

# Santa In-Depth

April-2019-macadmins-meeting

by Zentral.Pro

Henry Stamerjohann

twitter: @head\_min



# Zentral Pro Services

<https://www.zentral.pro>

- Consultancy
- Research & Development
- Based in Hamburg, Germany
- Creators of **Zentral** (open source)

# Santa In-Depth

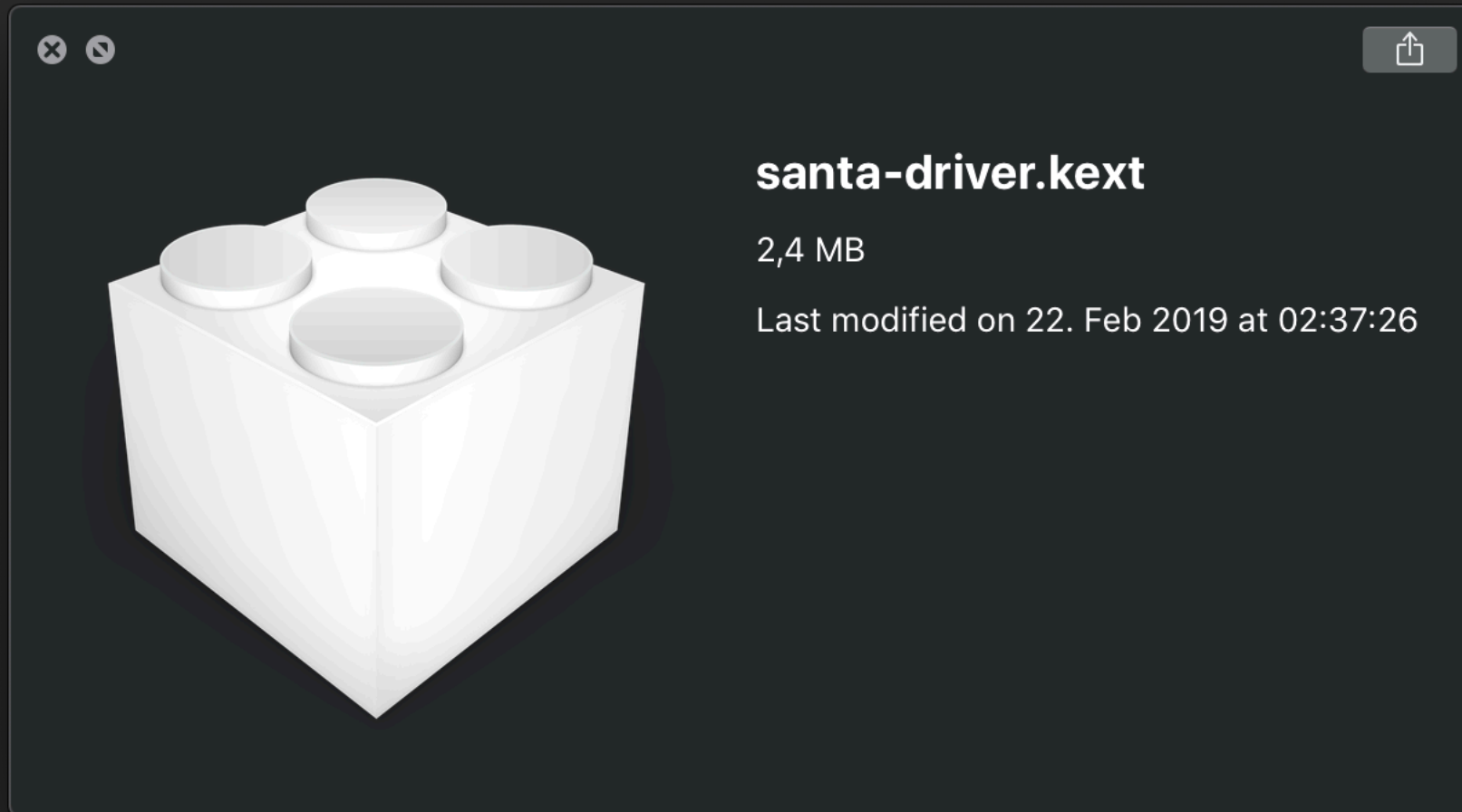
# What is Santa?

A binary whitelisting/blacklisting system for macOS ( $\geq 10.12$ )

- KEXT monitors executions
- Userland daemon makes execution decisions, based on rules
- GUI agent notifies user (*in case of a block decision*)
- managed via a CLI utility or a sync server
- configuration profile required for setup

Project on Github: <https://github.com/google/santa>

# Kernel Extension




- install path `/Library/Extensions/`
- Signed by Google
- Notarized soon (according to the developers)
- Attention: UAKEL better MDM KEXT whitelisting (*required*)

santa-0.9.31.pkg Update Available ▾

**Package Info** | **All Files** | **All Scripts**

Name	Date Modified	Size	Kind
Library	--	2,4 MB	Folder
Extensions	--	2,4 MB	Folder
santa-driver.kext	--	2,4 MB	Kernel extension
Contents	--	2,4 MB	Folder
_CodeSignature	--	6 KB	Folder
Info.plist	22.02.19, 02:37	2 KB	Property list
MacOS	--	1,4 MB	Folder
Resources	--	599 KB	Folder
Santa.app	--	599 KB	Application
XPCServices	--	364 KB	Folder
santabs.xpc	--	364 KB	XPC Service
LaunchAgents	--	531 bytes	Folder
com.google.santagui.plist	22.02.19, 02:37	531 bytes	Launchd job configuration
LaunchDaemons	--	658 bytes	Folder
com.google.santad.plist	22.02.19, 02:37	658 bytes	Launchd job configuration
private	--	632 bytes	Folder
etc	--	632 bytes	Folder
asl	--	447 bytes	Folder
newsyslog.d	--	185 bytes	Folder



Name **Santa.app**  
 Kind **Application**  
 Size **599 KB**  
 Modified --  
 Owner **root**  
 Group **wheel**

Permissions

root	Read & Write
wheel	Read only
Everyo...	Read only

Version --  
 Identifier --

All Files > Library > Extensions > santa-driver.kext > Contents > Resources > Santa.app

2 items, 2,4 MB installed

# Santa rules

- 2 kinds of executable matching:
  - **binary** – hash of the executable
  - **certificate** – hash of a signature certificate, anywhere in the signature chain
- 4 different policies:
  - BLACKLIST / SILENT BLACKLIST
  - WHITELIST
  - REMOVE

# Santa rule extra

- **Default rules** whitelist the executables signed by the same leaf certificates used for `santad` and `launchd`, to avoid locking the whole system.
- 4 critical binaries `trustd`, `securityd`, `xpcproxy`, `ocspd` get **individual binary whitelisting rules**, with extra decision information
- 2 different regexes available to respectively blacklist or whitelist executables based on their paths.

*Note: Only use if no other option is available*



# Santa modes

There are 2 modes: **Monitor** the default one and **Lockdown**.

The mode is set in the configuration profile or remotely with a sync server.

# lockdown mode

- Nothing runs unless it is approved with **whitelist** rules
- Very restrictive
- You have to maintain an up to date list of application hashes or signature certificates
- You know exactly what is allowed to run

## monitor mode

- Block specific apps with **blacklist** rules
- Unknown apps are allowed and the executions are logged (*good & bad*)
- Less administrative overhead

# CLI santactl

Get binary hash and code-signing information:

```
/usr/local/bin/santactl fileinfo </path/to/app>
```

```
santactl fileinfo "/Applications/Firefox.app"
Path           : /Applications/Firefox.app/Contents/MacOS/firefox
SHA-256        : 9c93b9a5bb4d6b6e19aeba8fff7963a3b431802f4e5b1465e8608cbeae71d1bf
SHA-1          : 7d46625d3fc42ee1712eae57e207606a9bca881c
Bundle Name    : Firefox
Bundle Version : 6619.4.9
Bundle Version Str : 66.0.3
Type           : Executable (x86_64)
Code-signed    : Yes
Rule           : Whitelisted (Unknown)
Signing Chain:
  1. SHA-256    : 96f18e09d65445985c7df5df74ef152a0bc42e8934175a626180d9700c343e7b
     SHA-1      : 266aa401a13906b0423b5332364f840587fd7a36
     Common Name : Developer ID Application: Mozilla Corporation (43AQ936H96)
     Organization : Mozilla Corporation
     Organizational Unit : 43AQ936H96
     Valid From   : 2017/05/08 21:08:58 +0200
```

# CLI santactl

## Set binary blacklist rule:

```
/usr/local/bin/santactl rule --blacklist --path </path/to/app>  
/usr/local/bin/santactl rule --blacklist --sha256 <sha256_hash>
```

```
● ● ●  
  
# block an app from path  
sudo santactl rule --blacklist --path "/Applications/macOS Compton.app"  
--message "Hey sorry, we're not yet ready for most wanted macOS 10.15 beta"  
Added rule for SHA-256:  
b379d6f11c3e9d318b517d25248477c50561b4d740a834bbdf74ccaecae7e53.  
  
# un-block app from path  
sudo santactl rule --remove --path "/Applications/macOS Compton.app"  
Removed rule for SHA-256:  
b379d6f11c3e9d318b517d25248477c50561b4d740a834bbdf74ccaecae7e53
```

# CLI santactl

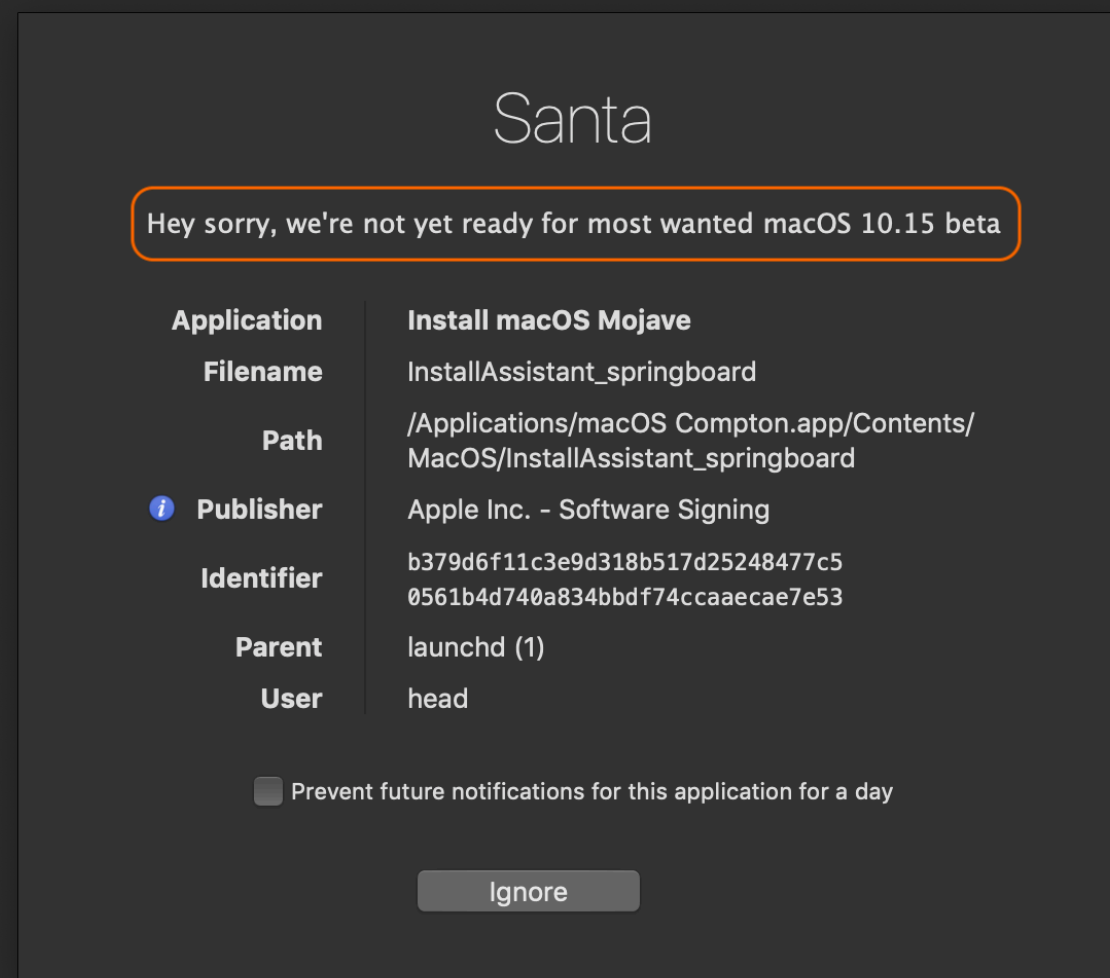
## Set binary blacklist rule with custom message:

```
/usr/local/bin/santactl rule --blacklist --path </path/to/app> --message "<custom message>"
```

```
● ● ●  
  
# block an app from path  
sudo santactl rule --blacklist --path "/Applications/macOS Compton.app"  
--message "Hey sorry, we're not yet ready for most wanted macOS 10.15 beta"  
Added rule for SHA-256:  
b379d6f11c3e9d318b517d25248477c50561b4d740a834bbdf74ccaecae7e53.  
  
# un-block app from path  
sudo santactl rule --remove --path "/Applications/macOS Compton.app"  
Removed rule for SHA-256:  
b379d6f11c3e9d318b517d25248477c50561b4d740a834bbdf74ccaecae7e53
```

# Santa Rule (*in action*)

- User facing alert with details



# Logging

2 destinations for the logs:

- logs:
  - simple structure written to `/var/db/santa/santa.log`
  - contain all the information
- events:
  - posted to the sync server to be aggregated and analysed
  - only the important information (*blocked, unknown exec*)



# executable - decisions

- ALLOW\_UNKNOWN - Monitor mode only
- ALLOW\_BINARY - Not in the events, logs only
- ALLOW\_CERTIFICATE - Not in the events, logs only
- ALLOW\_SCOPE - Not in the events, logs only
- BLOCK\_BINARY
- BLOCK\_CERTIFICATE
- BLOCK\_SCOPE
- BLOCK\_UNKNOWN - Lockdown mode only

# local logs (*in action*)

Decision: ALLOW\_CERT

```
●●●  
  
# santa.log - logging a fleetsmith install process  
[2019-04-15T19:59:21.890Z] I santad:  
action=EXEC|decision=ALLOW|reason=CERT|sha256=53a9a4112935ecf513eb1883118dbdf753  
553931f70517fb159069a05015bd3c|cert_sha256=2aa4b9973b7ba07add447ee4da8b5337c3ee2  
c3a991911e80e7282e8a751fc32|cert_cn=Software  
Signing|pid=21872|ppid=210|uid=0|user=root|gid=0|group=wheel|mode=M|path=/usr/sb  
in/installer|args=/usr/sbin/installer -verboseR -target / -pkg  
/opt/fleetsmith/data/downloads/filebeat-6.7.1.pkg  
  
# santa.log - logging a manual munki run  
[2019-04-15T20:02:07.438Z] I santad:  
action=EXEC|decision=ALLOW|reason=CERT|sha256=7ccac19e573f8d93165aa5fa193a9cf0fa  
9b3b97173a70916afff39fdb91aab|cert_sha256=2aa4b9973b7ba07add447ee4da8b5337c3ee2  
c3a991911e80e7282e8a751fc32|cert_cn=Software  
Signing|pid=22124|ppid=1|uid=0|user=root|gid=0|group=wheel|mode=M|path=/usr/bin/  
python|args=/usr/bin/python /usr/local/munki/supervisor --timeout 43200 --  
/usr/local/munki/managedsoftwareupdate --manualcheck
```

# local logs (*in action*)

Decisions: ALLOW\_UNKNOWN, ALLOW\_BINARY of a critical system (default rule).

```
# santa.log - PrivilegedHelperTools
[2019-04-16T07:10:47.437Z] I santad:
action=EXEC|decision=ALLOW|reason=UNKNOWN|sha256=dde54b033525e1cbbf3a5f52a71b2b796a688b
37d44d601dd39c41413b0e5317|cert_sha256=d9bcd1aca630bb95c39bbfaabc6959a4ec1c375811446a05
02711c2535fc794d|cert_cn=Developer ID Application: SAP SE (7R5ZEU67FQ)
|pid=54505|ppid=1|uid=0|user=root|gid=0|group=wheel|mode=M
|path=/Library/PrivilegedHelperTools/corp.sap.privileges.helper|args=/Library/Privilege
dHelperTools/corp.sap.privileges.helper

# santa.log - XPCProxy exec
[2019-04-16T07:10:48.804Z] I santad:
action=EXEC|decision=ALLOW|reason=BINARY|explain=critical system
binary|sha256=beb05fe9d3f8155bc4c142c115b0bc587eb667ba213b4f557ded08b9286f40bf|cert_sha
256=2aa4b9973b7ba07add447ee4da8b5337c3ee2c3a991911e80e7282e8a751fc32|cert_cn=Software
Signing|pid=54506|ppid=1|uid=0|user=root|gid=0|group=wheel|mode=M|path=/usr/libexec/xpc
proxy|args=xpcproxy corp.sap.privileges.30
```

## local logs - file changes monitoring

An extra configuration parameter - **FileChangesRegex** – can be set using the configuration profile (only).

All operations on matching files will be logged in the local logs (only):

```
<key>FileChangesRegex</key>
```

```
<string>^(/private/etc/.*/Users/Shared/.*)</string>
```

# FileChangesRegex in the local logs



```
# santa.log - create folder (/bin/mkdir)
[2019-04-16T10:46:21.420Z] I santad:
action=EXEC|decision=ALLOW|reason=CERT|sha256=e5d0328716e86c487f3e921b74589b2d7d60df0fe86df57f99c97f4ae
780ae57|cert_sha256=2aa4b9973b7ba07add447ee4da8b5337c3ee2c3a991911e80e7282e8a751fc32|cert_cn=Software
Signing|pid=79852|ppid=79730|uid=501|user=head|gid=20|group=staff|mode=M|path=/bin/mkdir|args=mkdir
hello Utah

# santa.log - create a file (/usr/bin/touch)
[2019-04-16T10:46:22.757Z] I santad: action=WRITE|path=/Users/Shared/hello Utah/hello_file.txt
|pid=79|ppid=1|process=mds|processpath=/System/Library/Frameworks/CoreServices.framework/Versions/A/Fra
meworks/Metadata.framework/Versions/A/Support/mds|uid=0|user=root|gid=0|group=wheel

# santa.log - remove a file (/bin/rm)
[2019-04-16T10:51:14.321Z] I santad: action=DELETE|path=/Users/Shared/hello Utah/hello_file.txt
|pid=80368|ppid=79730|process=rm|processpath=/bin/rm|uid=501|user=head|gid=20|group=staff
```

uploaded events

Discover: Santa Events Filtered 10 hits

Search... (e.g. status:200 AND extension:PHP) Options Refresh

Santa Filtered Add a filter + Actions

zentral-events April 16th 2019, 09:28:07.372 - April 16th 2019, 09:58:07.372 Auto

Count

created\_at per 30 seconds

Time	santa_event.file_bundle_id	santa_event.decision	santa_event.file_path	santa_event.file_name
▶ April 16th 2019, 09:45:32.263	name.tuley.jay.cdto	<b>BLOCK_BINARY</b>	/Applications/cd to.app/Contents/MacOS	cd to
▶ April 16th 2019, 09:40:20.283	-	ALLOW_UNKNOWN	/usr/local/bin	osqueryd
▶ April 16th 2019, 09:40:00.016	com.apple.Server.v4	ALLOW_UNKNOWN	/Applications/Server.app/Contents/ServerRoot/usr/libexec	servermetricsd
▶ April 16th 2019, 09:35:00.015	com.apple.Server.v4	ALLOW_UNKNOWN	/Applications/Server.app/Contents/ServerRoot/usr/libexec	servermetricsd
▶ April 16th 2019, 09:30:56.866	-	ALLOW_UNKNOWN	/opt/fleetsmith/bin	fsupdater
▶ April 16th 2019, 09:30:21.213	-	ALLOW_UNKNOWN	/usr/local/bin	osqueryd
▶ April 16th 2019, 09:26:37.774	com.google.Chrome.helper	ALLOW_UNKNOWN	/Applications/Google Chrome.app/Contents/Versions/73.0.3683.103/Google Chrome Helper.app/Contents/MacOS	Google Chrome Helper
▶ April 16th 2019, 09:26:04.162	com.apple.servermgrd.plugin	ALLOW_UNKNOWN	/Applications/Server.app/Contents/ServerRoot/System/Library/CoreServices/ServerManagerDaemon.bundle/Contents/MacOS	servermgrd
▶ April 16th 2019, 09:25:01.235	com.apple.Server.v4	ALLOW_UNKNOWN	/Applications/Server.app/Contents/ServerRoot/usr/libexec	servermetricsd
▶ April 16th 2019, 09:20:20.633	-	ALLOW_UNKNOWN	/usr/local/bin	osqueryd

Selected fields

- t santa\_event.decision
- t santa\_event.file\_bundle\_id
- t santa\_event.file\_name
- t santa\_event.file\_path

Available fields

Popular

- t santa\_event.parent\_name
- t \_id
- t \_index
- # \_score
- t \_type
- 🕒 created\_at
- t id
- # index
- ? machine.jamf.groups
- t machine.jamf.name
- t machine.jamf.os\_version
- ? machine.meta\_business\_units
- t machine.munki.name
- t machine.munki.os\_version
- t machine.osquery.name

Santa Dashboard - Kibana

https://zentral.../kibana/app/kibana#/dashboard/b8438dd0-603c-11e9-8f13-2b1ed43f96d0?\_g=(refreshInterval:(pause:lt,value:0),time:(from:now

Dashboard / Santa Dashboard

Search... (e.g. status:200 AND extension:PHP) Options Refresh

Santa Filter Add a filter + Actions

Santa-Name-Tag-Cloud

Count - Santa events

Block Binary

santa\_event.decision: Descending

Decision	Count
ALLOW_UNKNOWN	~110
BLOCK_BINARY	~10

Santa Pie

- ALLOW\_UNKNOWN
- BLOCK\_BINARY
- com.apple.Server.v4
- com.google.Chrome...
- com.objective-see.W...
- com.tinyspeck.slack...
- org.mozilla.firefox
- name.tuley.jay.cdto

Santa Events Filtered

1-50 of 116

Time	santa_event.file_bundle_id	santa_event.decision	santa_event.file_path	santa_event.file_name	machine_serial_number	santa_event.file_sha256
▶ April 16th 2019, 13:55:00.030	com.apple.Server.v4	ALLOW_UNKNOWN	/Applications/Server.app/Contents/ServerRoot/usr/lib/exec	servermetricsd	C02 HD3	04e470de35b713d7882eac9b707a9a465e843e96e09c1e3f2941fb103997a262
▶ April 16th 2019, 13:45:00.021	com.apple.Server.v4	ALLOW_UNKNOWN	/Applications/Server.app/Contents/ServerRoot/usr/lib/exec	servermetricsd	C02 HD3	04e470de35b713d7882eac9b707a9a465e843e96e09c1e3f2941fb103997a262
▶ April 16th 2019, 13:43:17.988	com.google.Chrome.helper	ALLOW_UNKNOWN	/Applications/Google Chrome.app/Contents/Versions/73.0.3683.103/Google Chrome Helper.app/Contents/MacOS	Google Chrome Helper	C02 HD3	bb5b77d84c49f77ffa31684034d4b426fa9eb65481586957fb18a99e48b97be8
▶ April 16th 2019, 13:38:36.576	com.google.Chrome.helper	ALLOW_UNKNOWN	/Applications/Google Chrome.app/Contents/Versions/73.0.3683.103/Google Chrome Helper.app/Contents/MacOS	Google Chrome Helper	C02 HD3	bb5b77d84c49f77ffa31684034d4b426fa9eb65481586957fb18a99e48b97be8



Santa Dashboard - Kibana

https://zentral.../kibana/app/kibana#/dashboard/b8438dd0-603c-11e9-8f13-2b1ed43f96d0?\_g=(refreshInterval:(pause:lt,value:0),time:(from:now...))

Dashboard / Santa Dashboard

Search... (e.g. status:200 AND extension:PHP)

Santa Filter: **santa\_event.decision: "BLOCK\_BINARY"** Add a filter +

Santa-Name-Tag-Cloud

cd to

Count - Santa events

Block Binary

Santa Pie

Santa Events Filtered

Time	santa_event.file_bundle_id	santa_event.decision	santa_event.file_path	santa_event.file_name	machine_serial_number	santa_event.file_sha256
April 16th 2019, 09:45:32.263	name.tuley.jay.cdto	<b>BLOCK_BINARY</b>	/Applications/cd to.app/Contents/Ma cOS	cd to	C02 ID3	14256b9bd0969ee016f2a2bf4c70b87e73392afe6cff3b164dd cab9f6786481b
April 16th 2019, 08:33:18.782	name.tuley.jay.cdto	<b>BLOCK_BINARY</b>	/Applications/cd to.app/Contents/Ma cOS	cd to	C02 ID3	14256b9bd0969ee016f2a2bf4c70b87e73392afe6cff3b164dd cab9f6786481b

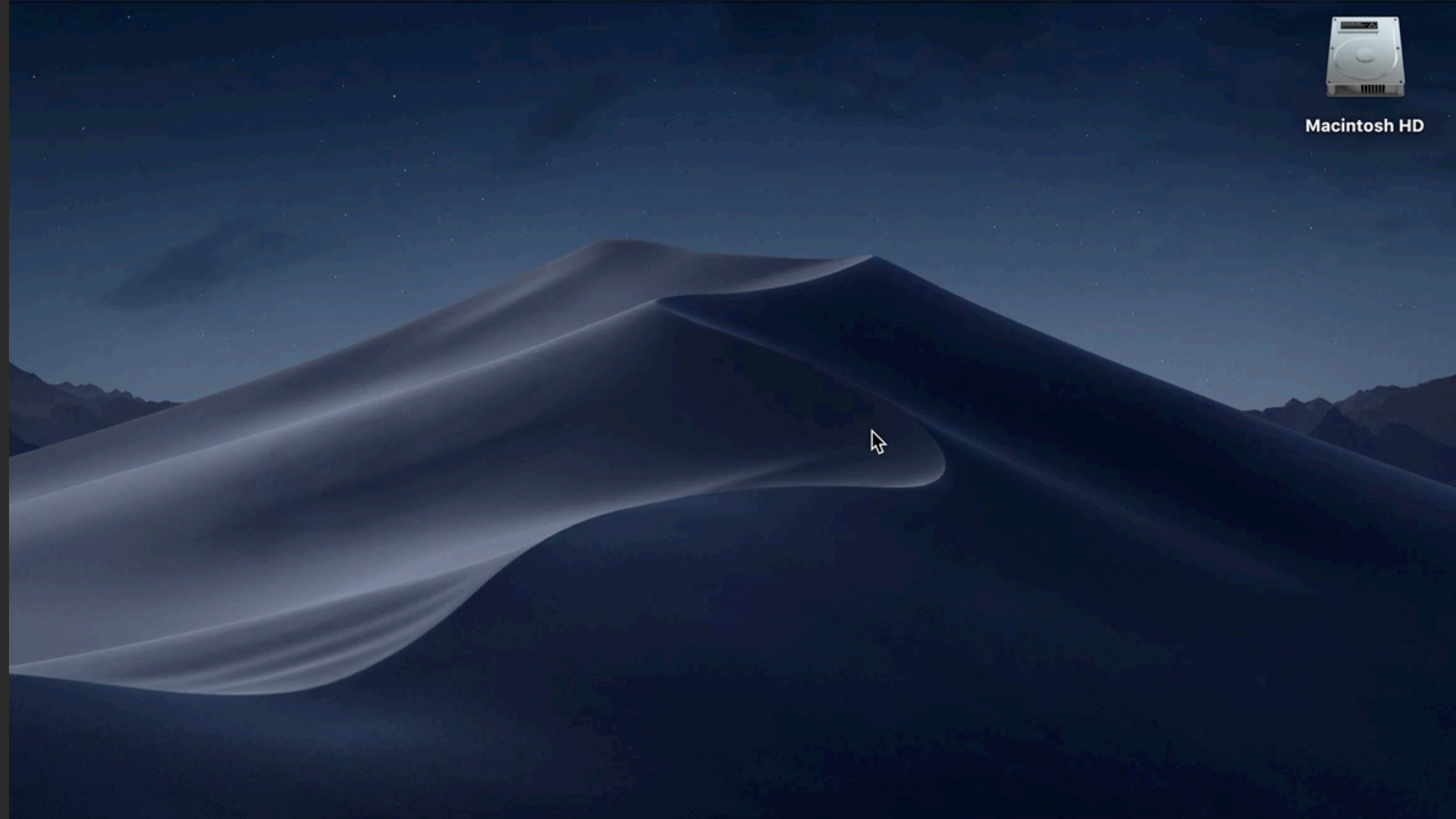
# Santa (*in action*)

Quick demo

1. Switch mode to *LOCKDOWN*
2. Block App - defaults deny
3. Switch mode to *MONITORING*
4. Allow App launch



Macintosh HD



- *Lockdown Mode* - carefully track what will be blocked

Santa

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

<b>Application</b>	<b>Google Chrome Helper</b>
<b>Filename</b>	Google Chrome Helper
<b>Path</b>	/Applications/Google Chrome.app/Contents/Versions/73.0.3683.103/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper
<b><i>i</i> Publisher</b>	Google, Inc. - Developer ID Application: Google, Inc. (EQHXZ8M8AV)
<b>Identifier</b>	bb5b77d84c49f77ffa31684034d4b426 fa9eb65481586957fb18a99e48b97be8
<b>Parent</b>	launchd (1)
<b>User</b>	head

Prevent future notifications for this application for a day

Ignore

Santa

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

<b>Application</b>	<b>Jamf Connect Sync Redirector</b>
<b>Filename</b>	Jamf Connect Redirector
<b>Path</b>	/Applications/Jamf Connect Sync.app/Contents/PlugIns/Jamf Connect Redirector.appex/Contents/MacOS/Jamf Connect Redirector
<b><i>i</i> Publisher</b>	JAMF Software - Mac Developer: Joel Rennich (NZR8GR3MD9)
<b>Identifier</b>	9b09bec11b838014a2a324bcfe53d923 516ba1c17023441f3cdab40ab4e60748
<b>Parent</b>	launchd (1)
<b>User</b>	head

Prevent future notifications for this application for a day

Ignore

The screenshot shows a web browser window with the URL `https://santa.readthedocs.io/en/latest/deployment/configuration/`. The page features a dark sidebar on the left with a search bar and a navigation menu. The main content area has a red header with the 'Santa' logo and a search bar. Below the header, there are sections for 'Important', 'Configuration', and 'Local Configuration Profile'. The 'Local Configuration Profile' section contains a table with columns for 'Key', 'Value Type', and 'Description'. A 'v: latest' dropdown menu is visible in the bottom right corner of the page.

**Important**

Santa v0.9.21 has moved to using an Apple [Configuration Profile](#) to manage the local configuration. The old config file ( `/var/db/santa/config.plist` ) is no longer used.

## Configuration

Two configuration methods can be used to control Santa: a local configuration profile and a sync server controlled configuration. There are certain options that can only be controlled with a local configuration profile and others that can only be controlled with a sync server controlled configuration. Additionally, there are options that can be controlled by both.

### Local Configuration Profile

Key	Value Type	Description
ClientMode*	Integer	1 = MONITOR, 2 = LOCKDOWN, defaults to MONITOR
FileChangesRegex*	String	The regex of paths to log file changes. Regexes are specified in ICU format.
WhitelistRegex*	String	A regex to whitelist if the binary or certificate scopes did not allow execution. Regexes are specified in ICU format.
BlacklistRegex*	String	A regex to blacklist if the binary or certificate scopes did not block an execution. Regexes are specified in ICU format.
EnablePageZeroProtection	Bool	Enable <code>__PAGEZERO</code> protection, defaults to YES. If this flag is set to YES, 32-bit binaries that are missing the <code>__PAGEZERO</code> segment will be blocked even in MONITOR mode, unless the binary is whitelisted by an explicit rule.
MoreInfoURL	String	The URL to open when the user clicks "More Info..." when opening Santa.app. If unset, the button will not be displayed.
EventDetailURL	String	See the <a href="#">EventDetailURL</a> section below.
EventDetailText	String	Related to the above property, this string represents the text to show on the button.

<https://santa.readthedocs.io/en/latest/>


# Santa deployment

- Free & open source full sync server projects:
  - Moroz
  - Zentral
  - Upvote
- Commercial - remote config & rules:
  - Fleetsmith

GitHub - groob/moroz: Moroz 1: X

GitHub, Inc. (US) | https://github.com/groob/moroz

README.md



Moroz is a server for the [Santa](#) project.

Santa is a binary whitelisting/blacklisting system for macOS. It consists of a kernel extension that monitors for executions, a userland daemon that makes execution decisions based on the contents of a SQLite database, a GUI agent that notifies the user in case of a block decision and a command-line utility for managing the system and synchronizing the database with a server.

Santa is a project of Google's Macintosh Operations Team.

See this [short video](#) for a demo.

## Configurations

Moroz uses [TOML](#) rule files to specify configuration for Santa. The path to the folder with the configurations can be specified with `-configs /path/to/configs`.

Moroz expects a `global.toml` file which contains a list of rules. The `global` config can be overridden by providing a machine specific config. To do so, name the file for each host with the `santa machine_id configuration parameter`. By default, this is the hardware UUID of the mac.

Below is a sample configuration file:

```
client_mode = "MONITOR"
```

<https://github.com/groob/moroz>

Home - zentralopensource/zentral X +

GitHub, Inc. (US) | https://github.com/zentralopensource/zentral/wiki


zentralopensource / zentral

Watch 35 Star 385 Fork 43

Code Issues 16 Pull requests 3 Projects 1 Wiki Insights

## Home

headmin edited this page on Jan 20, 2018 · 27 revisions



## Zentral

### Quickstart

You're impatient? You want to try it now before reading the docs? Check [Docker](#) for the quickest path to get you started.

### What is Zentral?

[Zentral](#) is a open source Framework and server solution to gather, process, and monitor system events and link them to an inventory.

[Zentral](#) is a centralized service to manage configurations for [osquery](#)'s powerful endpoint inventory and security features. Zentral also support [Google Santa](#) in a similar way. A build in

Pages 22

Find a Page...

- [Home](#)
- [aws elasticsearch service](#)
- [client enroll](#)
- [config create probe](#)
- [deployment aws](#)
- [deployment docker](#)
- [deployment gcp](#)
- [deployment overview](#)
- [deployment vagrant](#)
- [deployment vmware](#)
- [dev recommendation for agents](#)
- [event types](#)
- [faq](#)
- [monolith reference](#)
- [release notes](#)

Show 7 more pages...

<https://github.com/zentralopensource/zentral/wiki>




GitHub - google/upvote: A multi-... X

GitHub, Inc. (US) | https://github.com/google/upvote

README.md

# Upvote build passing

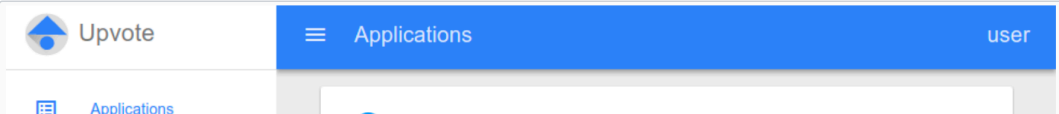


Upvote is a multi-platform binary whitelisting solution. It provides both a sync server and management interface for binary enforcement clients. Upvote currently supports [Santa](#) on macOS and [Bit9](#) (now known as Carbon Black Protection) on Windows.

## Features

- **First-party sync server for Santa**
  - Written in coordination with Santa's development team
- **User-oriented Policy Creation**
  - Apply policies to users instead of hosts
  - No migration necessary when users get new hosts
- **BigQuery streaming**
  - Fast, easy, and scalable relational access to Santa and Bit9 execution data
- **Bundled Voting for .app bundles on macOS**
  - Easily create policy for an entire bundle at once
- **VirusTotal Integration**
  - View VirusTotal results directly in the detail page

## Screenshot



<https://github.com/google/upvote>

Google Santa | Fleetsmith

https://fleetsmith.com/apps/

FLEETSMITH

Apps & Settings

Google Santa

Henry

My Fleet **NEW**


Devices

Apps & Settings

Users

Profiles

MDM & DEP

 **Google Santa**  
0.9.31

Santa can analyze what applications run across your fleet and control them by blocking their use entirely. Santa can be configured to prevent users from using malicious, high risk, or prohibited applications. Santa is an open-source project from Google's Macintosh Operations Team.

Publisher: [Google, Inc.](#)  
Latest version: 0.9.31  
System requirements: 10.12.0

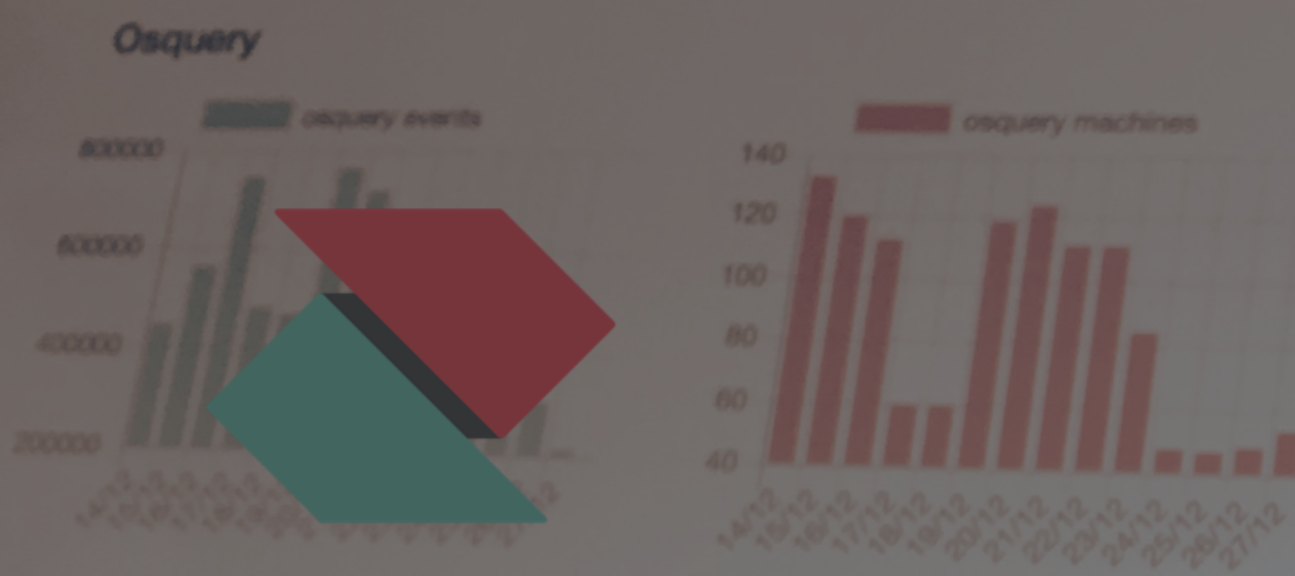
Google Santa requires kernel extensions for a successful deployment on devices running macOS 10.13.0 or higher. Partially Managed devices will require user interaction to "Allow" kernel extensions before installation.

Google Santa hasn't been added to any profiles 😞  
Select a profile below to manage Google Santa on your devices

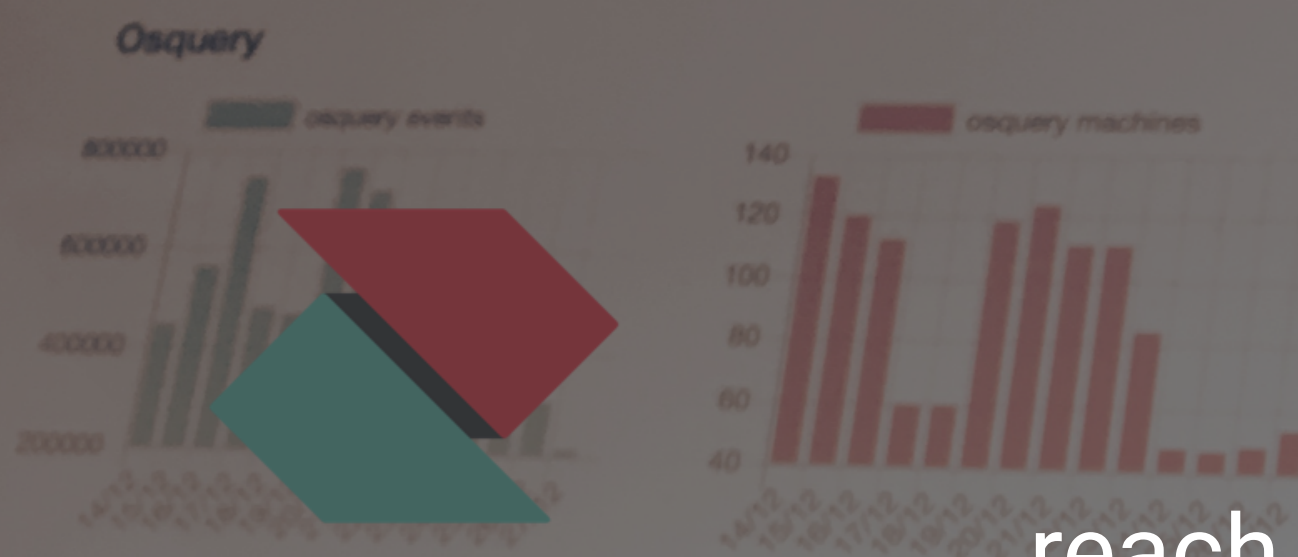
▼

Add to a Profile... Add

<https://www.fleetsmith.com/>



Thank You !



...reach out for R&D, consulting

Contact us via:

Web: <https://www.zentral.pro>

or Macadmins Slack