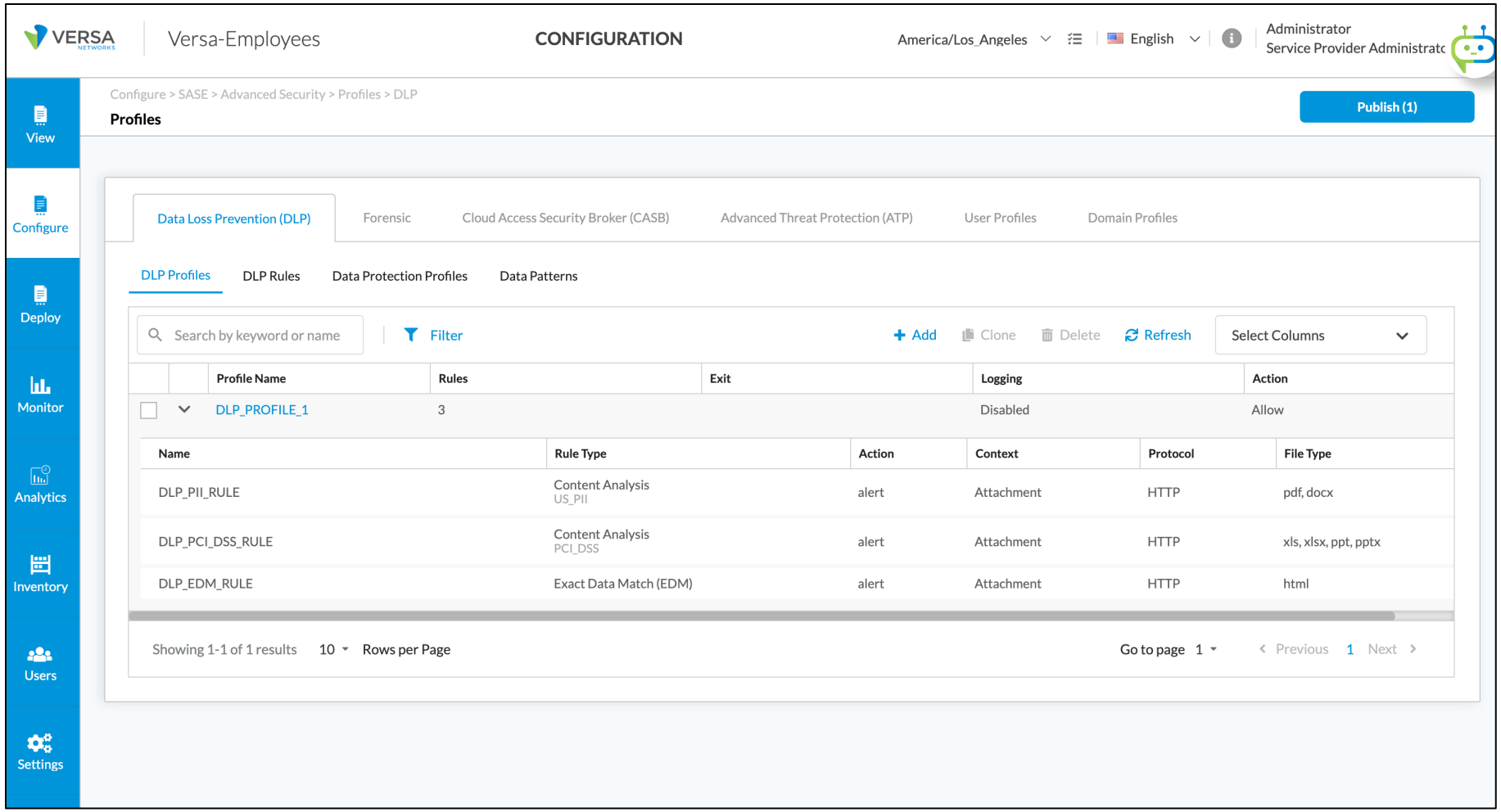
Offline CASB Rule



- Application specific activities and access control
- Fine-grained actions per activity
- Finer control on running DLP and ATP services at the user level or based on application specific activities

VERSA

DLP Profile



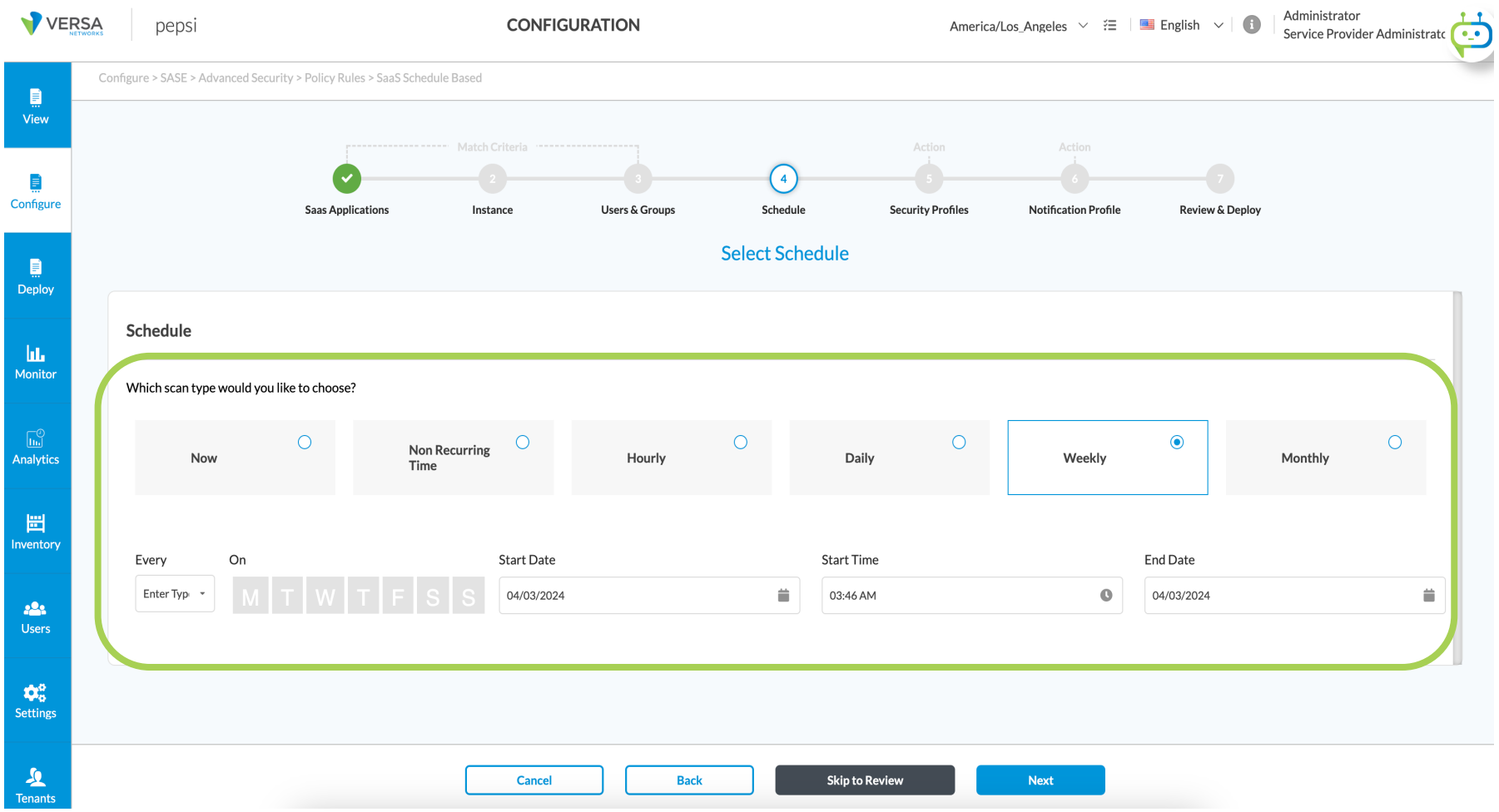
VERSA

Retroactive and Scheduled Scans

Versatility 2024

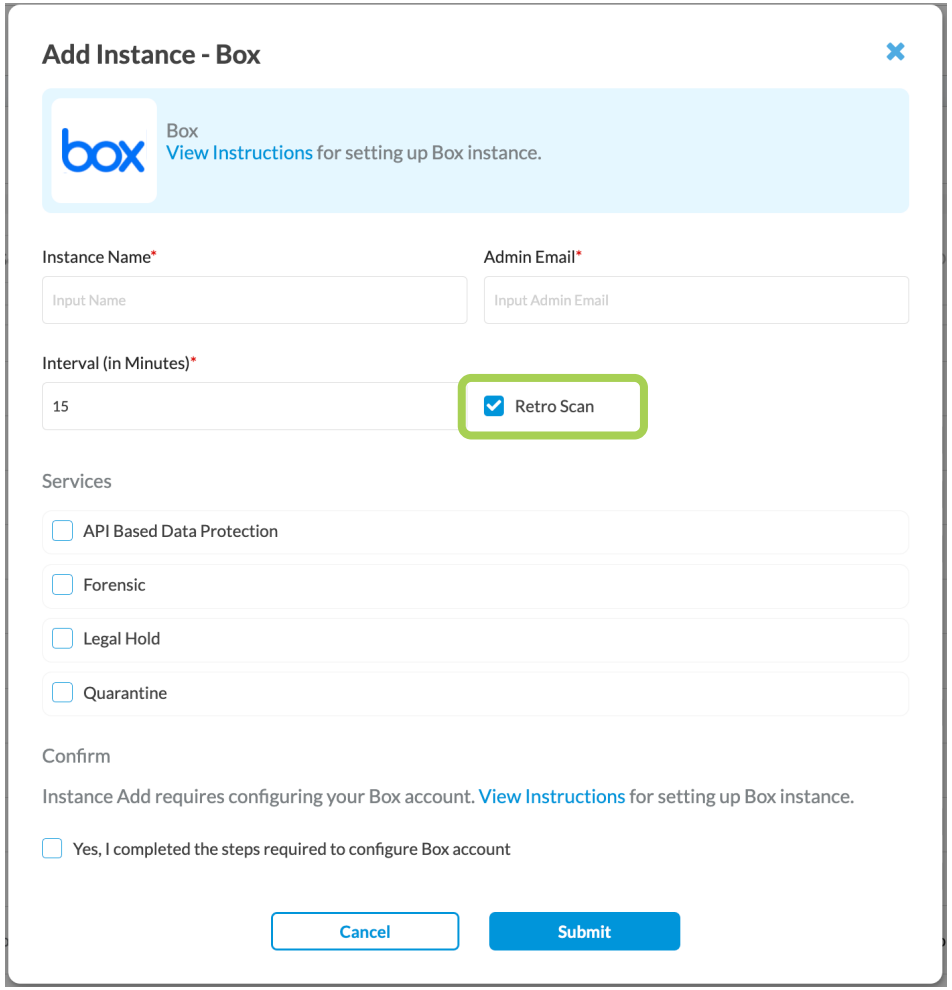
VERSA

Scheduled Job



VERSA

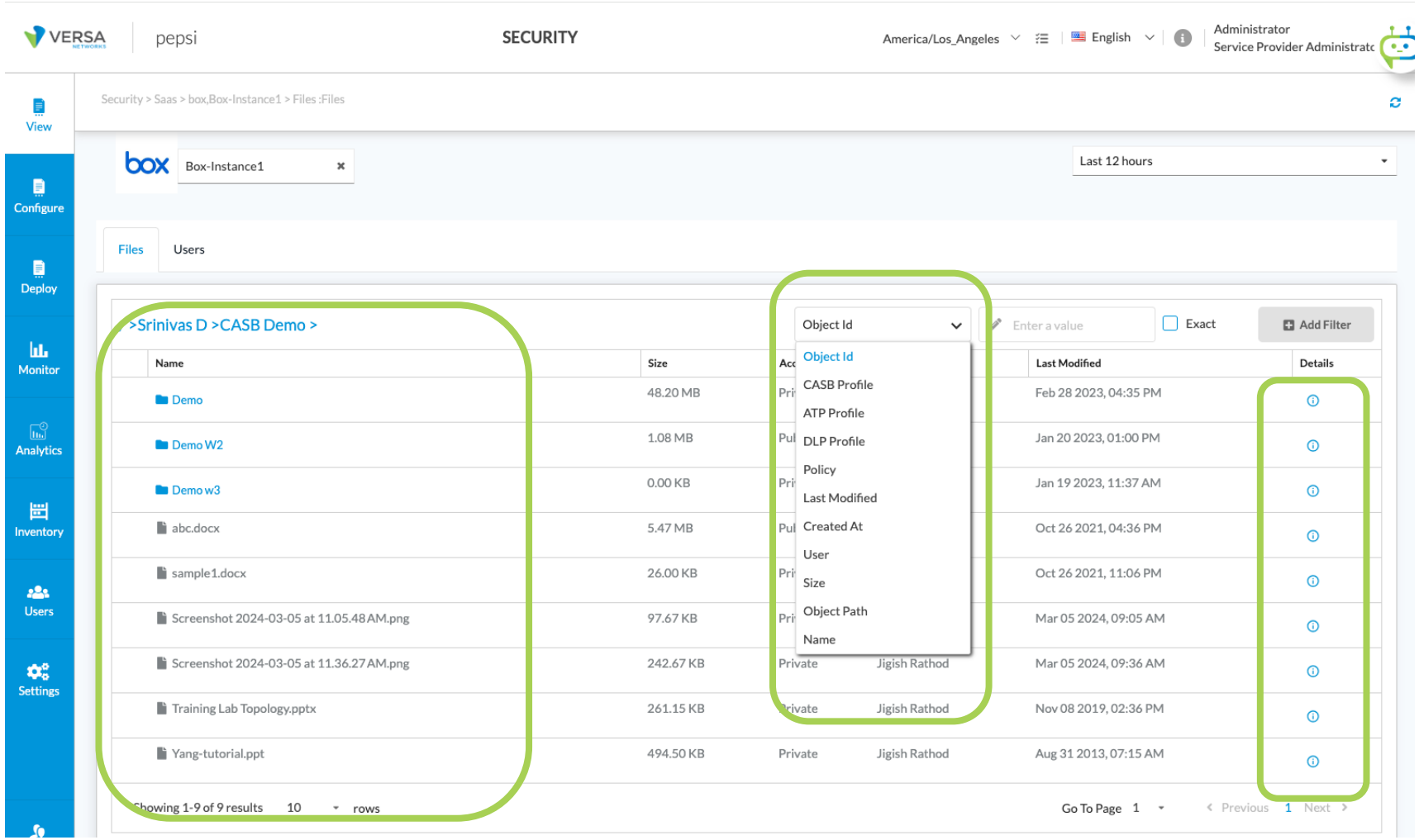
Retroactive Scan



- Retro scan can be enabled during the connector creation.
- Scans historical data at rest existing before using Versa API-DP
- Violation detected will be logged in Analytics

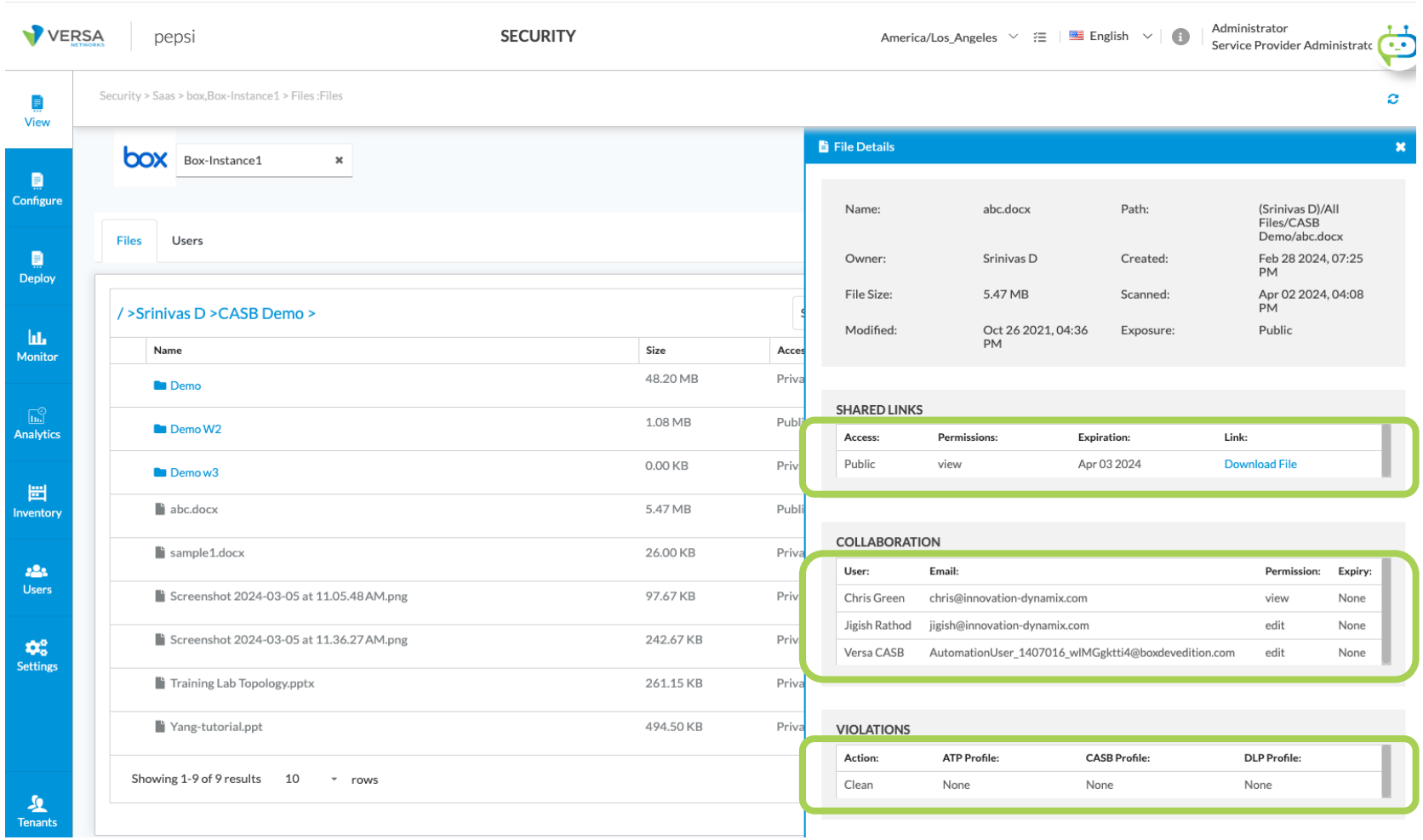
VERSA

Data at Rest



VERSA

Data at Rest



VERSA

Email Protection: SMTP Proxy

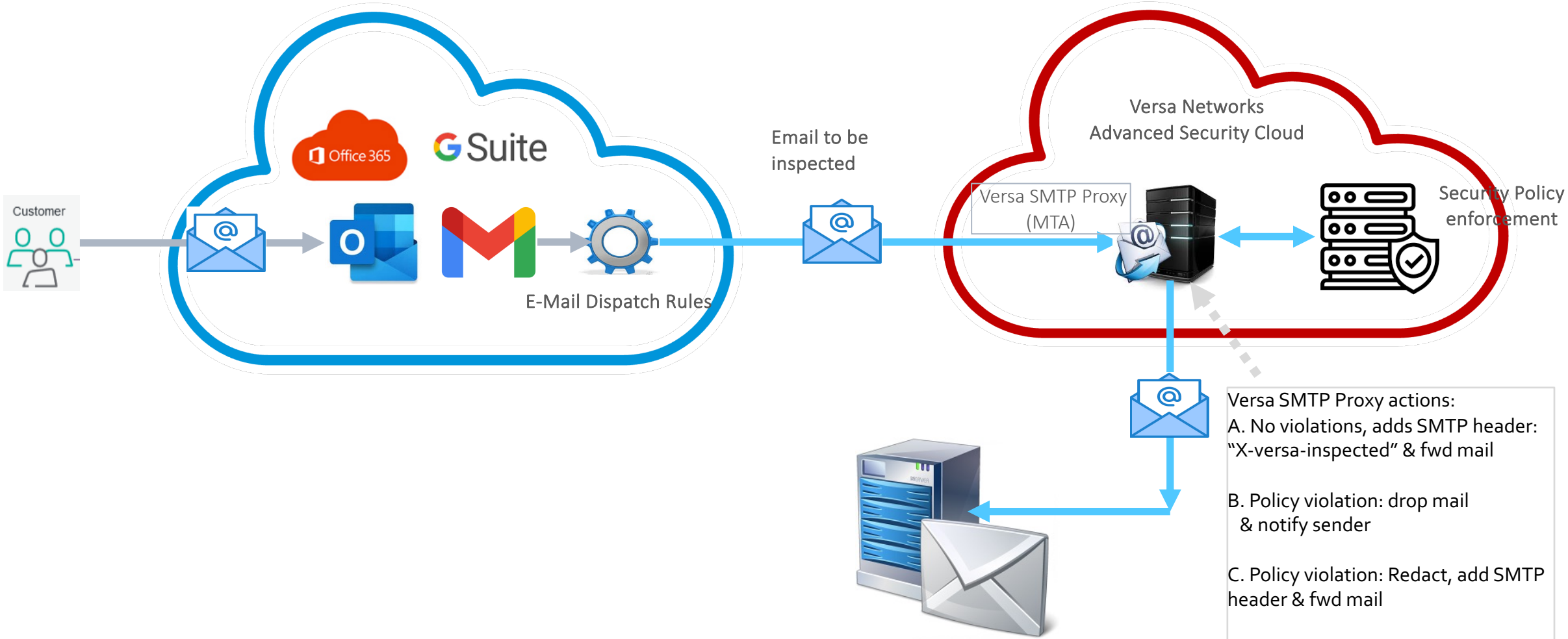
Versatility 2024

VERSA

Email Protection

- SMTP Proxy for Email Protection provides protection for cloud emails (cloud hosted email exchanges: GMAIL or O365 or a custom exchange)
- Design & workflow:
  - Organization/Tenants GMAIL (G-Suite) or O365:
    - Configure outbound connectors to filter/route emails outbound/inbound emails to SMTP proxy
    - Inbound connectors are configured to accept emails SMTP proxy
  - Outbound/inbound email received on the GMAIL/O365 exchanges is forwarded to SMTP Proxy
  - Proxy maps email to tenant specific security enforcement policies (DLP, ATP etc.)
  - Policy specific actions such as forward, redact, drop, notify
  - Inspected header is added, and emails can be routed through the same GMAIL or O365 exchange or any other configured MTA
- Integrated with Analytics

SMTP Proxy & Security Policy Enforcement



Versa SMTP Proxy actions:

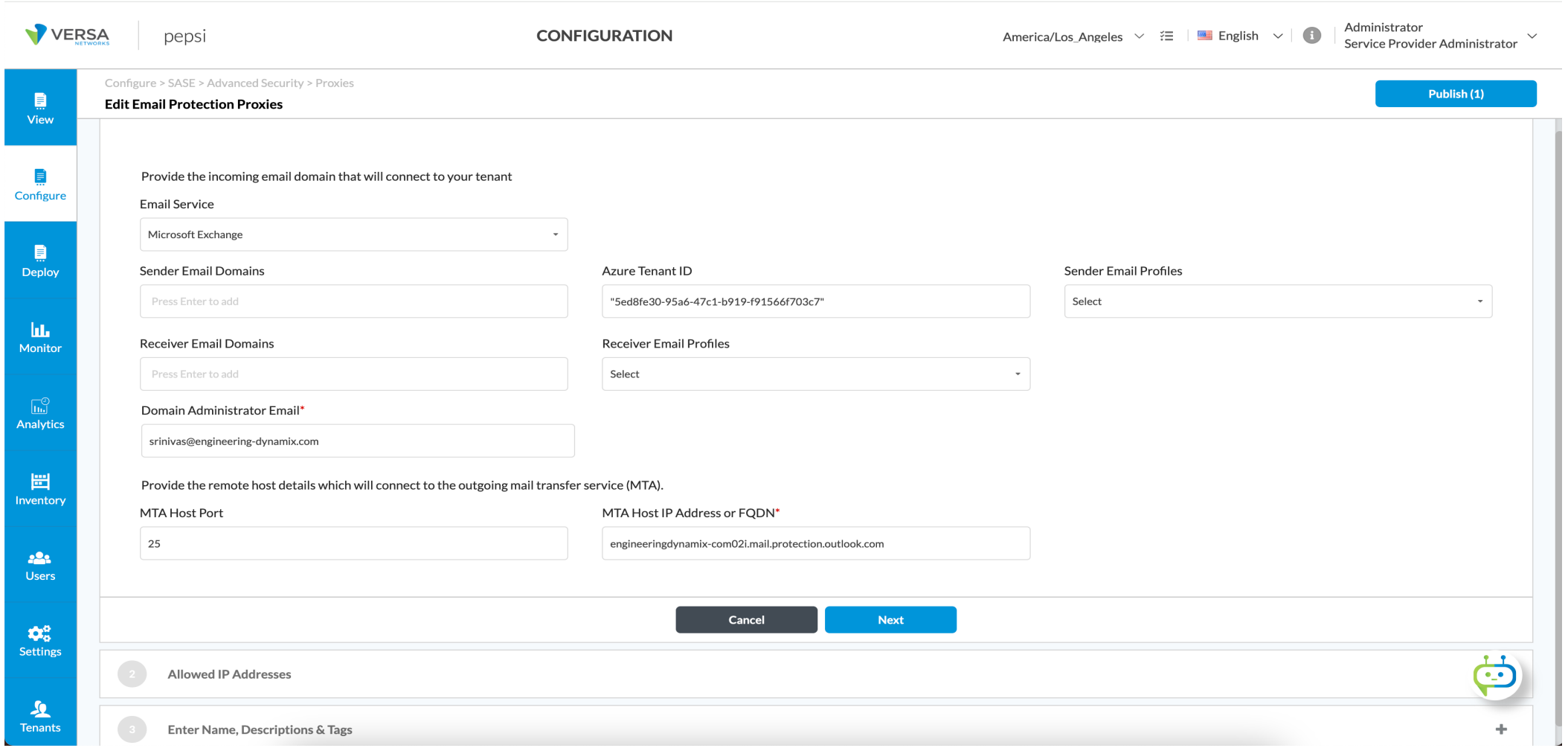
A. No violations, adds SMTP header: "X-versa-inspected" & fwd mail

B. Policy violation: drop mail & notify sender

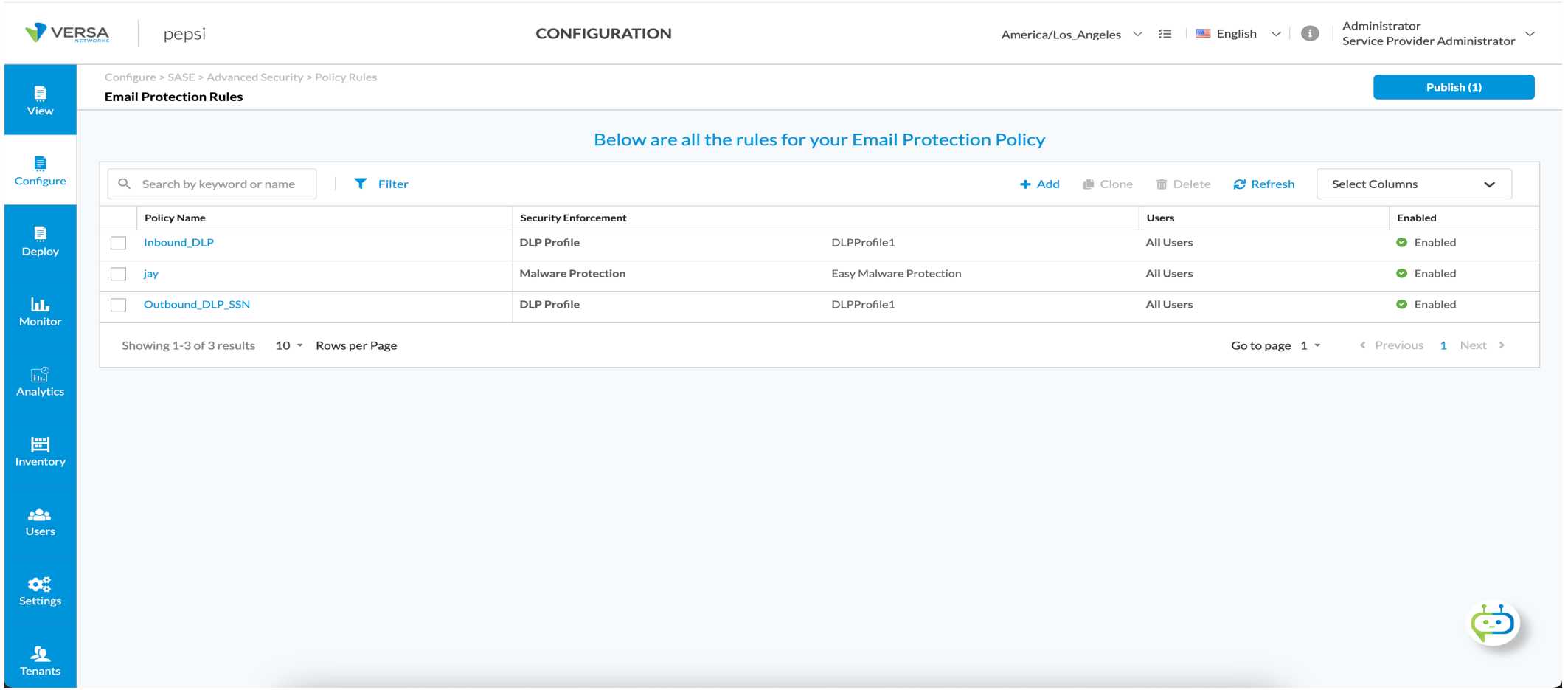
C. Policy violation: Redact, add SMTP header & fwd mail

VERSA

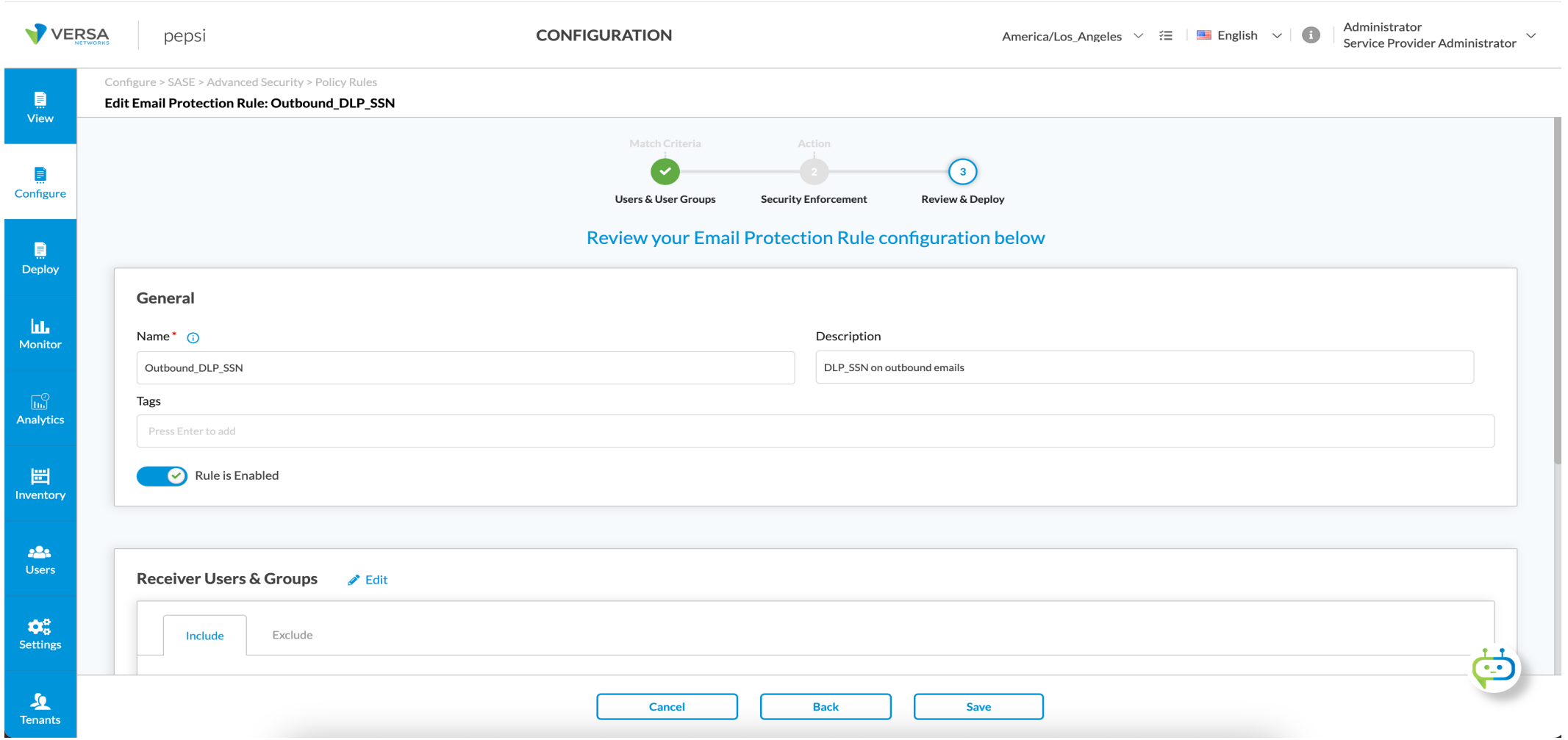
Email Protection: SMTP Proxy Configuration



Email Protection: Policy Detail



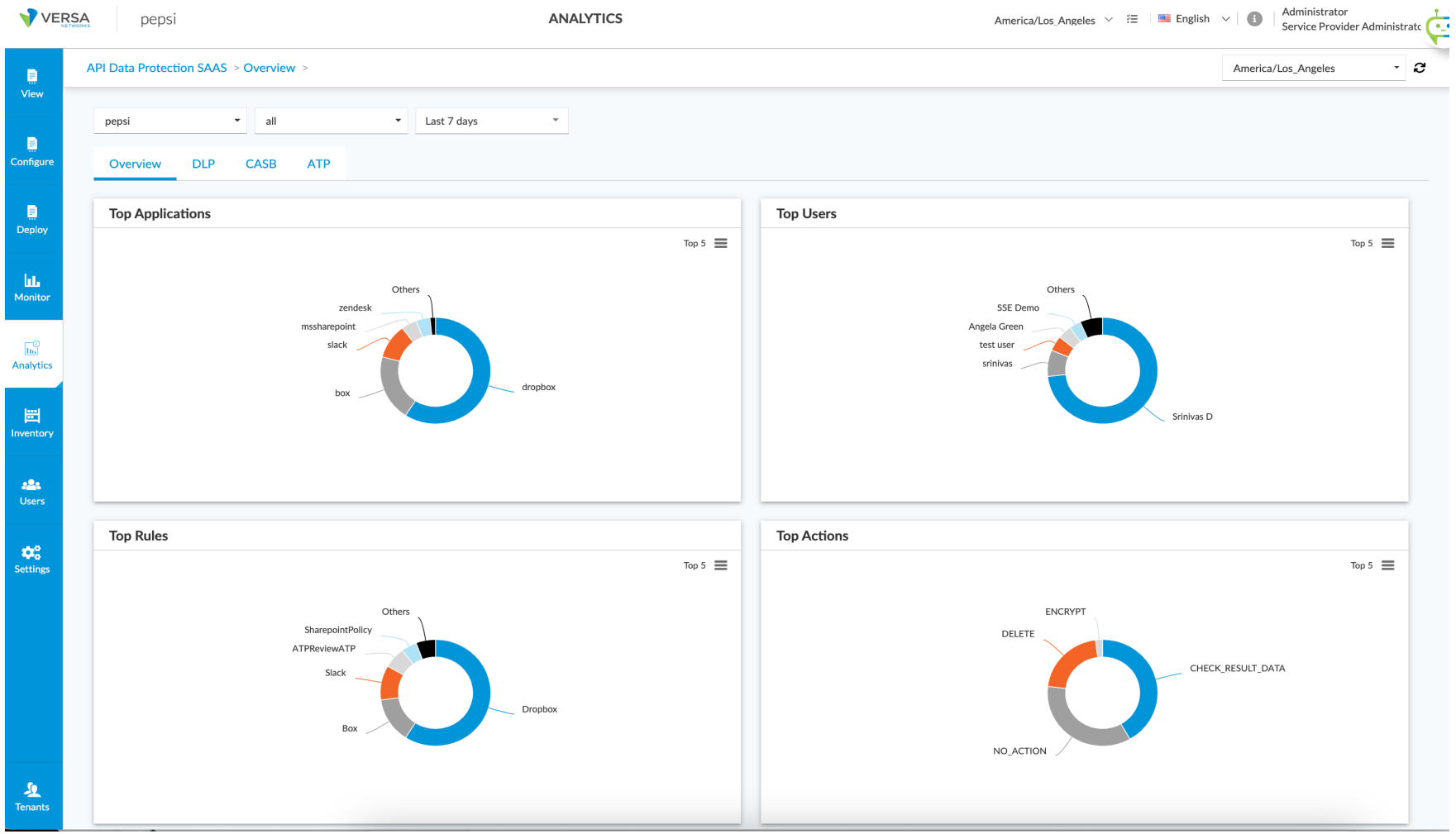
Email Protection: Policy Detail



Monitoring

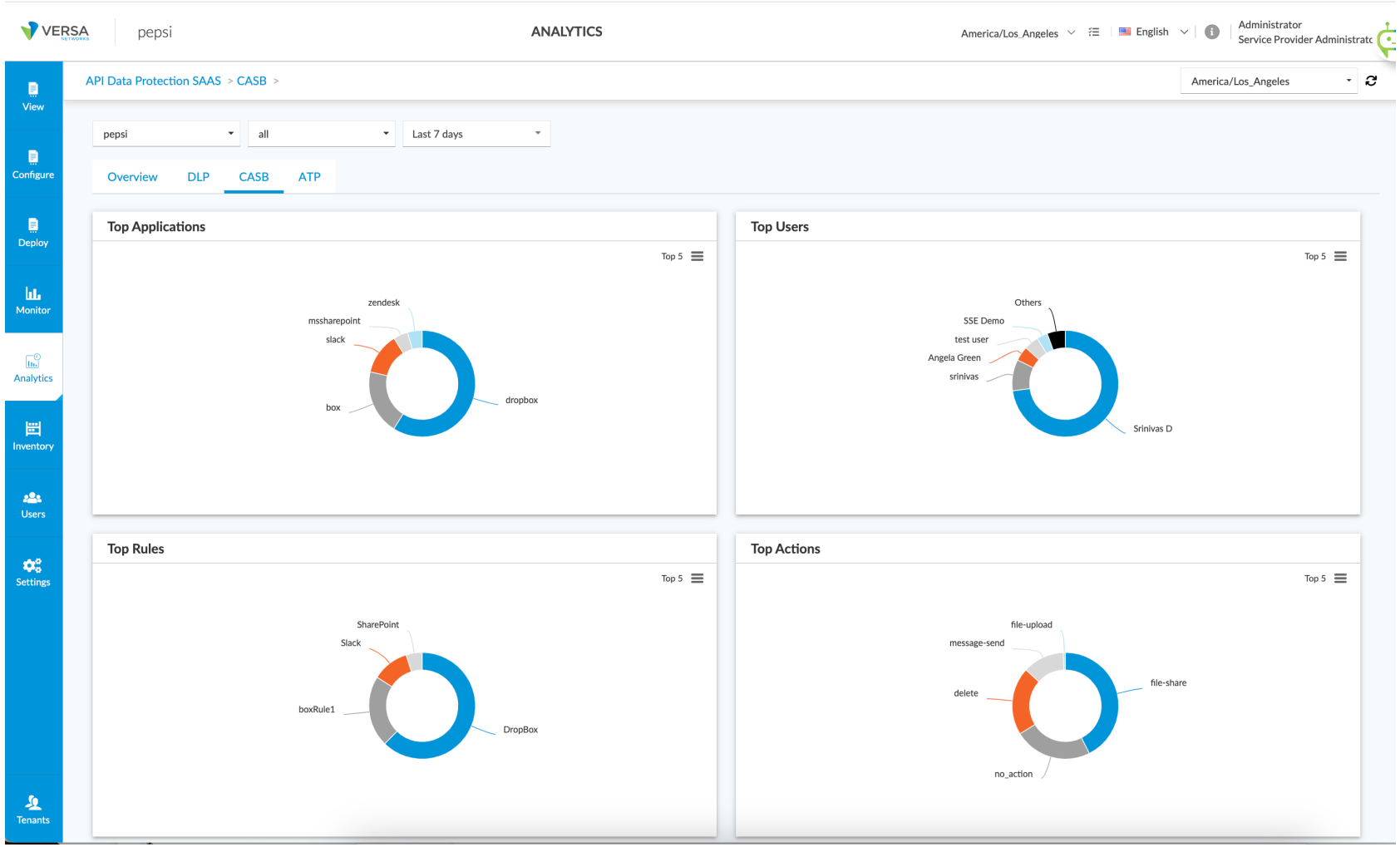
VERSA

API-DP Analytics



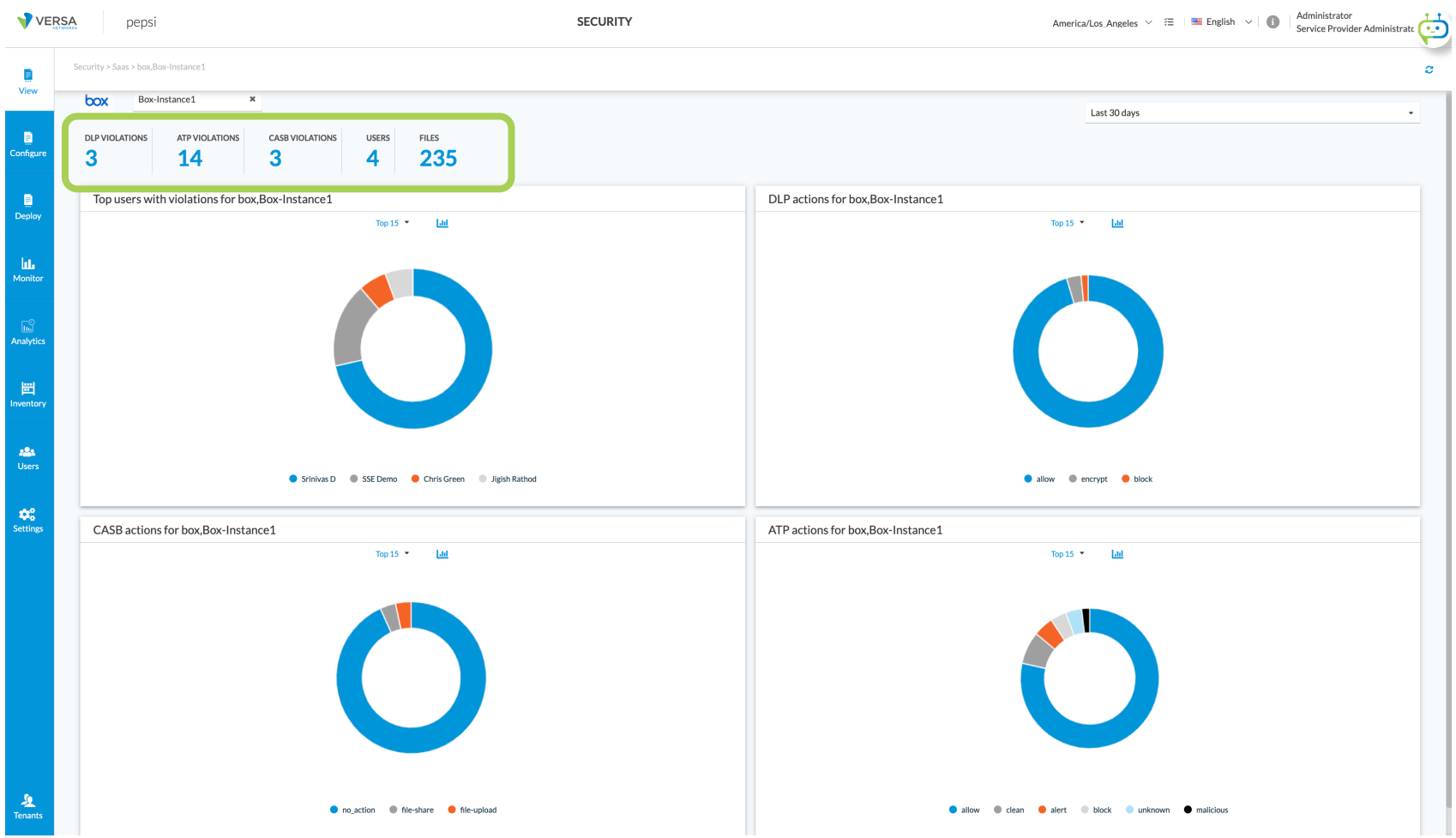
VERSA

Offline CASB Analytics



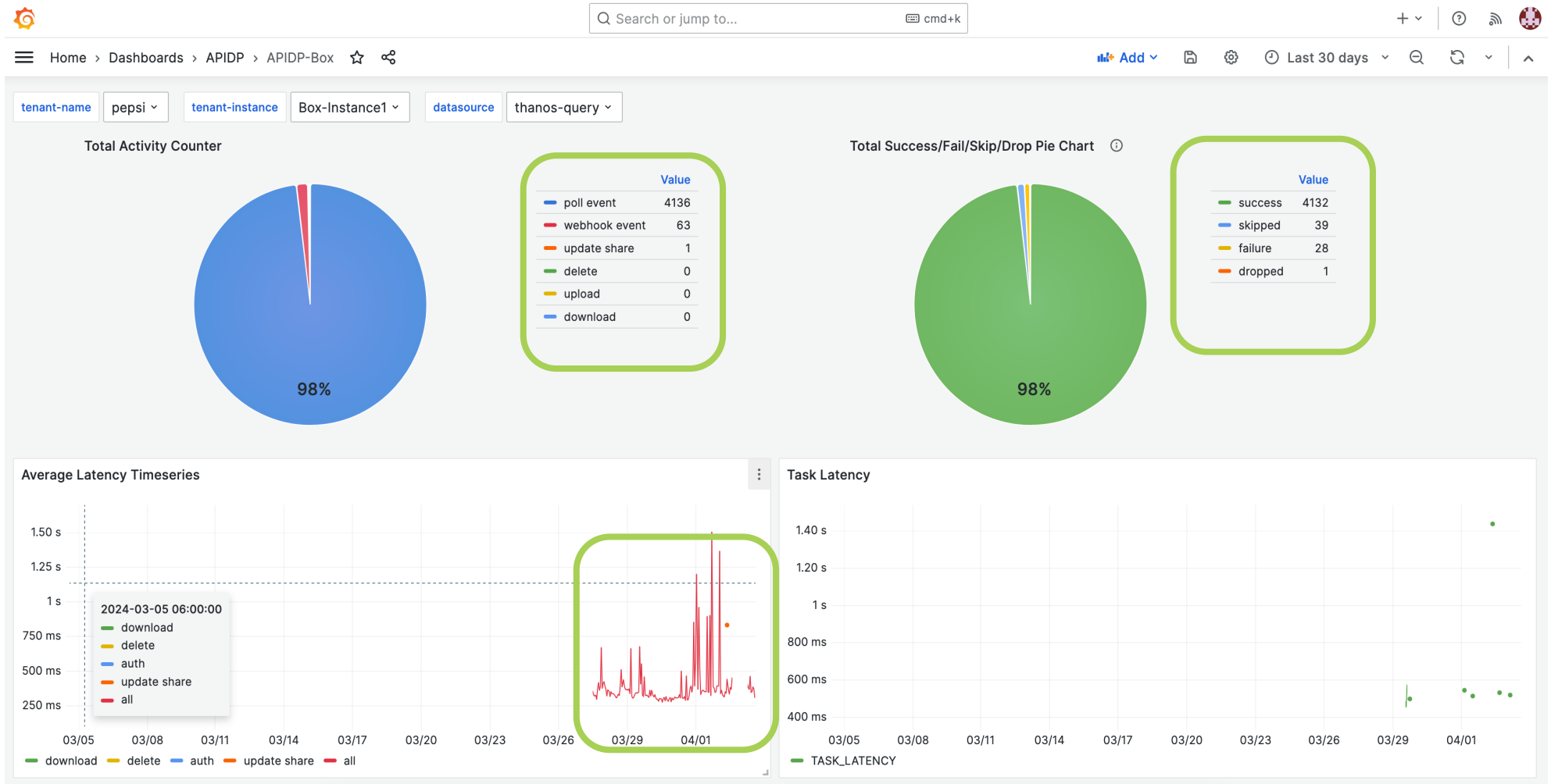
VERSA

Per Application Instance Analytics



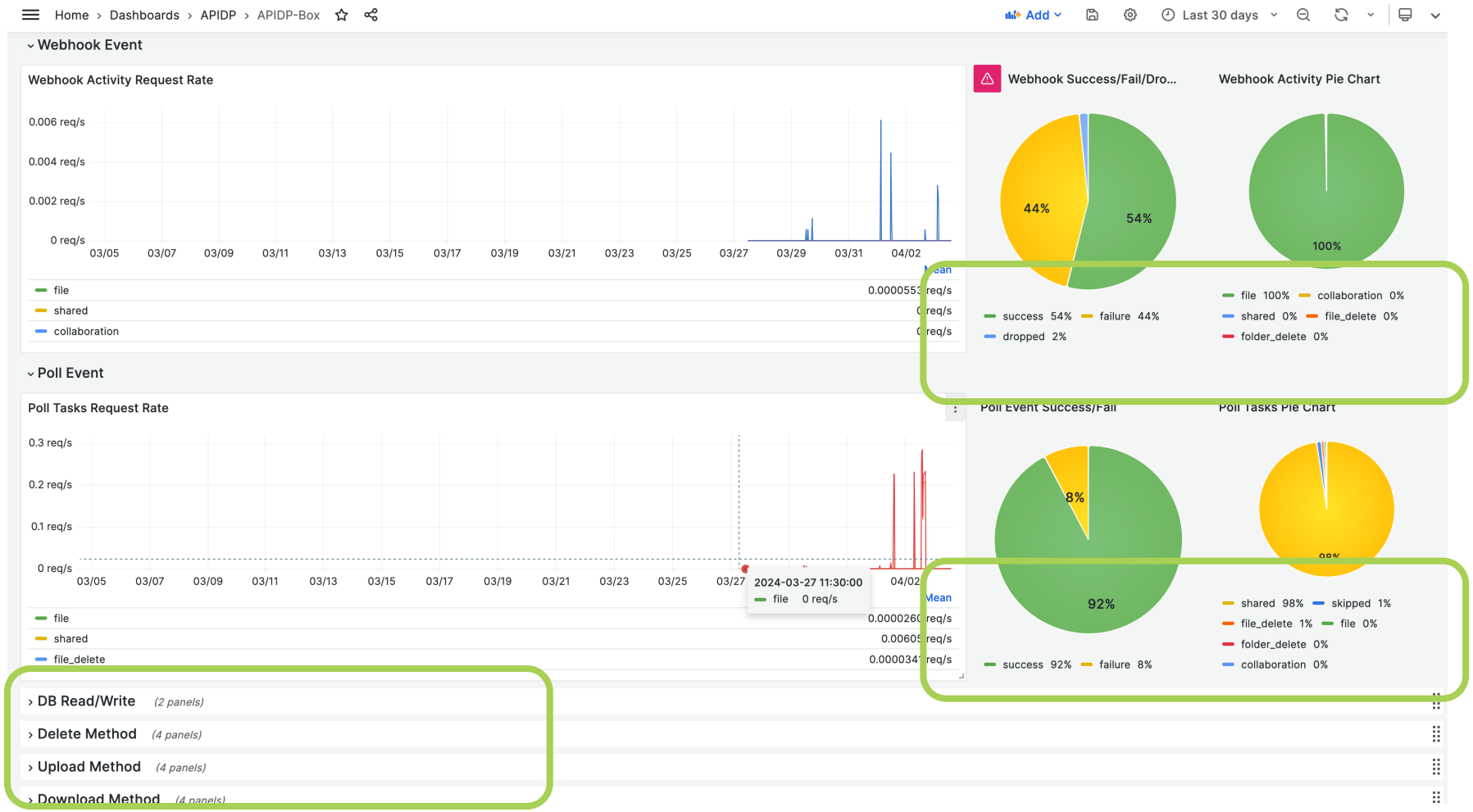
VERSA

Managed Ops Dashboard



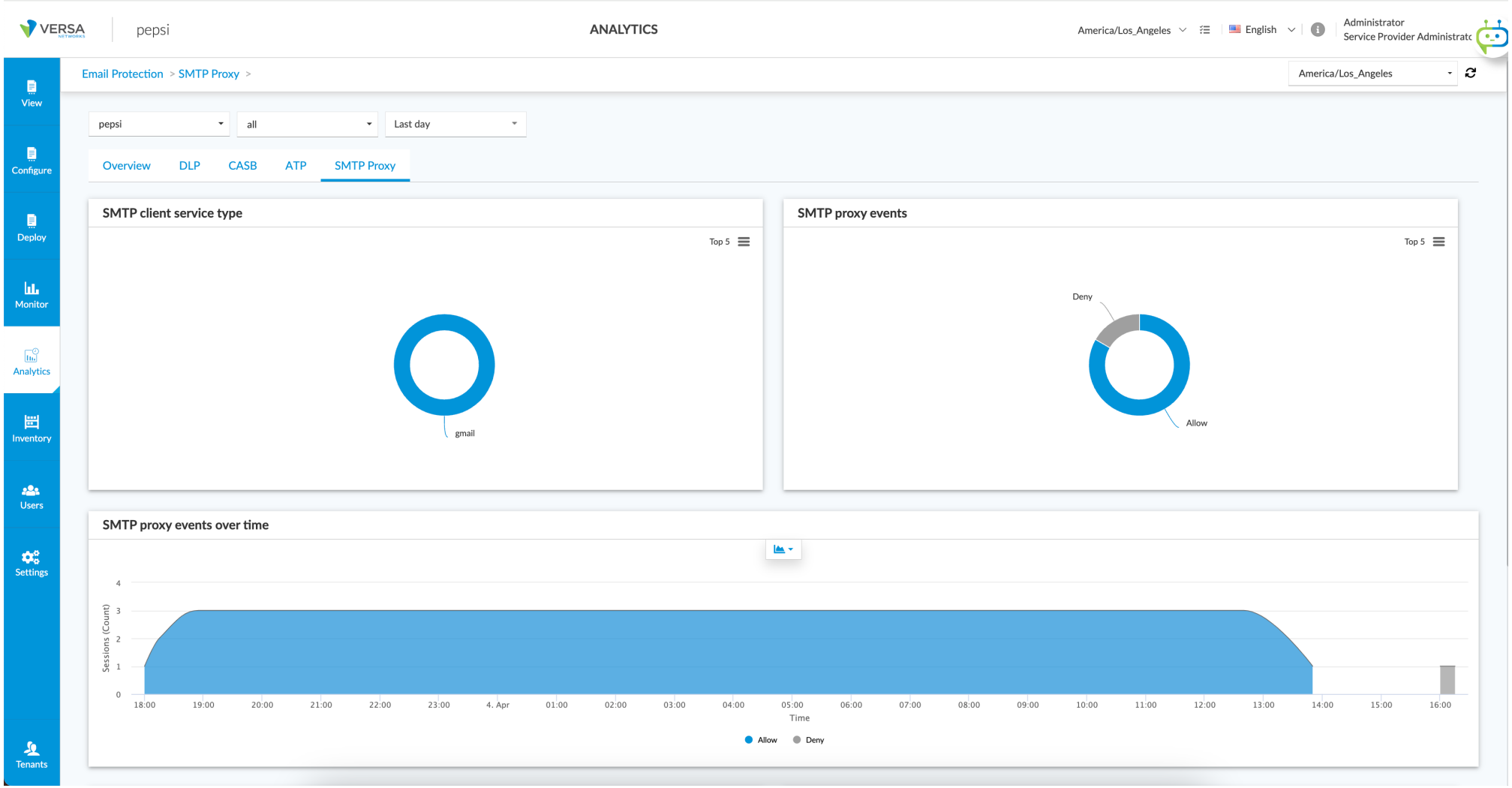
VERSA

Managed Ops Dashboard



VERSA

SMTP Proxy Analytics



Demo

VERSA

Demo

- File activity on Box
  - Shared publicly – Set link expiry
  - Infected with malware – Deleted
  - Containing confidential information – Replace with encrypted version
- User activity on Slack
  - User joining public channel – Remove
- Email Protection
  - Send email to external user from Gmail enterprise account
    - Attach document containing confidential information – DLP blocks
    - Attach clean document – Allow

Questions

VERSA

Thank you

VERSA