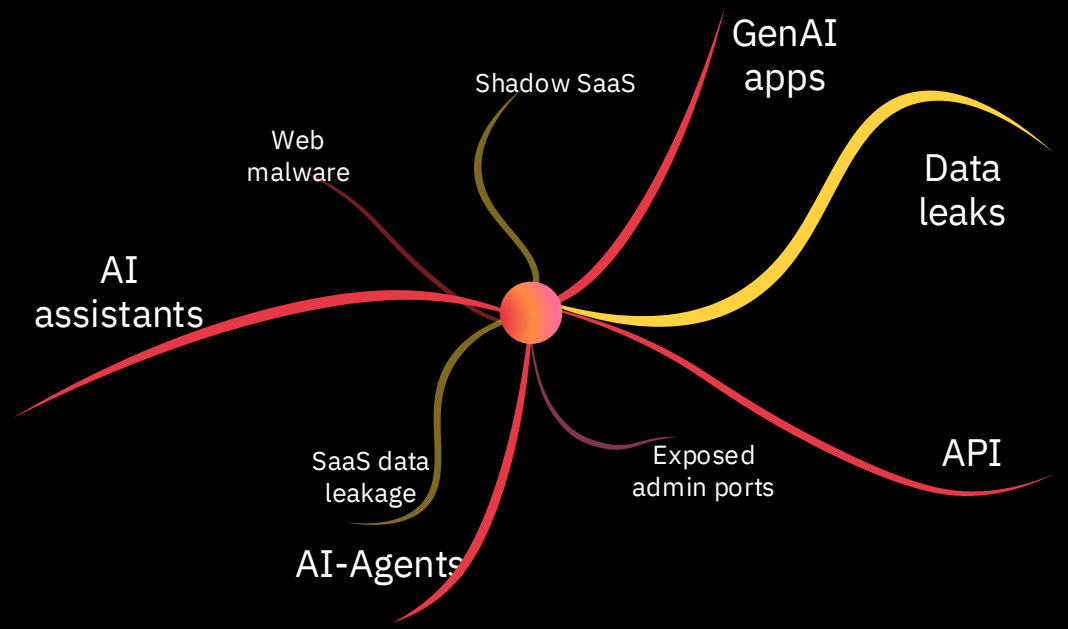
VERSATILITY

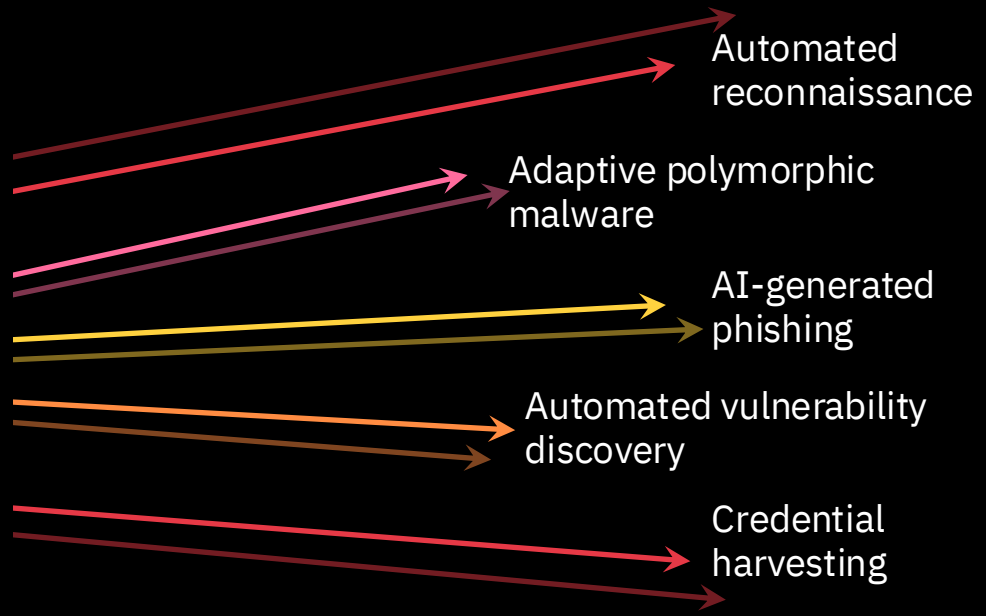
Implementing Advanced Data Protection

Kapil Bajaj, Dhiraj Sehgal

AI is accelerating security challenges in two ways



Expands the Attack Surface

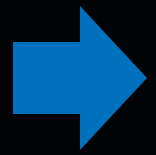


Increases the Threat Velocity

© Copyright Versa Networks. All Rights Reserved. CONFIDENTIAL.

Your Attack Surface Is Expanding Faster Than Ever: Cloud + SaaS + AI

- Multi-cloud infrastructure (AWS, Azure, GCP)
- SaaS ecosystems (Microsoft 365, Google Workspace, Salesforce, Slack, GitHub)
- Rapidly growing AI applications and copilots
- Thousands of third-party OAuth-connected integrations



Misconfigurations, policy drift, and risky SaaS integrations are now leading causes of cloud-originated breaches.

Why Traditional Security Tools Fall Short

CISO Challenges

- No unified risk posture score across cloud + SaaS
- Difficult audit readiness for SOC2 / ISO27001 / PCI
- Blind spots in shadow SaaS and OAuth sprawl

Security Engineer Challenges

- Manual policy reviews are slow and inconsistent
- Too many disconnected tools for CSPM and SSPM
- Limited drill-down evidence for remediation

Security teams need one control plane for posture, compliance, and governance.

VERSATILITY

Security Team Requirements

Posture Assessment

Complete Visibility
- cloud
- SaaS
- endpoints
- IoT

Zero Trust

Identity and device context are verified continuously.

Inline Enforcement

Security inspection occurs where connections happen, reducing response time.

Data Protection

DLP policies protect data across SaaS, endpoints, and GenAI platforms.

AI-Resilient Security

Behavioral analysis detects adaptive and AI-generated threats.

Data Protection

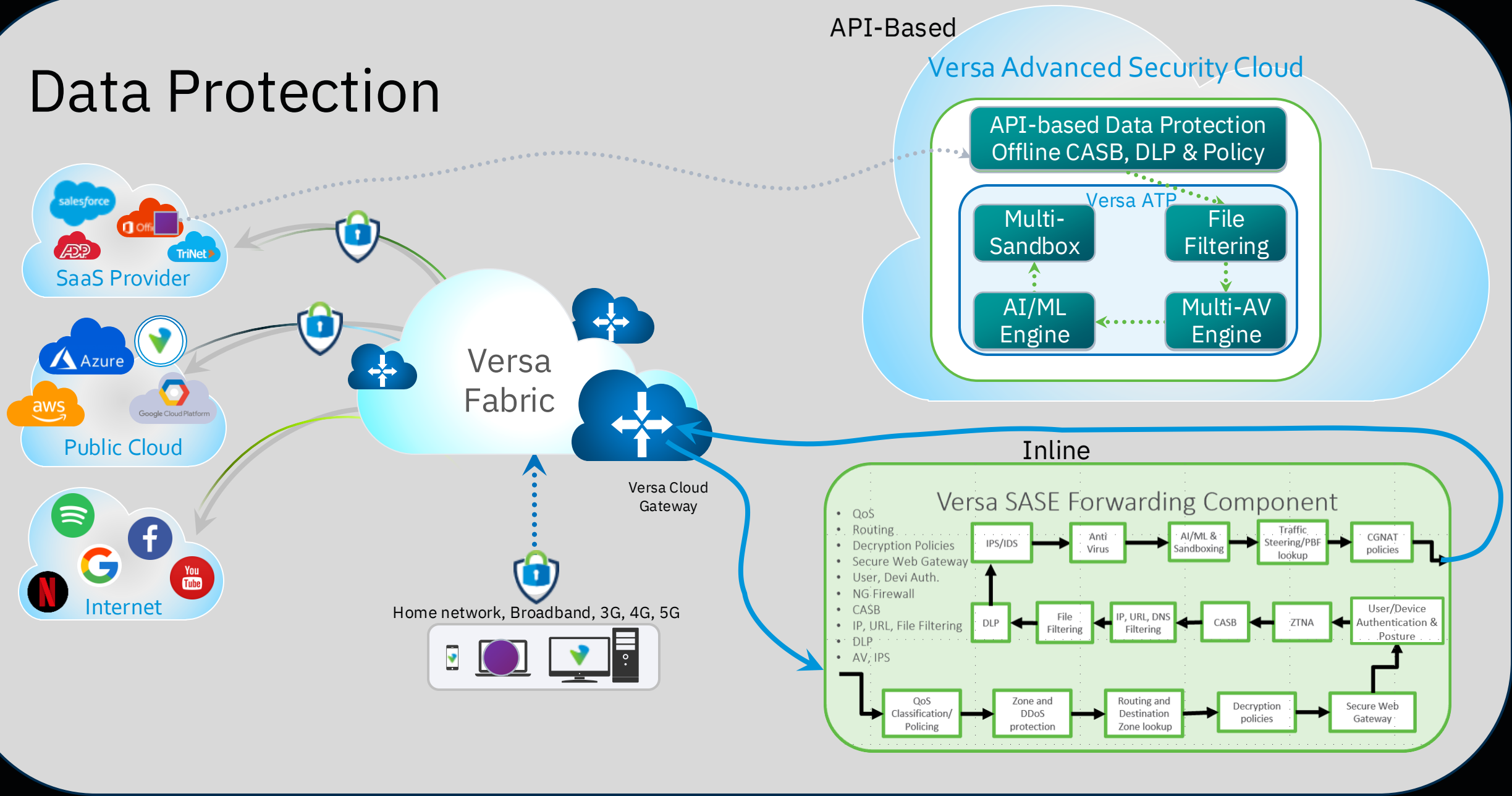
Inline-DP

- Analyzing data in transit and taking preventive action (e.g. blocking a malicious file from being uploaded)
- Use with managed devices and unmanaged devices

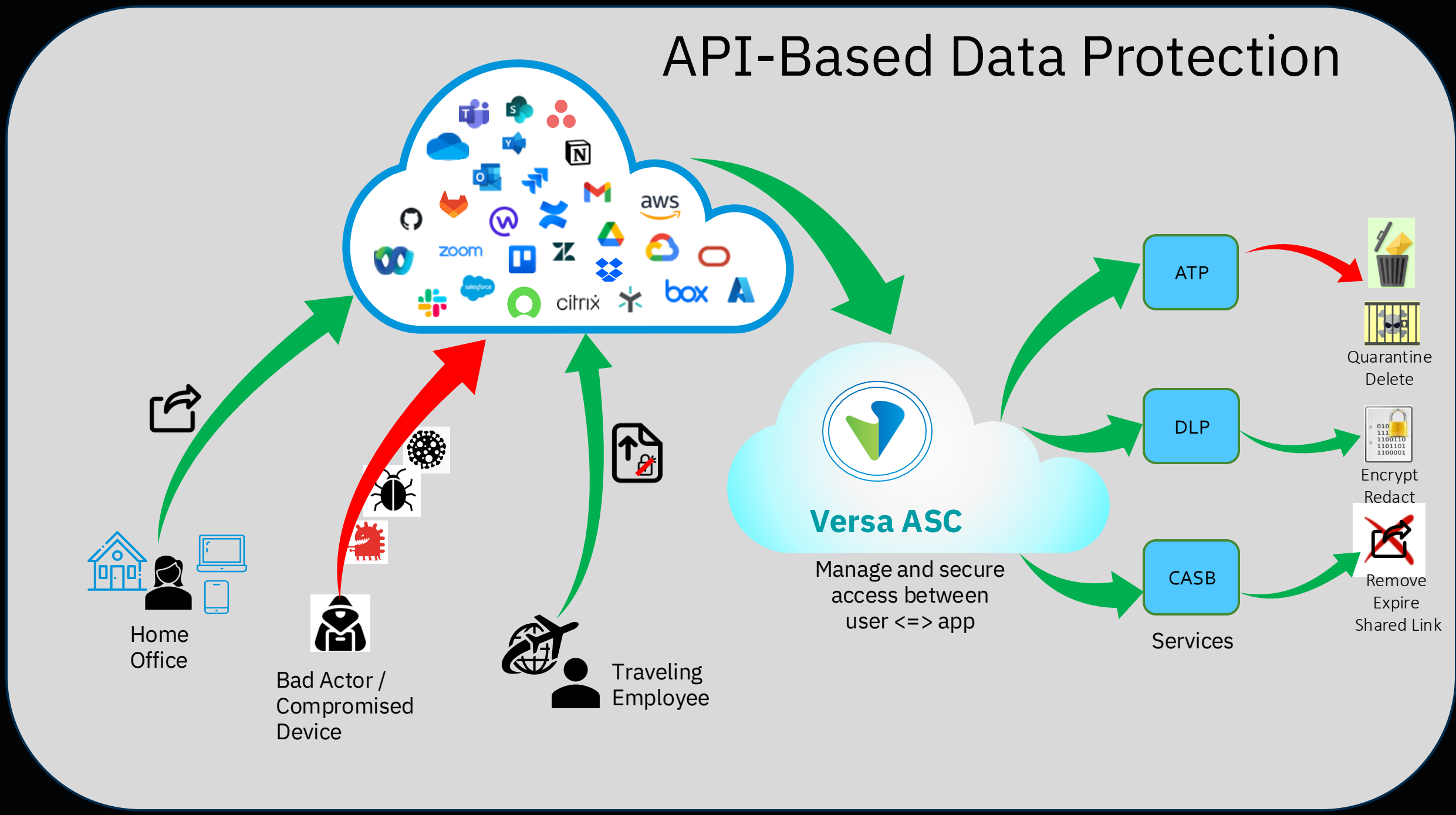
API-DP

- Analyzing data at rest (e.g. scheduled scans, post-incident forensics)
- Securing certificate-pinned apps
- Use with managed devices and unmanaged devices

Data Protection



API-Based Data Protection



API-Based Data Protection: Scan Types

Proactive Scan

Event-Based

- Triggers automatically on file upload, modification, or data creation events
- Detects threats and policy violations in near real time
- Prevents sensitive data from propagating before it can be accessed or shared
- Ideal for high-velocity environments with continuous data flows and strict compliance needs

Periodic Scan

Scheduled

- Runs on a predefined schedule — hourly, daily, weekly or monthly
- Ensures consistent coverage of all stored data, including unmodified or older content
- Catches violations missed by event-based scans or flagged by updated policy rules
- Lightweight on resources, making it easy to run during off-peak hours

Retroactive Scan

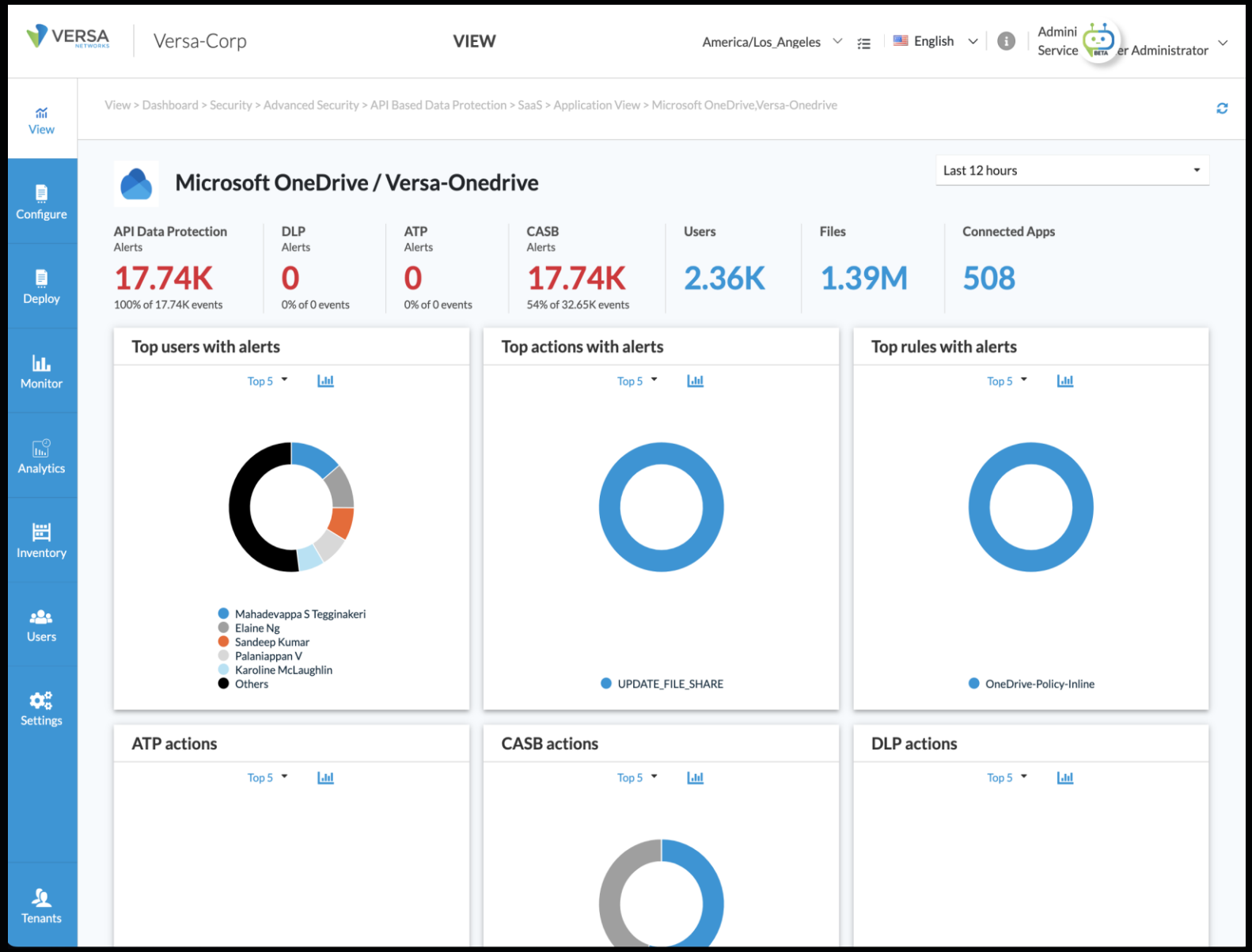
Retroactive

- Analyzes historical data created before DLP policies were configured or enforced
- Brings legacy content into compliance without the need for manual review
- Critical during onboarding, policy updates, or regulatory audits
- Closes compliance gaps by applying current classification rules to data

API-Based Data Protection: Reporting

Key Highlights

- **Global View**
  Unified dashboard aggregates activity across all connected SaaS apps — providing a single-pane-of-glass for security posture
- **Dedicated Module Reports**
  Separate report tabs for CASB, DLP, and ATP surface top alerts, actions, rules, and activity trends specific to each domain
- **Top Offenders at a Glance**
  Surface the highest-risk users, applications, and rules in a single view — making it easy to prioritize response and focus security attention where it matters most.
- **Per-App & Per-User Views**
  Drill into Application View or User View to isolate top apps, top users, and individual activity patterns



Data Security Posture Management

Discover, classify, and continuously govern sensitive data across every cloud, SaaS, and on-prem data store

Automated Data Discovery

Continuously scan GCP, AWS, Azure, OCI, Snowflake, MongoDB and SaaS stores to surface all sensitive data — including shadow stores.

Sensitive Data Classification

Auto-classify PII, PHI, PCI, financial and proprietary data with regulatory tagging for GDPR, HIPAA and PCI-DSS.

DSPM Risk Score

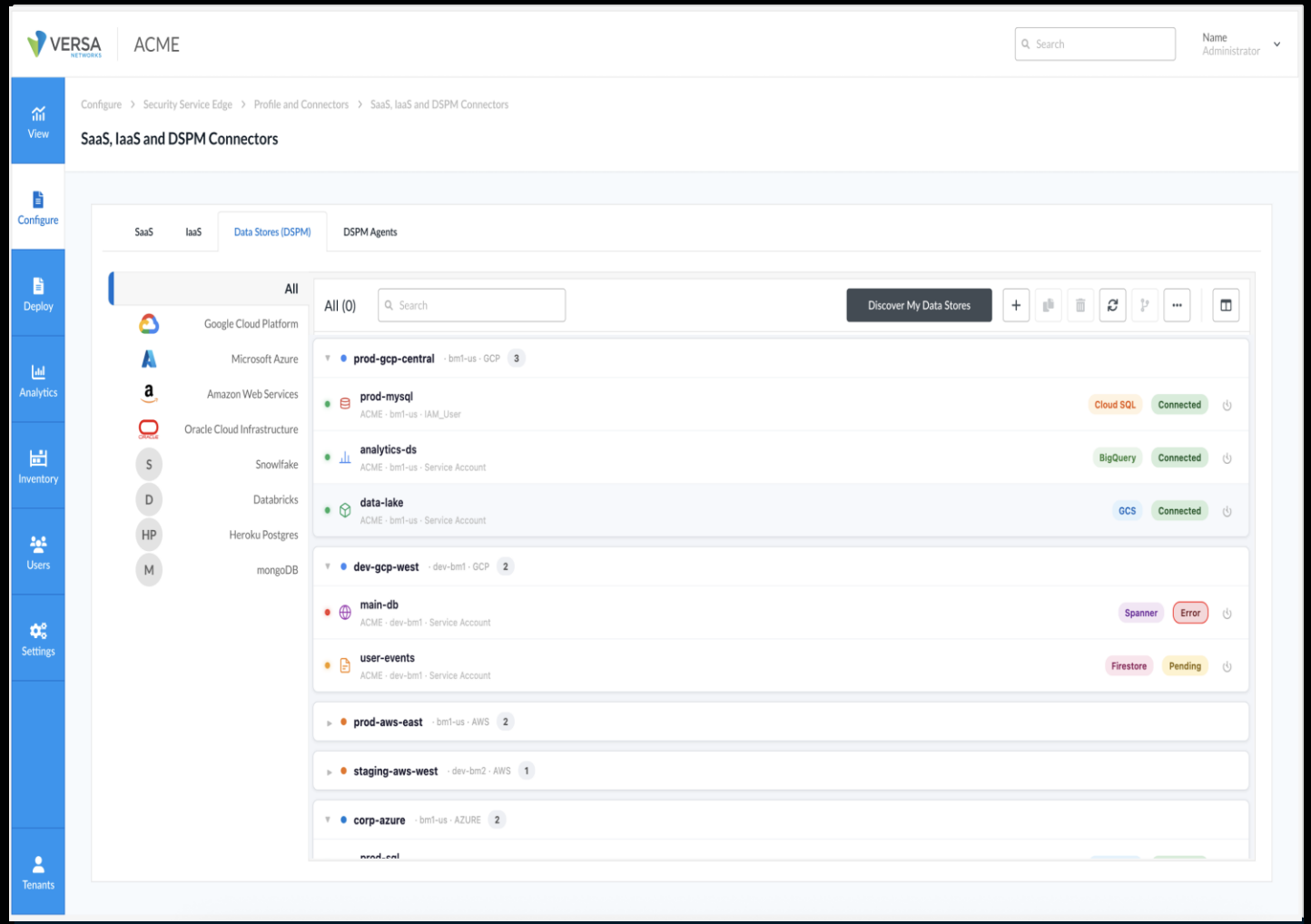
A single 0–100 posture score tracks infrastructure, data, user access and interaction risk.

Access Governance & Monitoring

Detect risky queries, over-privileged access, and abnormal user interactions with sensitive data in real time.

Data never leaves your cloud

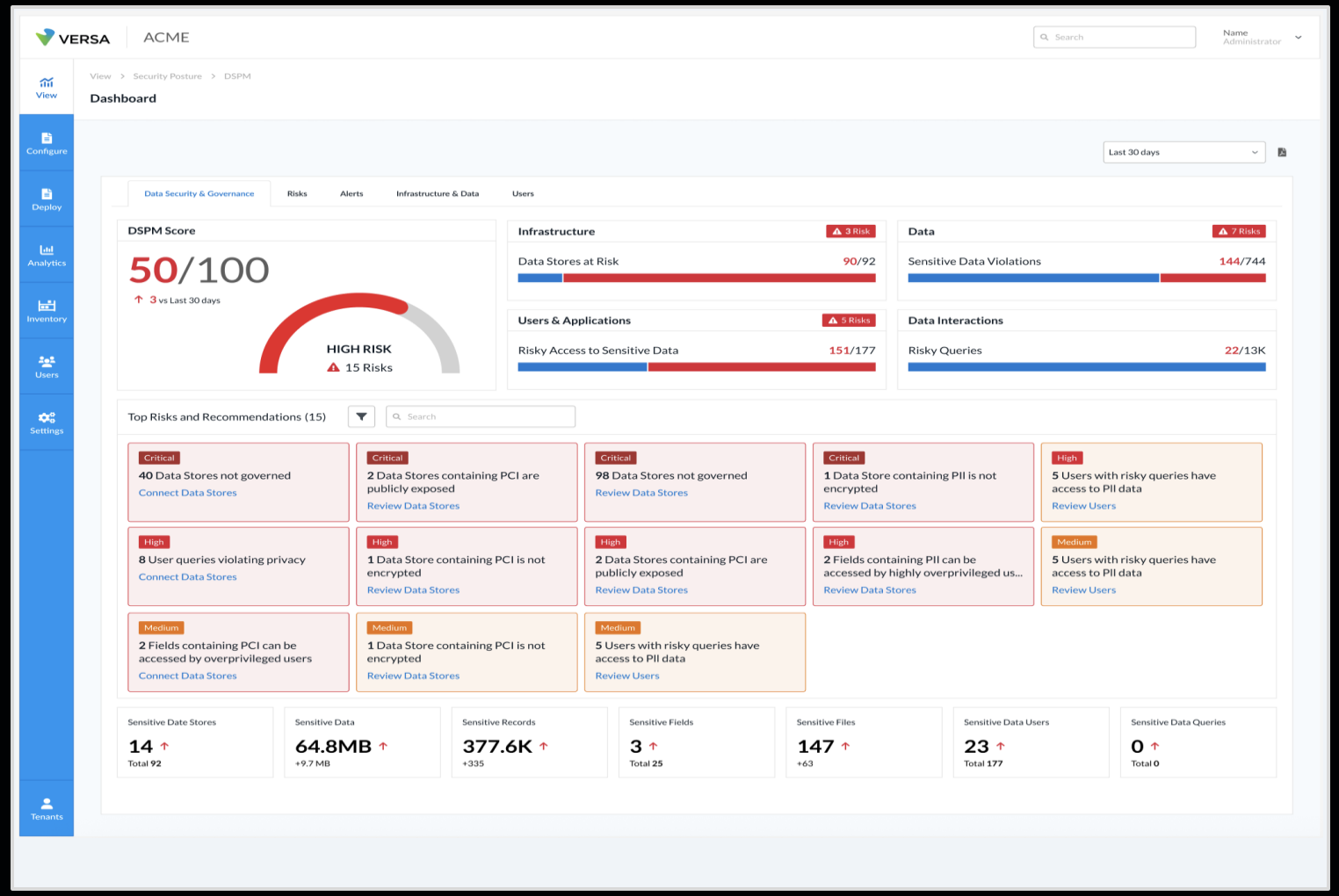
The DSPM Agent runs analysis entirely inside your cloud environment. Sensitive data is scanned and classified in-place — nothing is extracted or transmitted externally — so you stay in full control of your data at all times.



DSPM Connectors

VERSATILITY

Data Security Posture Management - Reports



Unified risk score

The DSPM Score rolls infrastructure risk, sensitive data violations, and risky access into a single metric — giving security teams and executives one number to track posture over time.

Prioritized remediation queue

Findings are ranked Critical → Medium so teams act on the highest-impact issues first — ungoverned data stores, publicly exposed PCI data, and privacy-violating queries — without sifting through noise.

Integrated inside Versa Unified SASE

DSPM runs natively alongside CSPM and SSPM, correlating access risk, cloud posture risk, and data security risk in one platform — eliminating the blind spots that come from disconnected point tools.

VERSATILITY