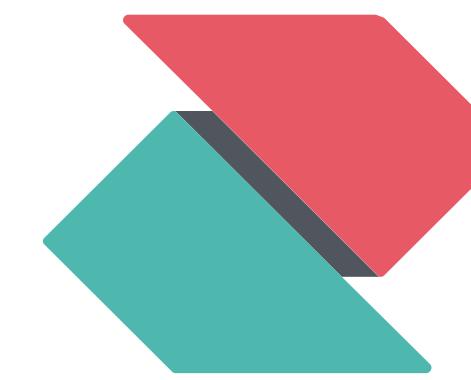




Zentral

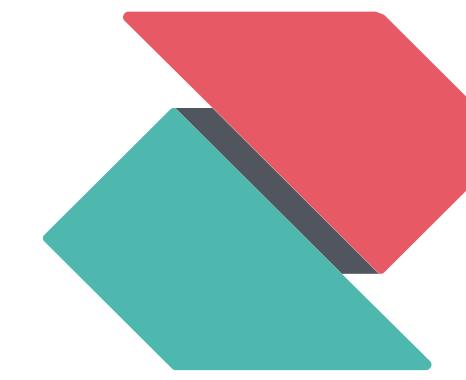
Open hub for monitoring

20. April 2017 London Apple Admin Meetup



zentral

event stream processing
and alerting

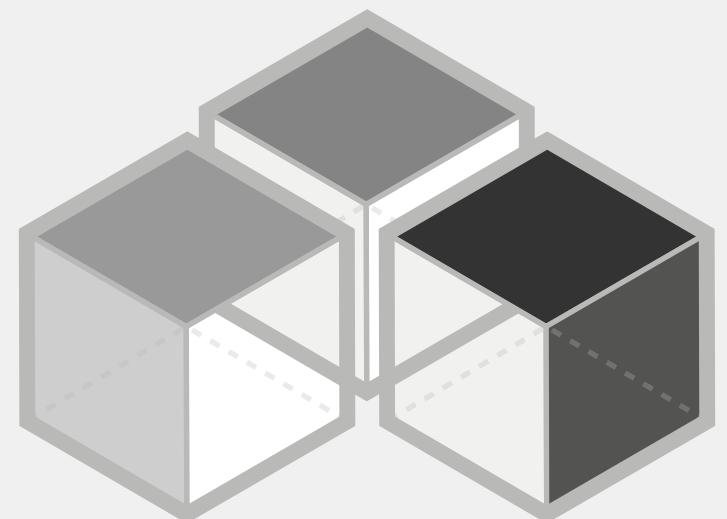


zentral

solution to verify integrity
and monitor endpoints

Framework

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



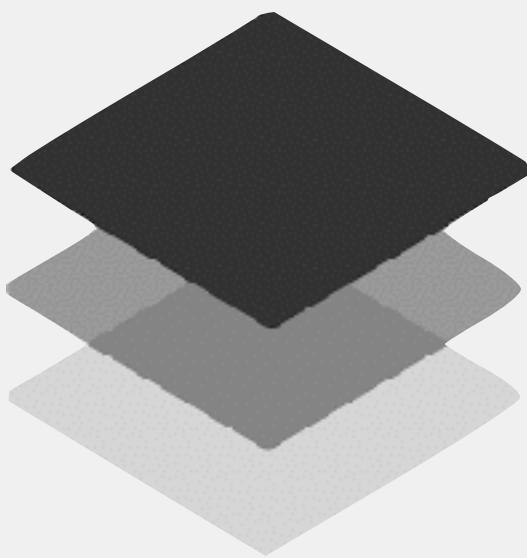
TLS server

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



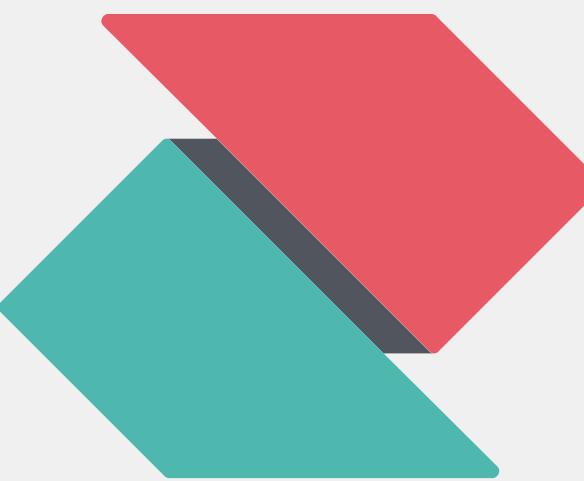
Inventory

- Multiple sources
- Parallel processing
- Store change history



Zentral -
open hub for monitoring



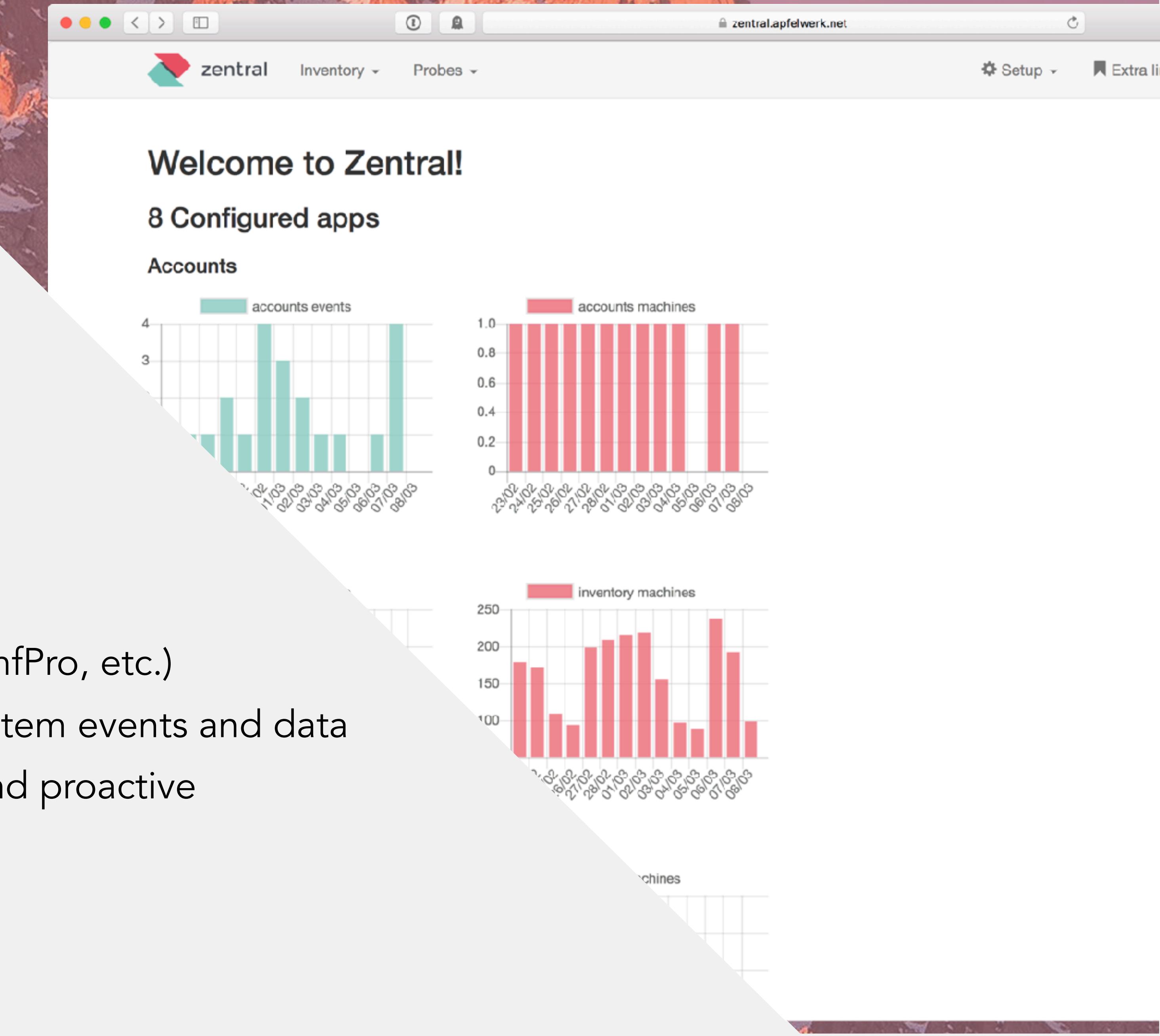


Zentral

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

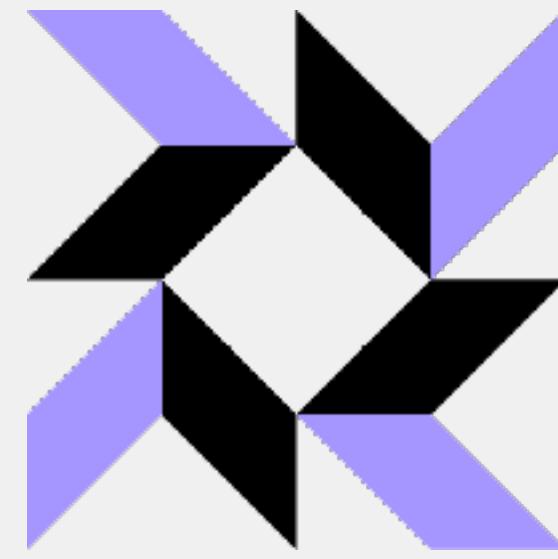


logstash



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)

```
osquery> select key, datetime(value, 'unixepoch') as last_update, cast(julianday('now') - julianday(datetime(value, 'unixepoch'))) as int as days_ago from preferences where path = '/Library/Preferences/com.apple.SoftwareUpdate.plist' and key like '%Date';
+-----+-----+-----+
| key | last_update | days_ago |
+-----+-----+-----+
| LastFullSuccessfulDate | 2017-03-04 13:32:59 | 0
| LastBackgroundSuccessfulDate | 2017-03-04 13:33:55 | 0
| LastSuccessfulDate | 2017-03-04 15:08:05 | 0
+-----+-----+-----+
osquery>
```



```
osquery> select * from sip_config;
+-----+-----+-----+
| config_flag | enabled | enabled_nvram |
+-----+-----+-----+
| sip | 1 | 1
| allow_apple_internal | 0 | 0
| allow_device_configuration | 0 | 0
| allow_kernel_debugger | 0 | 0
| allow_task_for_pid | 0 | 0
| allow_unrestricted_dtrace | 0 | 0
| allow_unrestricted_fs | 0 | 0
| allow_unrestricted_nvram | 0 | 0
| allow_untrusted_kexts | 0 | 0
+-----+-----+-----+
osquery>
```



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)

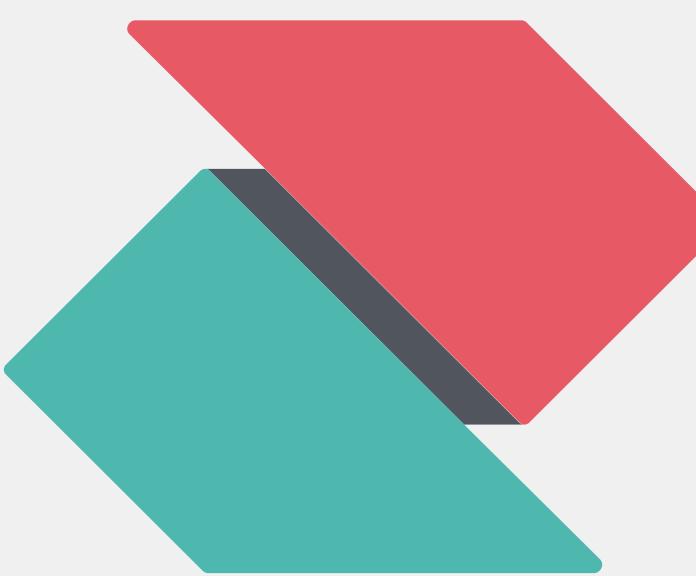
```
MacBook-Dev:~ std$ santactl fileinfo /Applications/Android\ Studio.app
Path          : /Applications/Android Studio.app/Contents/MacOS/studio
SHA-256       : 346f84d059d652674bbb51c7692005d527cbd6461d3c7d92eb77bd1b88c87500
SHA-1         : 92fd1c9ad1e295b1c35f08e972aea9a1d008c442
Bundle Name   : Android Studio
Bundle Version: AI-162.3764568
Bundle Version Str: 2.3
Type          : Executable (x86-64, i386)
Code-signed   : Yes
Rule          : Whitelisted (Certificate)

 Signing Chain:
 1. SHA-256      : 33b9aeee3b089c922952c9240a40a0daa271bebf192cf3f7d964722e8f2170e48
    SHA-1        : 34f0bdf7f87d4f3a955862c351472e52250e4c2b
    Common Name  : Developer ID Application: Google, Inc. (EQHXZ8M8AV)
    Organization : Google, Inc.
    Organizational Unit: GOOGLE
    ROM
    File
```

The following application has been blocked from executing because its trustworthiness cannot be determined.

Filename	Path	Signature
jspawnhelper	/Applications/Android Studio.app/Contents/jre/jdk/Contents/Home/jre/lib/jspawnhelper	Not code-signed
ba60ef8ffb373cd1ae047368146ab8d8	/db03e8a08fb31125544a04cc567b0f	hd (1)

this application for a day



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)

The screenshot shows the zentral web application interface. At the top, there's a navigation bar with the zentral logo, 'Inventory', 'Probes', and a URL 'zentral.apfelwein'. Below the navigation, the breadcrumb path is 'Home / Probes / 1Password security settings'. The main title is 'Probe 1Password security settings'. It displays probe details: status 'Active', feed 'Osquery demo', and feed probe '1Password security settings'. Below this are buttons for 'Edit' (red), 'Delete' (red), and links to 'Events', 'Dashboard', 'elasticsearch', and 'Export gist'. A 'Filters' section has a 'Add filter' button. The 'Osquery compliance' section has an 'Add' button. The 'Preference file' section shows a snippet of a plist file:

```
/Users/%/Library/Preferences/2BUA8C4S2C.com.agilebits.onepassword4-helper.plist
ClearPasteboardAfterTimeout = 1
InvisiblePasswords = 1
Idle = 1
ScreenSaver = 1
= 1
integer ≤ 5
integer ≤ 90
Agilebits recommended defaults
```



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

Slack
Team chat
notifications

Trello

Trello
Kanban Board
workflows

zendesk

Zendesk
Ticketing system
workflows

JIRA

Jira
Ticketing system
workflows

Supported actions

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



Workshop / Demo





Deployment options



Google Cloud Platform

GoogleCloudPlatform

zentral-all-in-one image
SaaS Zentral
+ Support contract

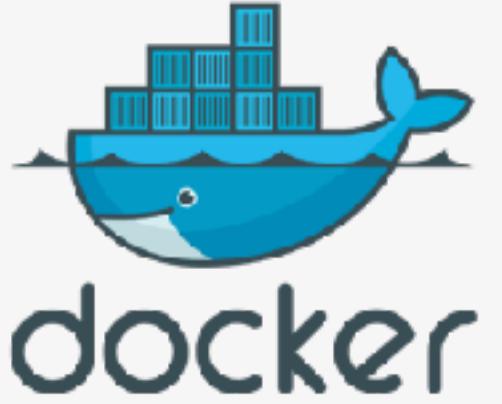
production



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)

A black and white photograph of a server room. Rows of server racks are visible on both sides, receding into the distance. The ceiling has a grid of lights and ventilation ducts.

info@zentral.io



Thank you !