

Useful techniques for a successful Santa deployment



Henry Stamerjohann, June 11 2021

<https://zentral.pro>

Whats ahead

Fleet-wide use of binary authorization and control

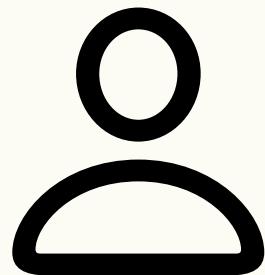
Deploying Google Santa for binary control under macOS

Collecting information about the executables

Organize rules and policies for provisioning to the endpoints

When you begin with a binary control

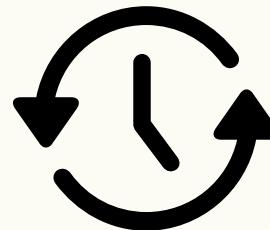
There are a number of questions that need to be clarified



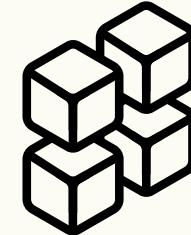
Who



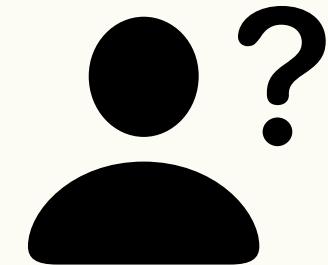
What



When



Where



Why

Look at Google Santa

A leading binary authorization system for macOS

- Userland daemon makes execution decisions
- Based on signing certificate or binary hash (SHA-256)
- Endpoint Security Extension for macOS 10.15 and higher*
- Rules and events could be synced with a server



*Kernel Extension available for older macOS versions

Rules and policies

Declare and control based on sha-256 information

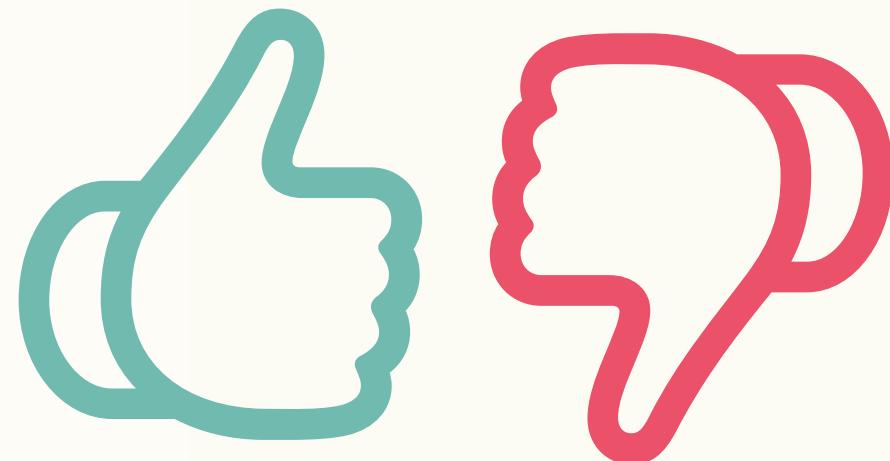
```
Santa-Rules.md

Santa Rules

• Target type: CERTIFICATE | BINARY | BUNDLE
• Target sha256: <hash to add/remove/check>
• Policy: ALLOWLIST | BLOCKLIST | SILENT BLOCKLIST | ALLOWLIST COMPILER
• Custom message: custom message to display

example

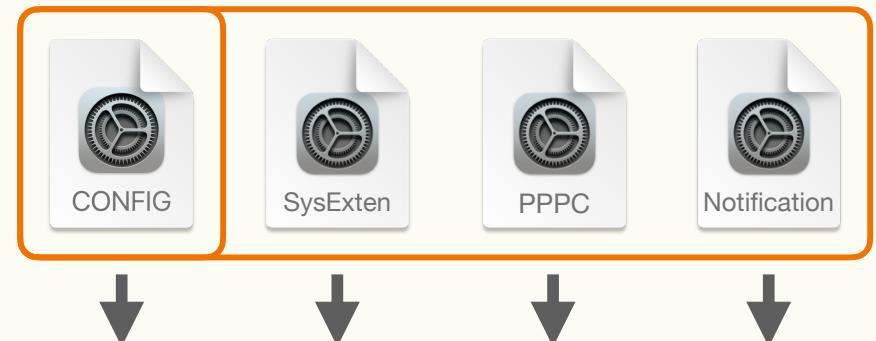
# Add rule, allow based on certificate sha256
sudo santactl rule --allow --certificate --sha256 c0fb0030f381b2794b4be8722616b806787a0...
```



What is required to deploy Santa

Deploy required settings via MDM

- Configuration
- Installation package
- System Extension policy payload
- PPPC payload (allow full disk access)
- Notification payload



```
# santactl - the santa command line tool
santactl version
santa-driver | un-needed (SystemExtension being used)
santad | 2021.5
santactl | 2021.5
SantaGUI | 2021.5

# systemextensionsctl - show active extension listing
systemextensionsctl list
1 extension(s)
--- com.apple.system_extension.endpoint_security
enabled active teamID bundleID (version) name [state]
* * EQHXZ8M8AV com.google.santa.daemon (2021.5/2021.5) santad [activated enabled]
```

This Mac is supervised and managed by Zentral Pro Services GmbH & Co. KG.

Sync server config

MDM distributed setting

- Client mode
(LOCKDOWN, MONITORING)
- Mutual TLS option (device certificate)
- Sync interval, batch size
- Allowed/blocked path regex
- Info URL for blocked executions

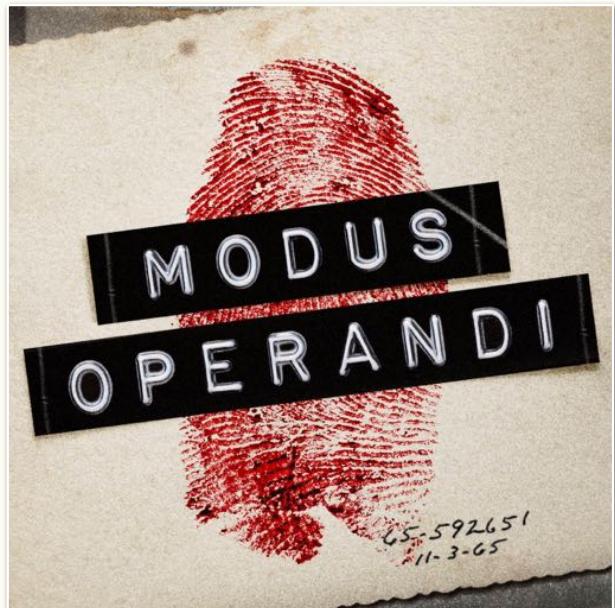
The screenshot shows a macOS application window titled "Santa". The left sidebar contains navigation links: Introduction, Welcome to Santa, Binary Authorization Overview, Syncing Overview, Deployment, Configuration (selected), Local Configuration Profile, Sync server Provided Configuration, Development, Building, Details, santa-driver, santactl, santabot, santacli, santa-gui, mode, events, rules, scopes, ipc, logs. The main content area is titled "Sync server Provided Configuration" and lists configuration options:

Key	Type	Description
client_mode	String	MONITOR or LOCKDOWN, defaults to MONITOR.
clear_sync**	Bool	If set to <code>true</code> , Santa will clear all local rules and download a fresh copy from the sync-server. Defaults to <code>false</code> .
batch_size	Integer	The number of rules to download or events to upload per request. Multiple requests will be made if there is more work than can fit in single request. Defaults to 10.
upload_logs_url**	String	If set, the endpoint to send Santa's current logs. No default.
allowed_path_regex	String	Same as the "Local Configuration" AllowedPathRegex. No default.
blocked_path_regex	String	Same as the "Local Configuration" BlockedPathRegex. No default.
full_sync_interval*	Integer	The max time to wait before performing a full sync with the server. (Defaults to 600 secs (30 minutes) if not set.)
token_token*	String	The FCM token used by Santa to listen for FCM messages. Unique for every machine. No default.
token_full_sync_interval*	Integer	The full sync interval if a token_token is set. (Defaults to 14400 secs (4 hours).)
token_global_rule_sync_deadline*	Integer	The max time to wait before performing a rule sync when a global rule sync FCM message is received. This allows syncing to be staggered for global events to avoid spikes in server load. Defaults to 600 secs (10 min).
enable_bundles*	Bool	If set to <code>true</code> , the bundle scanning feature is enabled. Defaults to <code>false</code> .
enable_transitive_rules	Bool	If set to <code>true</code> , the transitive rule feature is enabled. Defaults to <code>false</code> .

*Hold only in memory. Not persistent upon process restart.

Operational mode

Deny or monitor binary execution



MONITORING / LOCKDOWN

Know what to control

Gathering sha256 hash information

- Vendor code signed and binary details
- Use `santactl` to scan a local system
- Search in logs or data store (Splunk, et-al.)
- Fine tune collected information
- Build set of rules



Collecting event data

Perform inspection over time

The screenshot shows a Splunk search results page. On the left, a sidebar lists various event fields. In the center, a specific event is displayed with its timestamp and source. A modal window titled "santa_event.decision" is open, showing a table of values and their counts.

Values	Count	%
ALLOW_UNKNOWN	323	91.74%
BLOCK_UNKNOWN	10	3.11%
BLOCK_BINARY	11	3.15%

Below the table, the event's raw JSON data is visible, including fields like "namespaces", "probes", "request", "santa_event", "current_sessions", "decision", "executing_user", and "execution_file".

Collecting event data

Known apps/binaries no longer return ALLOW_UNKNOWN

The screenshot shows a Splunk search results page with the following details:

- Search Query:** index="santa" sourceType="santa.event" "santa.event.decision"="ALLOW_UNKNOWN" "santa.event.file_bundle_name"="Little Snitch Software Update"
- Time Range:** 4/13/21 2:00:00.000 AM to 4/13/21 3:00:00.000 AM
- Event Count:** > 90 events
- Event Timeline:** A horizontal timeline showing green bars representing event intervals. One bar is highlighted with a red border.
- Event List:** A table with columns: ID, Time, Event. One event is highlighted with a red border.

ID	Time	Event
1	4/13/21 2:48:56.706 AM	{ [-] id: 2072064-1f7e-48f1-aefb-aedaf0d9 index: # machine: { [-} } namespace: santa.event problem: { [-} } requestId: { [-} } santa.event: { [-} current_sessions: { [-} } decision: ALLOW_UNKNOWN executing_user: Henry execution_time: 1618274699.7063432 file_bundle_id: art.odev.littlesnitch.softwareupdate file_bundle_name: Little Snitch Software Update
- Annotations:** A red dotted arrow points from the highlighted timeline bar to the highlighted event in the list.
- Right Panel:** Shows two sections:
 - ALLOW_UNKNOWN recurring events:** A list of known vendor names.
 - ALLOW_CERTIFICATE known vendor name:** A list of known vendor names.
- Bottom Panel:** A terminal window showing command-line output for synchronization and rule validation.

Collecting event data

Known apps/binaries no longer return ALLOW_UNKNOWN

The screenshot shows a Splunk search results page for events indexed by 'santa' with source type 'santa_event'. The search results show 90 events from April 13, 2021, at 2:48 AM to 3:00 AM. The visualization section includes a timeline and a table of events. The event table highlights two rows:

ID	Time	Event
1	4/13/21 2:48:16 AM	{ [-] id: 21729645-1f7e-41f1-aefb-a8d4a0d01c index: # machine: { [-] } namespace: santa_event problem: { [-] } request_id: { [-] } santa_event: { [-] current_sessions: { [-] } } decision: ALLOW_UNKNOWN executing_user: bengy execution_time: 1618274699.7063432 file_bundle_id: art-objdev-little-santa-softwareupdate file_bundle_name: Little_Santa_software_update
2	4/13/21 2:48:16 AM	ALLOW_CERTIFICATE a known vendor now

A callout box on the right shows a file icon with a fingerprint and the command:

```
sudo santactl rule --allow  
--certificate --sha256  
0cabecede81a05175da0be5a3f825a  
25aa7e27f6a841e7cba7cd57ec
```

Another callout box shows terminal command output:

```
# Enforce synchronization with server  
sudo santactl sync  
Missing Machine Owner.  
Received 1 rules  
Processed 1 rules  
Sync completed successfully
```

```
# Validate rule status with sha-256 of a code-signed app  
sudo santactl rule --check --certificate --sha256 0cabecede81a05175da0be5a3f825a  
Allowed (Certificate)
```



Collecting event data

Watch out for the spill of ALLOW_UNKNOWN events

2021.3, Apple-signed binaries being flagged with ALLOW_UNKNOWN post 10.15.7 supplemental update/reboot #552

arubdesu commented on 27 Apr

I'm only seeing this on less than 1% of the deployed clients, but we're in monitor mode and the computers that recently upgraded to the 10.15.7 supplemental update (build 19H524) are sending hundreds of ALLOW_UNKNOWN events for Apple's binaries. The leaf signing cert is the same as launchd's, 2aa4b0f973b7ba07add447ee4daab533fc3ae2c3a991911e80e7252e8a75ff32 and logic would make me think they had to have rebooted to apply it so the fact we warm-upgraded to 2021.3 recently should not have had an effect, but perhaps there's something happening there. I have not been able to get a tech to see (or get a shell on) one of these devices exhibiting the symptom, but I'll follow up if I do.

Assignees: tburgen

Labels: bug

Projects: None yet

Milestone: No milestones

<https://github.com/google/santa/issues/552>

Gathering information

Exception workflow

- Direct users to a web page with more information about the event
- Limit approved exception to specific criteria (e.g. principal user)

The screenshot illustrates the Santa application's exception workflow across three panels:

- Santa Event Form:** A web-based form titled "Santa Event" where users can enter information to require access to an application. Fields include "File Sha" (daa9a265590206d24947d63846c39e704d63f), "Machine ID" (c6dc634-6426-4ae8-881a-cff33011a9f9), "Username" (jappleseed), "Serial" (FVFD74PZP05G), and "UUID".
- Blocked Application Details:** A modal window titled "Santa" showing details of a blocked application. It includes:
 - Application:** Tor Browser
 - Filename:** firefox
 - Path:** /var/folders/tx/ctps48q14wddw5fwy4d8c8xw000gn/T/AppTranslocation/F3C824C9-80B4-4F12-B128-5FD707CEE8E6/d/Tor Browser.app/Contents/MacOS/firefox
 - Publisher:** The Tor Project, Inc - Developer ID Application: The Tor Project, Inc (MADPSAYN6T)
 - Identifier:** daa9a265590206d24947d63846c39e704d63f
 - Bundle Identifier:** 803b780592ca7ac94d285fdacff6ce4bf7679b7e8ee159485ce08f09c4003d4
 - Parent:** launchd (1)
 - User:** jappleseed
- Principal User Configuration:** A panel titled "Principal user" showing configuration details for the "Santa" machine owner. It lists:
 - Source:** Santa machine owner
 - Unique ID:** jappleseed@zentral.pro
 - Principal name:** jappleseed@zentral.pro
- System Configuration:** A panel titled "Santa" listing system configuration details:
 - Configuration:** Default
 - Primary user:** jappleseed@zentral.pro
 - UUID:** c6dc634-6426-4ae8-881a-cff33011a9f9
 - Client mode:** Monitor
 - Version:** 2021.5
 - Binary rules:** 19
 - Certificate rules:** 38
 - Compiler rules:** 0
 - Transitive rules:** 0
- Key Definitions:** A table mapping keys to their descriptions:

KEY	DESCRIPTION
%file_sha%	SHA-256 of the file that was blocked
%machine_id%	ID of the machine
%username%	The executing user
%serial%	System's serial number
%uuid%	System's UUID
%hostname%	System's full hostname

Gathering information

Know in advance what is commonly used

RAW - collected sha256 hash info

Vendor - codesigned hashes

Binary exec - hashes

devtools exec - hashes

PROD Rules - processed sha256 hash info

Core operating
rules

Containment
mode rules

Common app / vendor rules

Devtools rules

Denylist rules

Exceptions requested
by users

Gathering information

Know in advance what is commonly used

RAW - collected sha256 hash info

Vendor - codesigned hashes

Binary exec - hashes

devtools exec - hashes

PROD Rules - processed sha256 hash info

Core operating
rules

Containment
mode rules

Common app / vendor rules

Devtools rules

Denylist rules

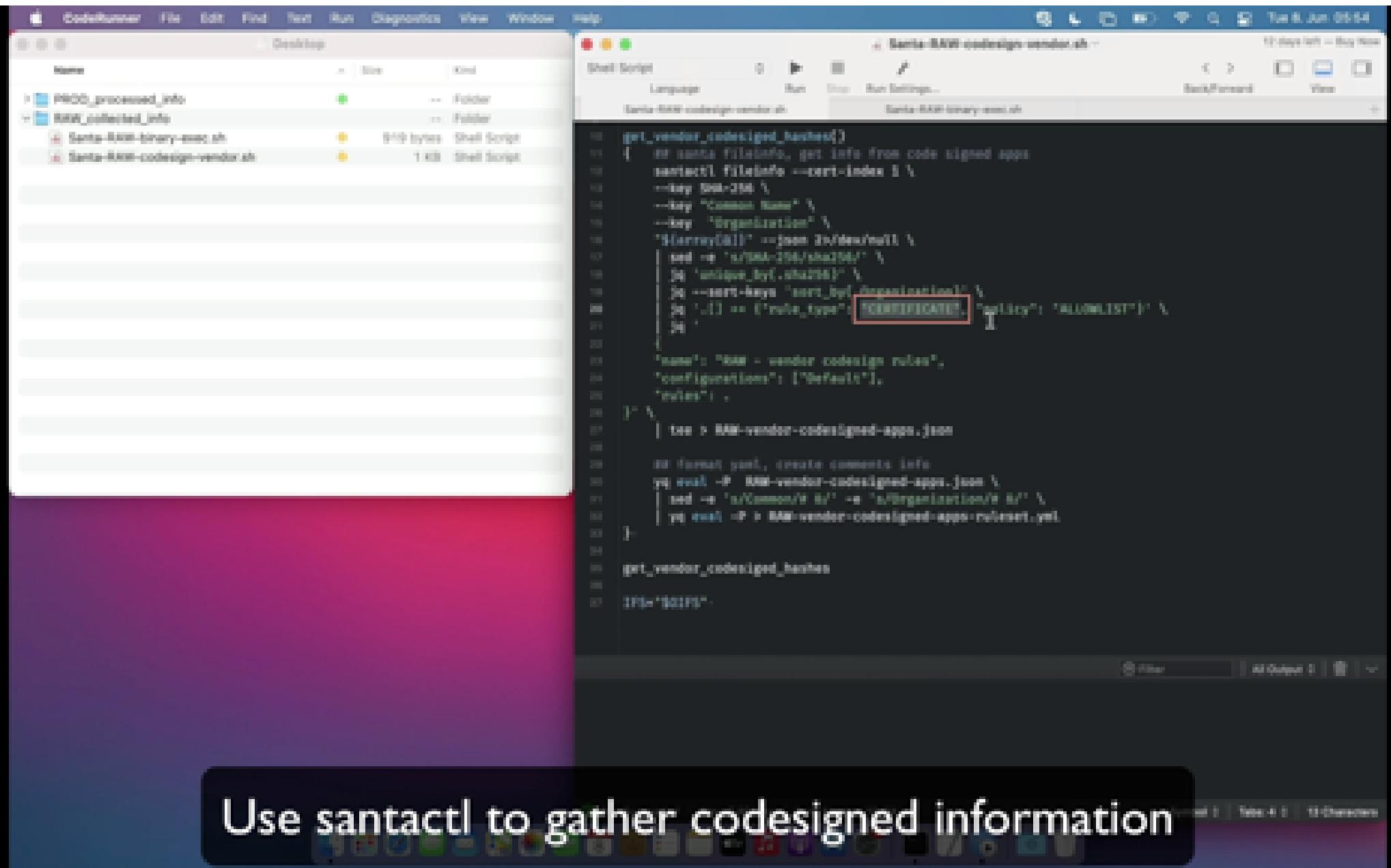
Exceptions requested
by users



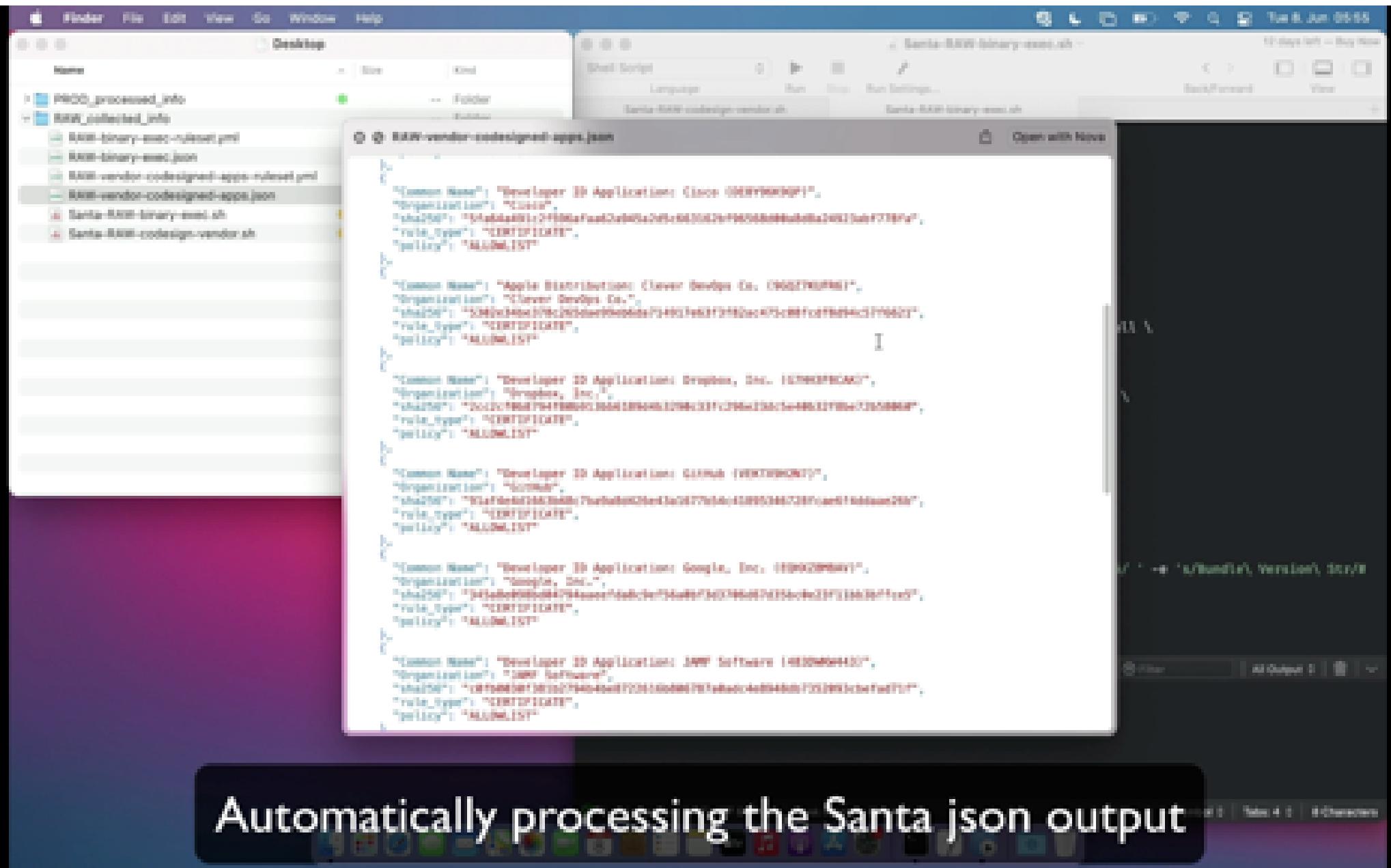
Plan of action - Demo #1

Acquiring data on a sample or canary system

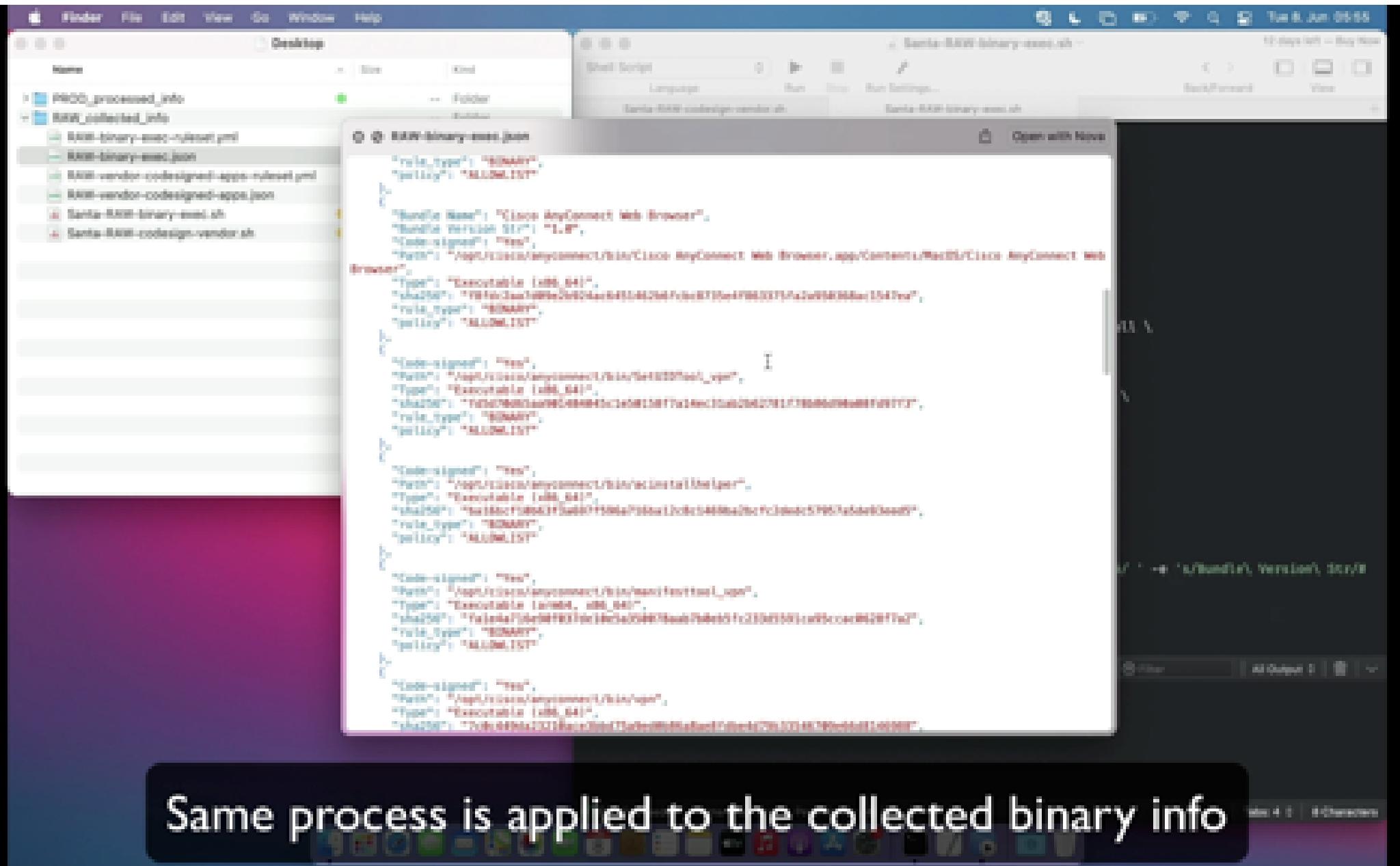
- Get "raw" information with `santactl`
- Process JSON output into set of rules
- Post-processing to preserve the data in JSON or YAML
- Use `jq` / `yq` tools for processing



Use `santactl` to gather codesigned information



Automatically processing the Santa json output

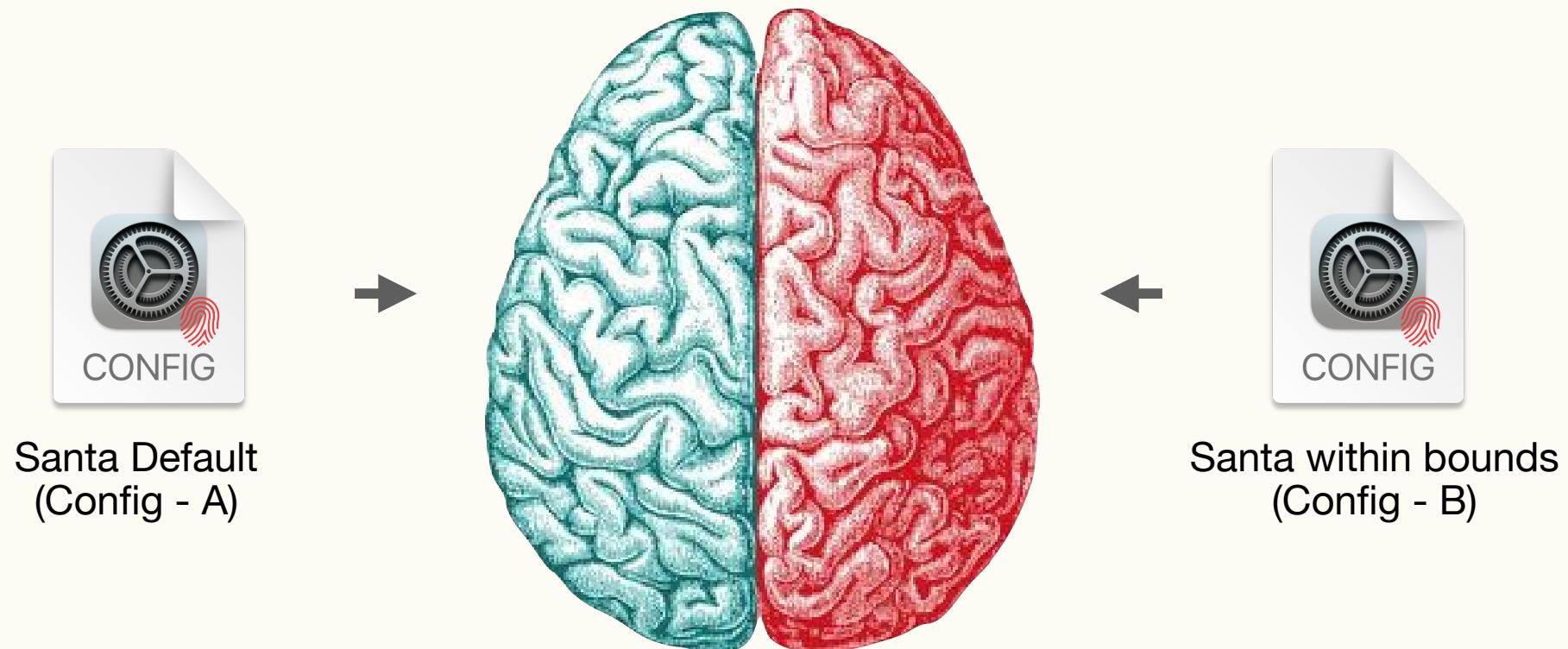


80/20

Lockdown vs. Monitoring

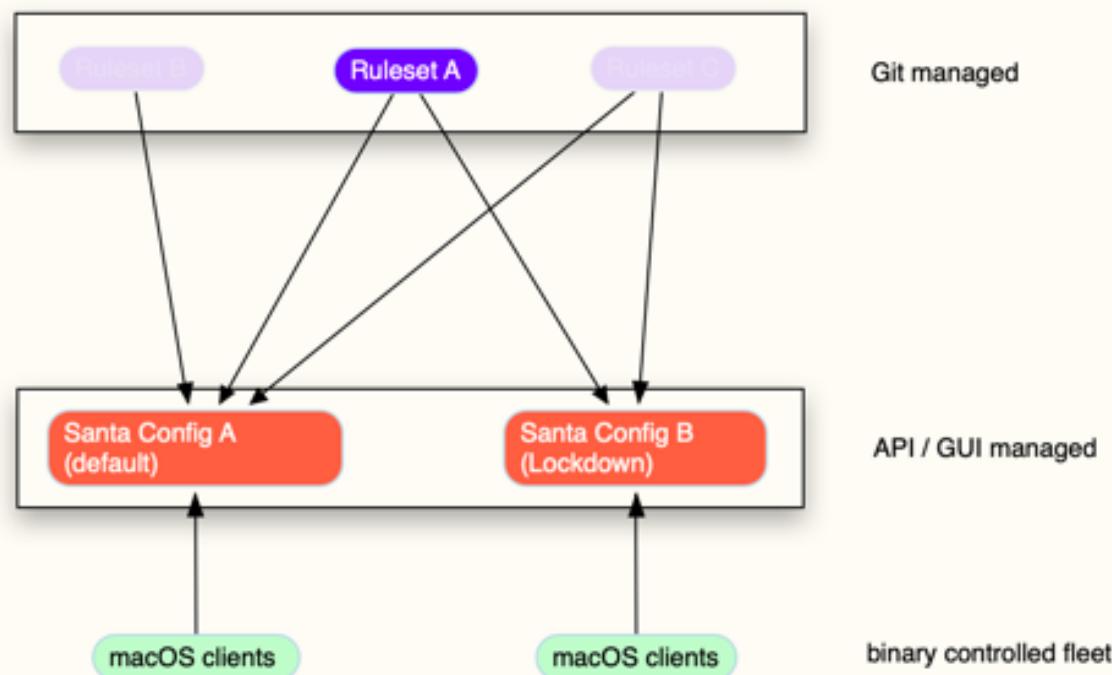
Split Brain

Lockdown vs. Monitoring



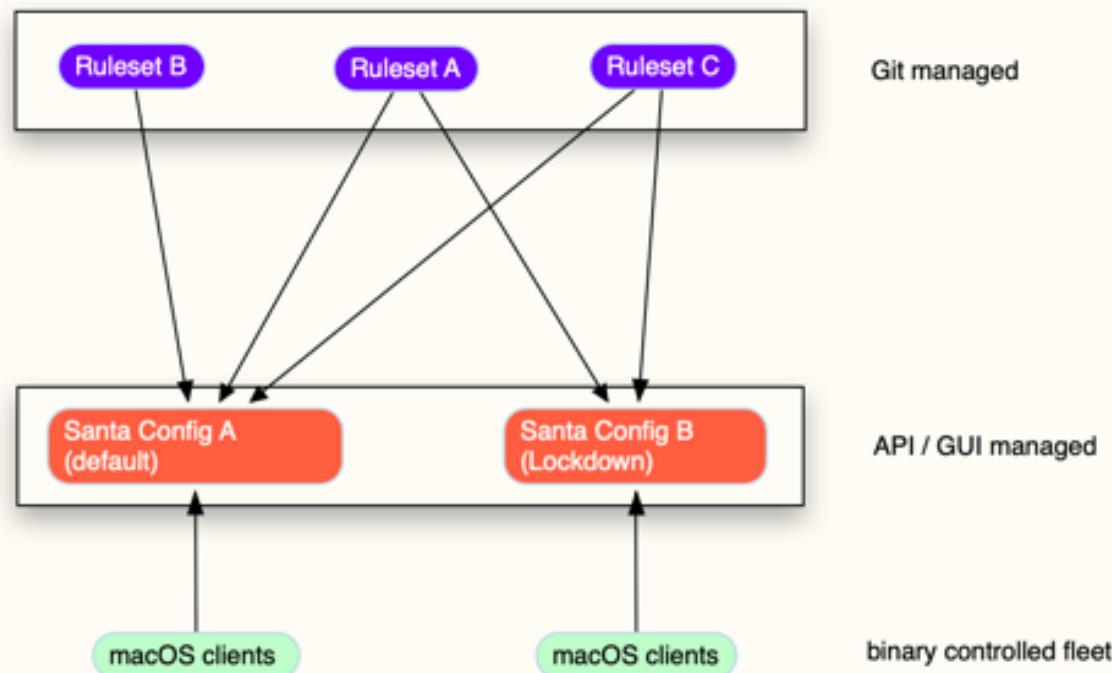
Building Rulesets

Git based workflows



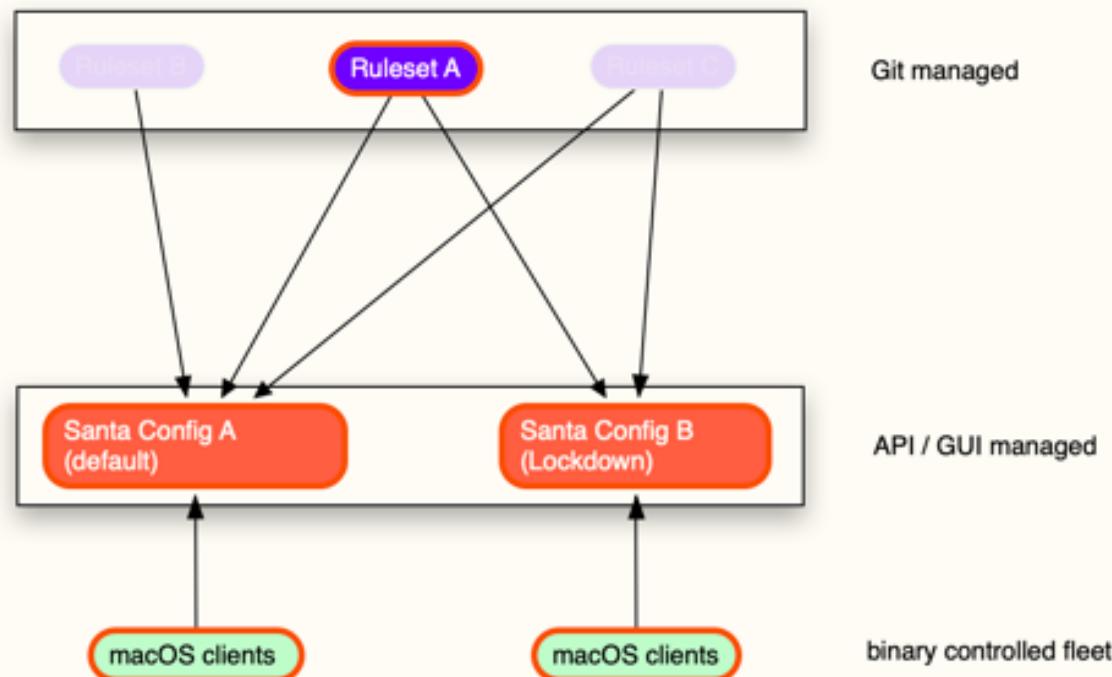
Building Rulesets

Git based workflows



Containment mode

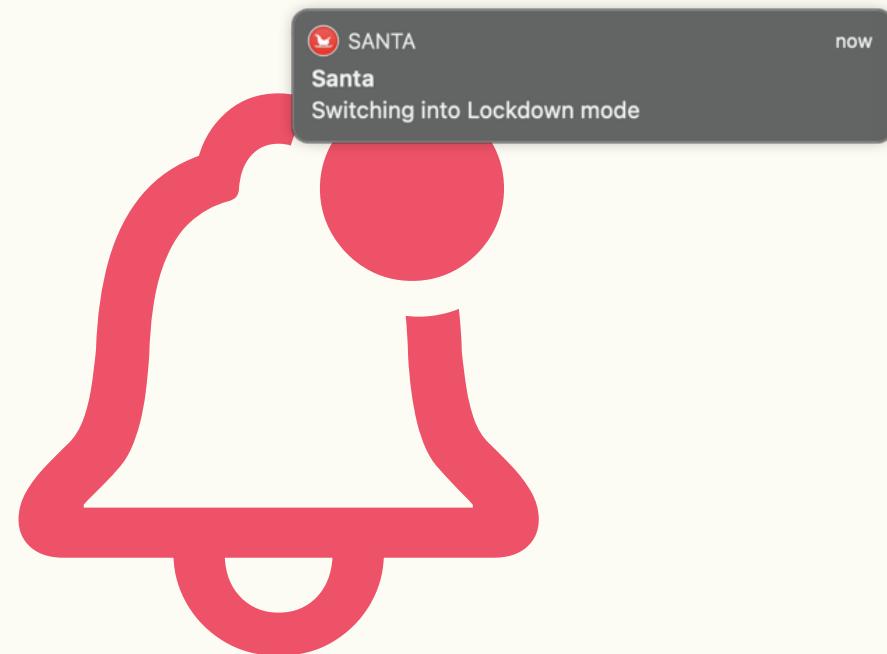
Allow only the most important tools



Panic switch

Be organized on your playbook (when the shit hits the fan)

- Allow only the minimum
- Run in Lockdown mode
- Control events in data store / SIEM
- Revert on a granular basis



Plan of action - Demo #2

Run git based workflow

- GitHub Actions
- Zentral HTTP API
- Santa Sync server is a Zentral instance running in the cloud

The screenshot shows the Zentral web interface. The top navigation bar includes links for Home, Help, View, History, Analytics, Devices, Metrics, and Help. The main header shows "Samba configuration" and "Default". The left sidebar has sections for Home, Devices, Policies, and Metrics, with "Metrics" currently selected. The main content area displays the "Samba configuration Default" page, which lists various configuration parameters with their values. A note at the bottom indicates that the configuration file is being updated. Below this, there's a section for "1 Enrollment" with a "Create" button. At the bottom, there's a table for "0 Rules" and a "Metrics" link.

Samba configuration Default

Variable	Value
Name	(Default)
Mode	Enabled
Unknown user message	The following application has been blocked from executing because its hydroshare name could not be determined.
Blocked user message	The following application has been blocked from executing because it has been declared malicious.
Malicious user message	Executing via Worker mode
Malicious notification message	Executing via Lockdown mode
Client certificate path	/etc
Root user	/etc
Full sync interval	600s
Disable location	/etc
Disable execution rules	/etc

Execution via
Unknown user
Unknown, 1 user denied execution

1 Enrollment:

Business unit	Type	Created at	Request count	Version	Timestamp
Default	-	June 6, 2021, 10:00 pm	0	0.0	-

0 Rules

Santa configuration Default

Variable	Value
Name	(Default)
Mode	Enabled
Unknown binary message	The following application has been blocked from executing due to binary file hash detection.
Blocked binary message	The following application has been blocked from executing due to file has been detected malicious.
Block notification interval	Checking for blocked code
Mode notification interval	Checking for lockdown mode
Client certificate path	/etc
Root user	/root
Full sync interval	00000000
Disable location	none
Disable location rules	none

Execution of suspicious application detected.
File /usr/bin/malicious_code

Delete

1 Enrollment:

Status

Business unit	Type	Created at	Request count	Version	Timestamp
Default	-	June 6, 2017, 10:00 pm	1	1.0	-

View logs Configuration profile

0 Rules

Create new



Up-to-date Santa sync server

(It's yaml and json all the way down)

Zentral open source:
<https://github.com/zentralopensource/zentral>

A screenshot of a web browser displaying the Zentral application. The URL in the address bar is "m10yvr.zentral.io". The page title is "zentral". The main content area shows the "Santa configurations / Default" section. The table lists various configuration attributes and their values. A note at the bottom right indicates that the application has been blocked from executing certain commands due to uncertainty or malicious intent.

Attribute	Value
Name	Default
Mode	Monitor
Unknown block message	The following application has been blocked from executing<code>/bin/</code> because its trustworthiness cannot be determined.
Banned block message	The following application has been blocked from executing<code>/bin/</code> because it has been deemed malicious.
Mode notification monitor	Switching into Monitor mode
Mode notification lockdown	Switching into Lockdown mode
Client certificate auth	no
Batch size	50
Full sync interval	600s
Enable bundles	yes
Enable transitive rules	yes

The Zentral project

Typically runs in a cloud-based deployment

- Complete Santa and Osquery configuration and event management
- Connecting multiple inventories (Jamf, PuppetDB, et-al.)
- Comprehensive event sources (Munki, Jamf Protect, et-al.)
- Manage dynamic Munki manifests (effectively replaces Simian)
- Scalable operation in a full cloud-native setup (GCP, AWS, Azure)*
- SSO and Role Base Access Control (RBAC)
- Multiple primary event data stores



*Support plan for cloud provider deployment (w/Terraform) or use of the free appliance in smaller setups.

Summary

Effective binary control for macOS

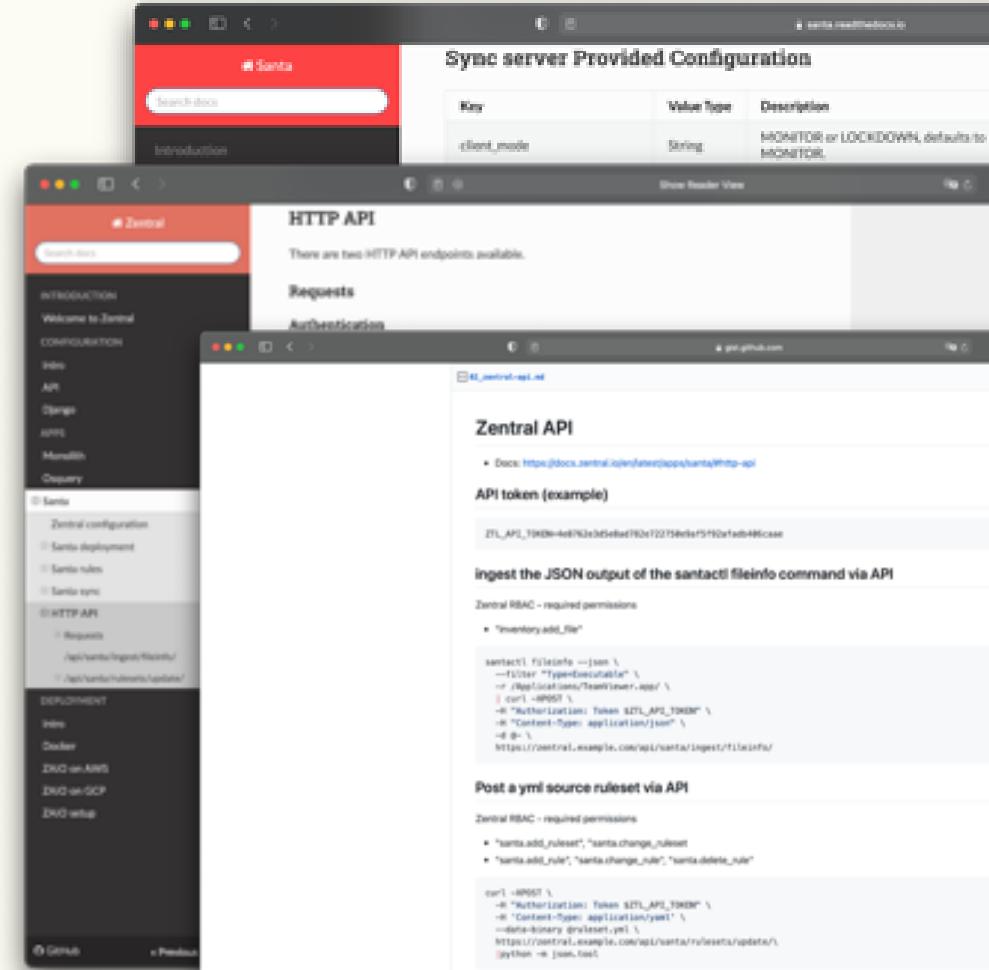
- Know what to approve for whom
- Update rules and policies in a effective time frame
- Consider more than one possible configuration
- Keep control with Git based workflows
- Embrace lockdown mode for a substantial share of the fleet



Learn more resources

Manage an effective binary control for macOS

- Santa Documentation
<https://santa.readthedocs.io>
- Zentral Documentation
<https://docs.zentral.io>
- Santa project
<https://github.com/google/santa>
- Zentral open source project
<https://github.com/zentralopensource/zentral>
- Moroz open source project
<https://github.com/groob/moroz>



Thank you



Say hello / contact us

Twitter: @head_min
Slack: @headmin

Zentral Pro Services
<https://zentral.pro>