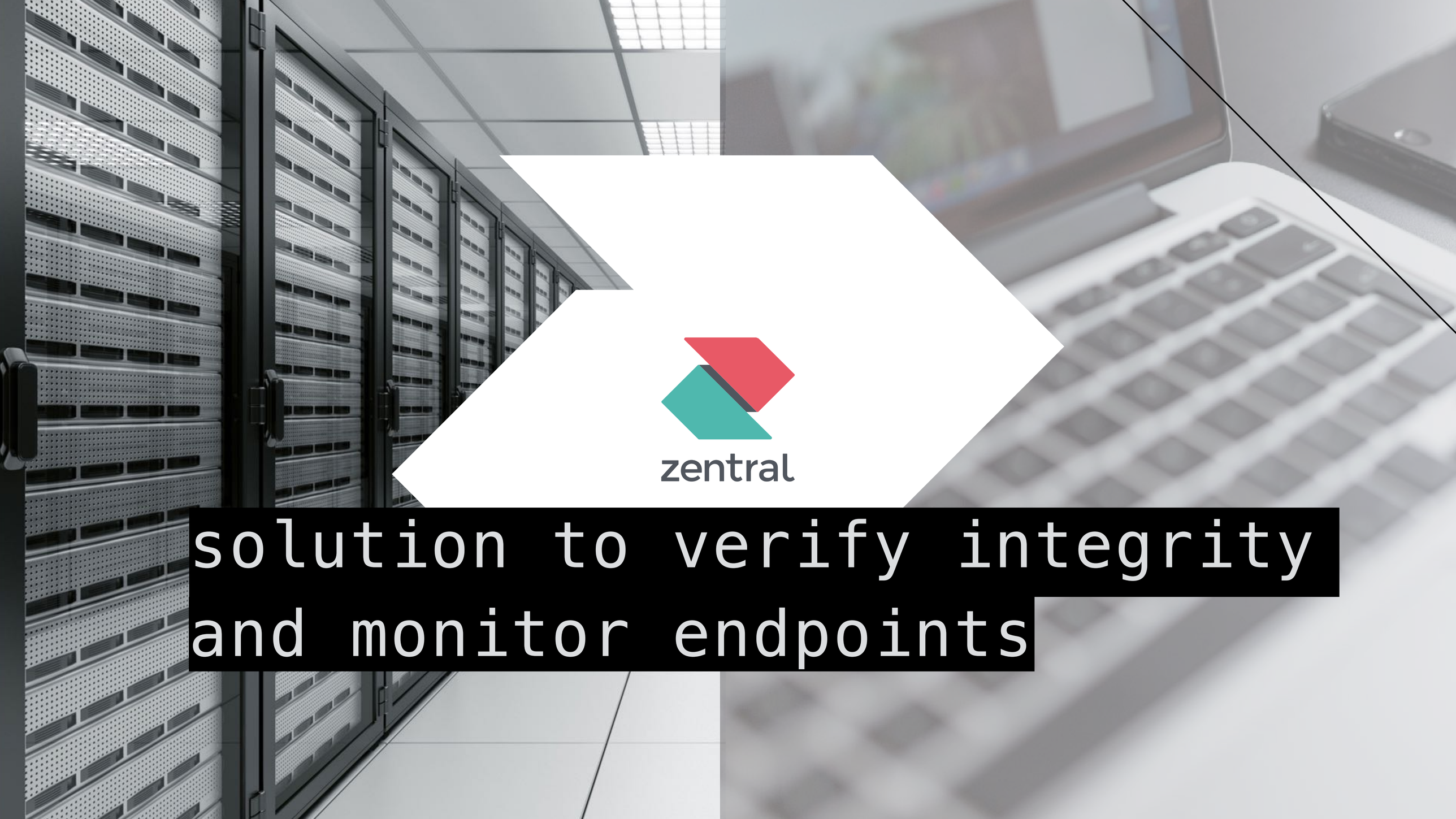
Zentral

Open hub for monitoring

20. April 2017 London Apple Admin Meetup

zentral

event stream processing and alerting

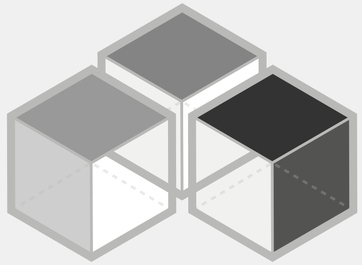


zentral

solution to verify integrity and monitor endpoints

Framework

- Organised deployment of open source tools
- Modular architecture
- Python3 / Django

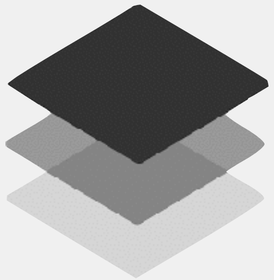


TLS server

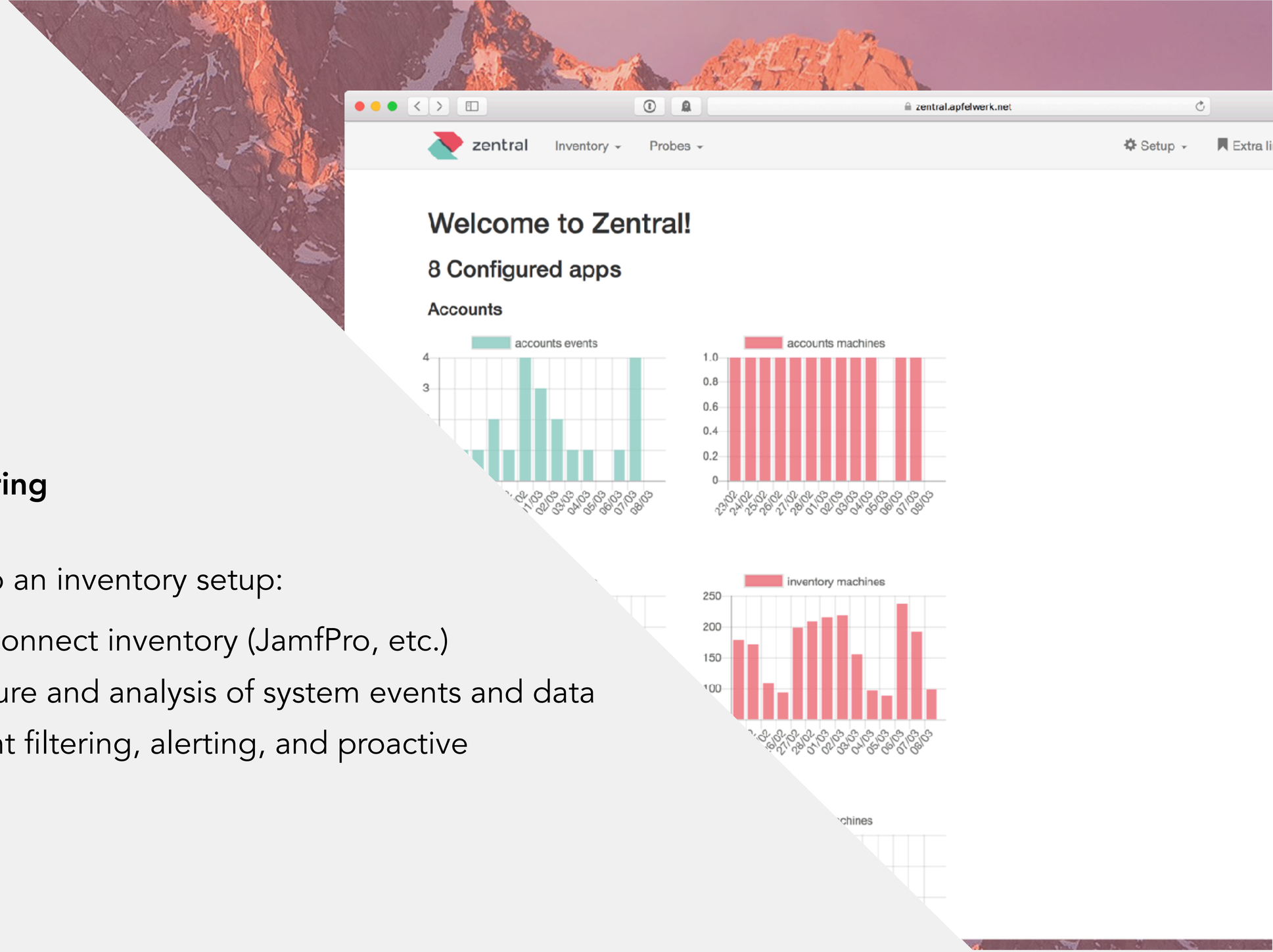
- Event logging APIs
- Dedicated log / configuration for Osquery & Santa

Inventory

- Multiple sources
- Parallel processing
- Store change history



Zentral - open hub for monitoring



Zentral

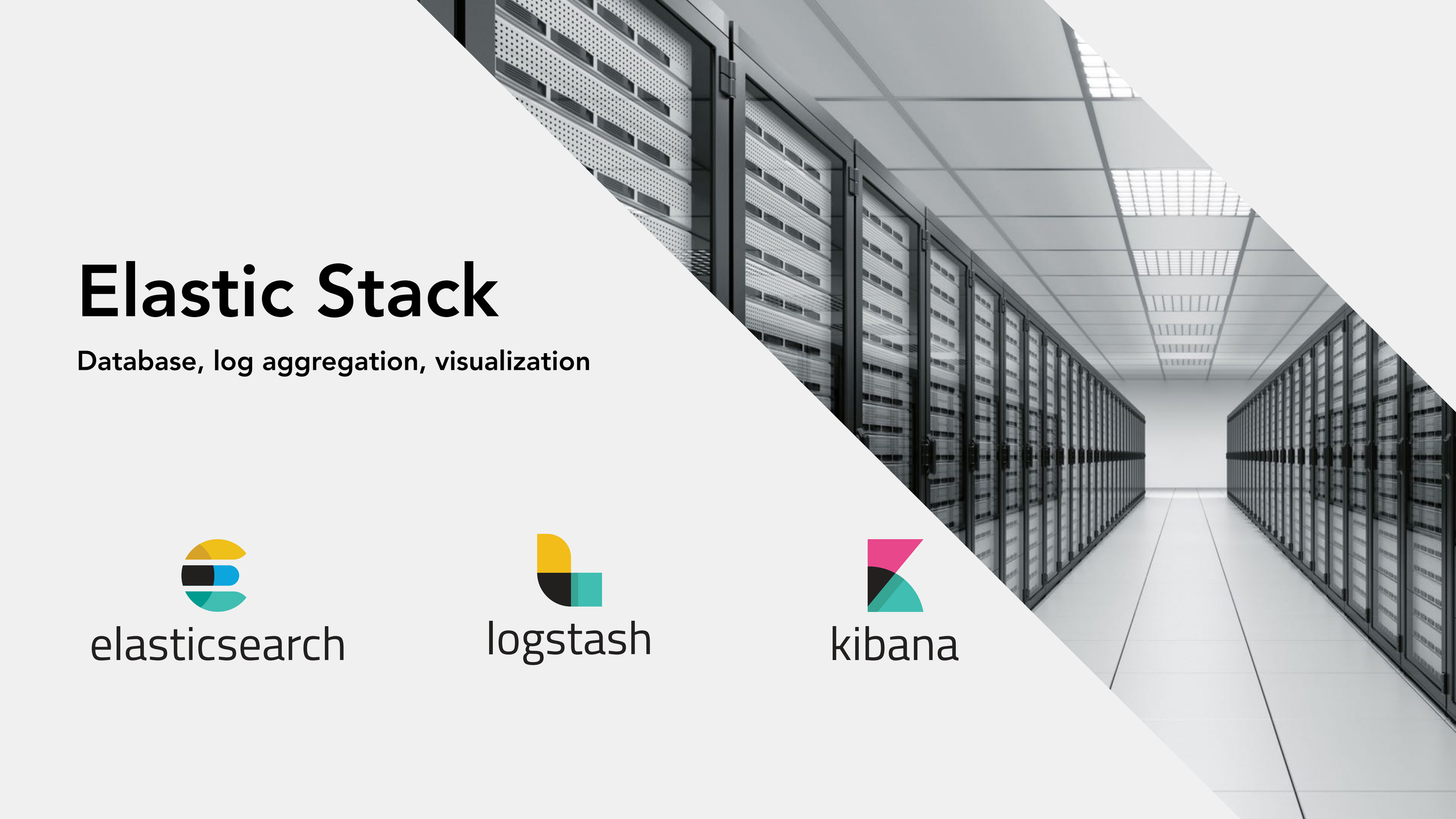
Open hub for monitoring

Monitor events / link to an inventory setup:

1. Enroll devices and connect inventory (JamfPro, etc.)
2. Near-real-time capture and analysis of system events and data
3. Run probes for event filtering, alerting, and proactive automations (IFTTT)

Elastic Stack

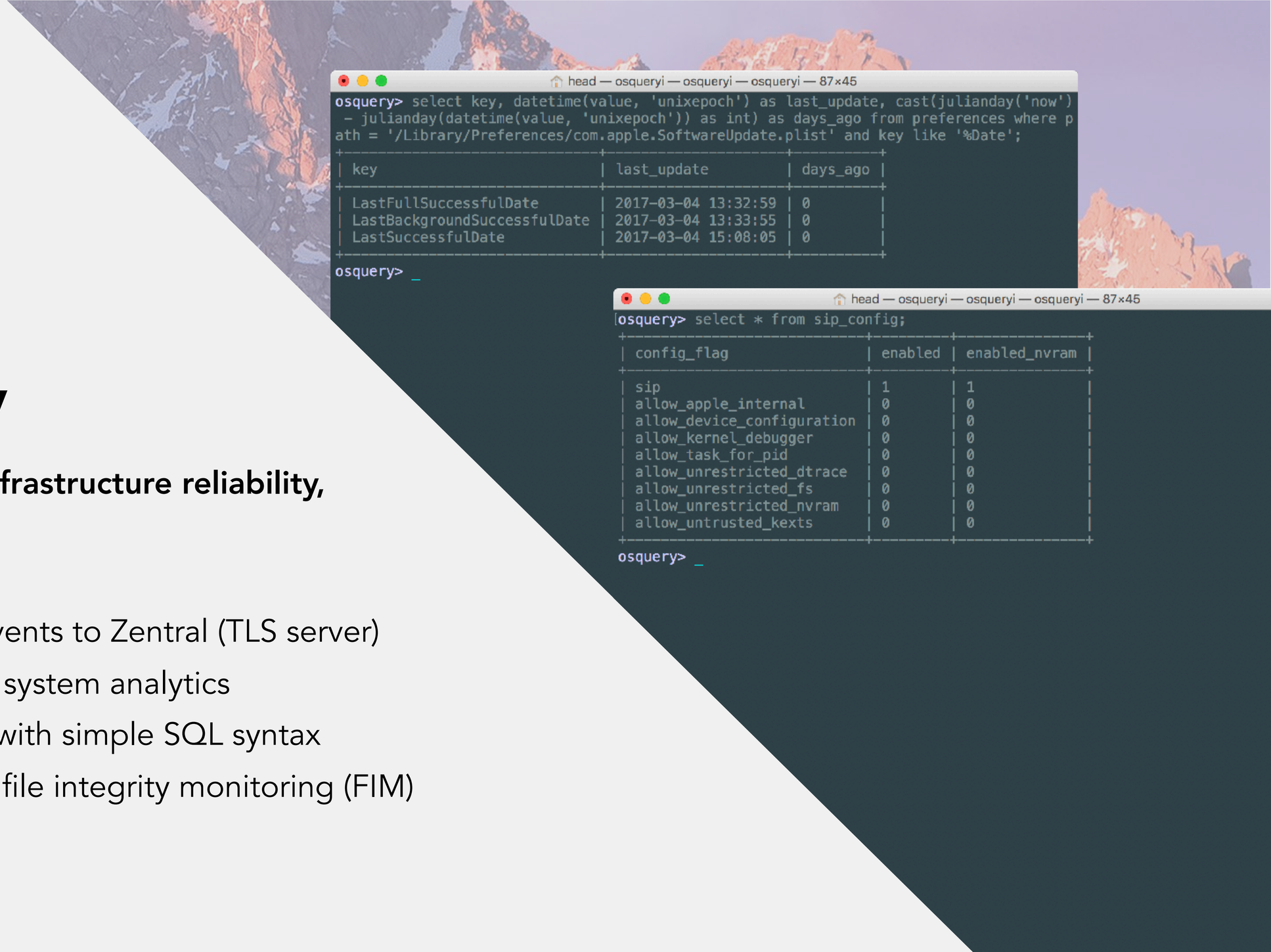
Database, log aggregation, visualization



elasticsearch

logstash

kibana



Osquery

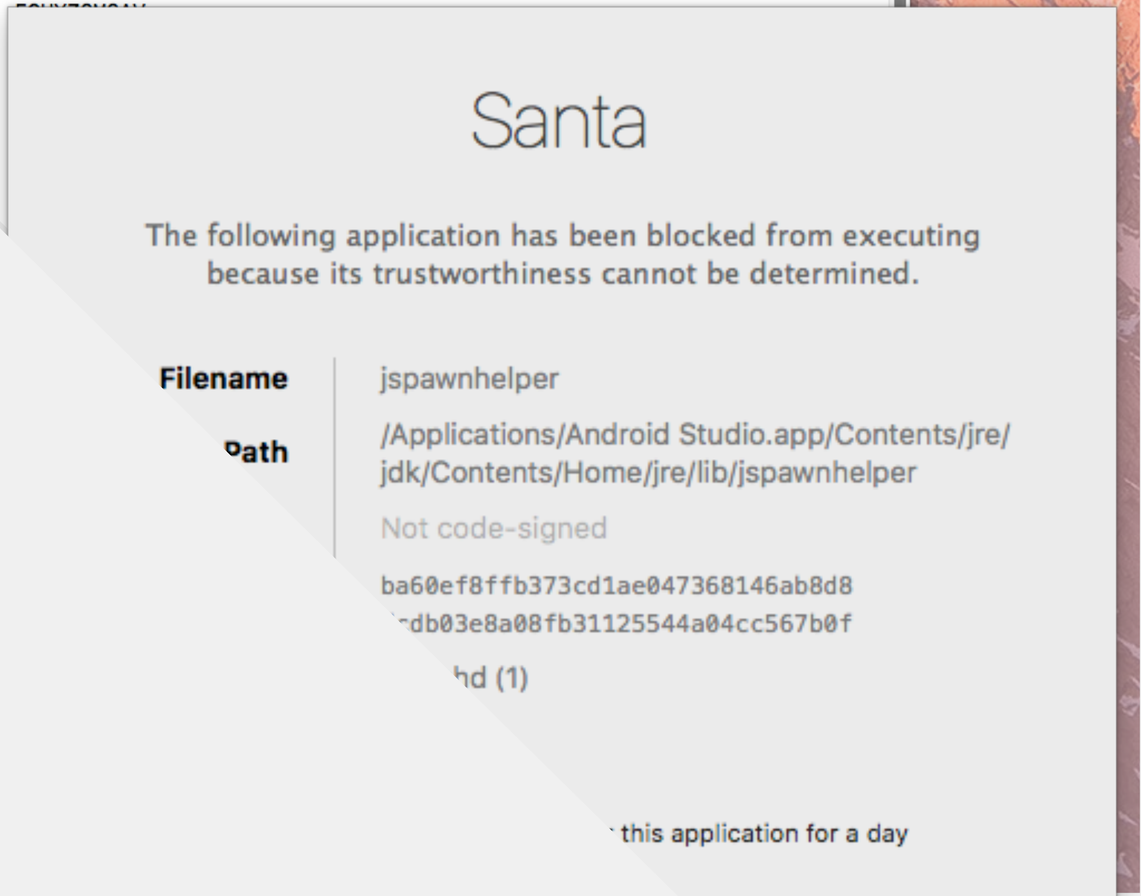
Intrusion detection, infrastructure reliability, and compliance

- Sync config, push events to Zentral (TLS server)
- Low-level operating system analytics
- Query system state with simple SQL syntax
- Distributed queries, file integrity monitoring (FIM)

Google Santa

Binary logging, blacklisting/whitelisting for macOS

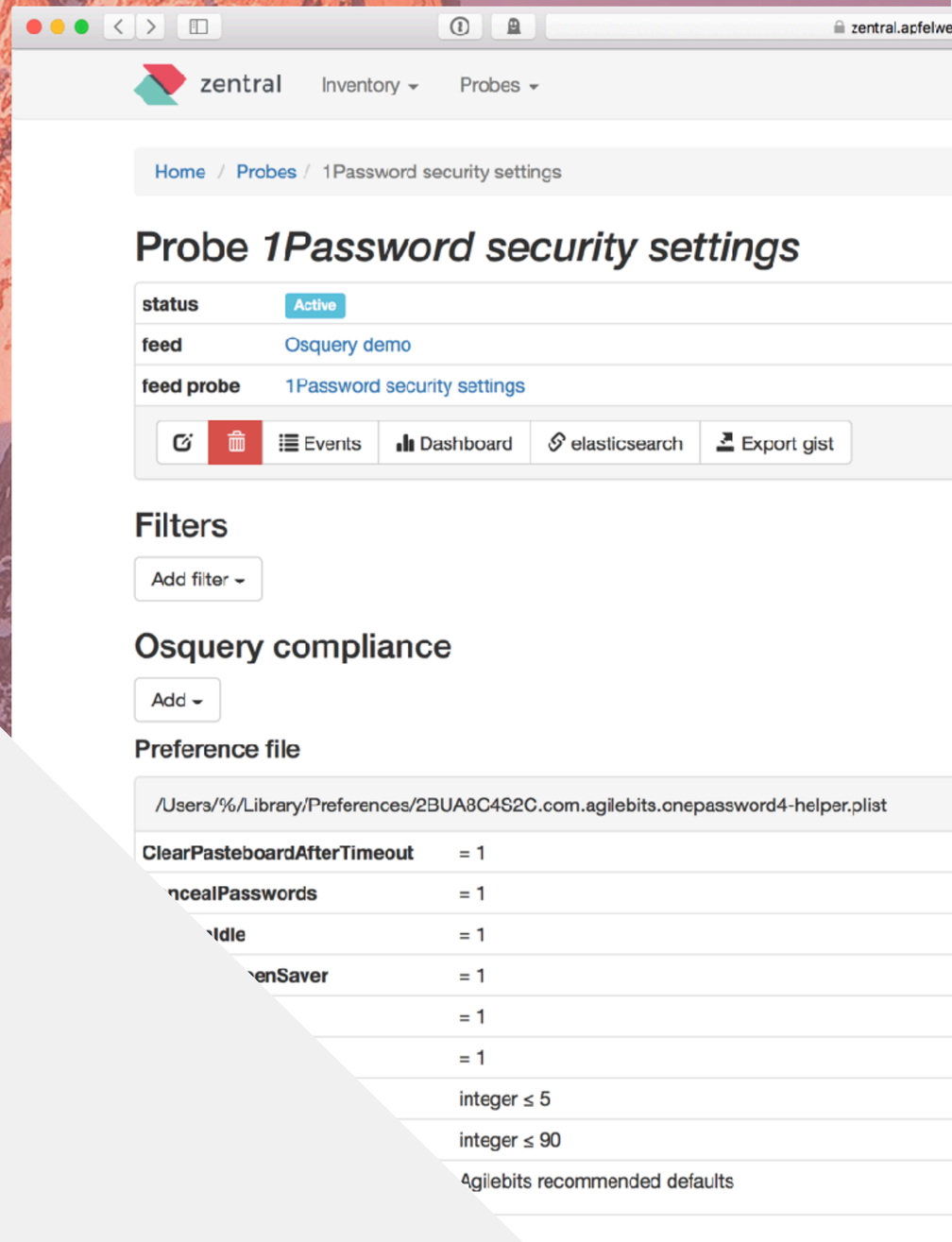
- Sync config, push events to Zentral (TLS server)
- All binary launches are logged
- Client mode: MONITOR
- Client mode: LOCKDOWN (defaults deny)



Probe

Bundle filters, actions and optional configuration

- Filter on events, inventory, metadata
- Organize Santa rules or Osquery SQL (dynamic config)
- Control and minimize event overhead
- Trigger actions (API calls, notify)
- Export, share as Gist (GitHub)



Open hub for deployed tools

Combine powerful existing tools to meet your operational requirements

JamfPro
Client management
Inventory
MDM solution

Munki
Client management
Inventory

Filewave
Client management
Inventory

Watchman Monitoring
Health monitoring
agent

Supported inventory

Open hub for deployed tools

Combine powerful existing tools to meet your operational requirements

Slack
Team chat
notifications

Trello
Kanban Board
workflows

Zendesk
Ticketing system
workflows

Jira
Ticketing system
workflows

Supported actions

+ actions / notifications available for
GitHub, Email, SMS, Push Notifications,…

Workshop / Demo

zentral

Deployment options

GoogleCloudPlatform

zentral-all-in-one image

SaaS Zentral
+ Support contract

production

Amazon AWS

zentral-all-in-one AMI

SaaS Zentral
+ Support contract

production

Docker

Docker-Compose

(development env)

OVA / Vagrant

VMware ESXi / vSphere
+ on prem support option

Vagrant (eval)

Combine tools & meet operational requirements

- Integrate services already deployed
- Enhance control and monitor endpoints
- Tight integration with JamfPro and other APIs
- Combine system monitoring and automation
- Full audit trail for management frameworks

Flexible, proactive, actionable

Service / Support

- SaaS (Cloud based service)
- Professional services, custom development
- Integration support (on premise)

Community support via github (free)
Paid support / integration / development (on request)

info@zentral.io

Thank you !