Getting Started with Santa

Todd Houle - MIT

toddhoule@protonmail.com

thoule on macadmins slack

Feb 2020 uMac

bash$ whoami

- Todd Houle
- Macintosh admin for 25 years
- Higher education & research
- Responsible for Software Packaging, QA Testing, Distribution, Backup, and macOS services

What to Expect

- Introduction to Google Santa
- Extensive Command Line Usage
  - Basic Terminal familiarity is enough
- Lots of terminal text on screen

What is it?

- Whitelist / Blacklist Tool
- Makes decision to allow or deny launch
- Managed by Command Line, or Sync Server
- Created by Google
- Released Open Source in 2014
- Responsive community support
  macadmins slack #santa

What is it not?

No single system or process will stop all attacks, or provide 100 percent security. Santa is written with the intention of helping protect users from themselves. People often download malware and trust it, giving the malware credentials, or allowing unknown software to exfiltrate more data about your system.

As a centrally managed component, Santa can help stop the spread of malware among a larger fleet of machines. Independently, Santa can aid in analyzing what is running on your computer.

Santa is part of a defense-in-depth strategy, and you should continue to protect hosts in whatever other ways you see fit.

--Ed Marczak

Downloading

Download Prebuilt Release: https://github.com/google/santa

Documentation: https://santa.readthedocs.io/en/latest/

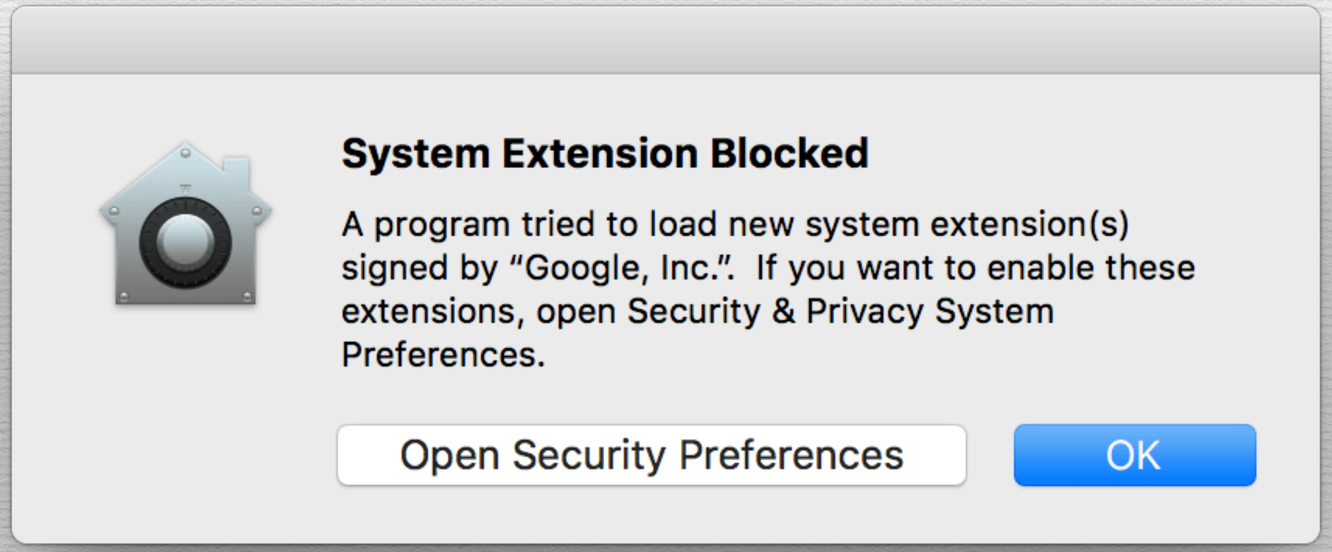
Building Yourself: Signed Kernel Extension required. Must have signing cert with entitlement for kernel extensions.

Components

- Kernel Extension: monitor application execution
- Userland daemon: make execution decisions based on rules
- GUI Application: notifies user in case of block
- CLI Utility: santactl: To configure standalone rules and more
- Config Profile: Required to configure additional settings

Components

- Kernel Extension: monitor application execution



Monitor vs Lockdown

	Monitor	Lockdown
Whitelisted	✅	✅
Blacklisted	❌*	❌*
Unknown	✅*	❌*

* Events sent to server

Basic Commands - fileinfo

bash$ santactl fileinfo /Applications/CrashPlan.app

```
Path              : /Applications/CrashPlan.app/Contents/MacOS/CrashPlanWeb
SHA-256           : bc727cc64731cacbfe5f6cb895658efc66bf952c084a0febe193
Rule              : Whitelisted (Certificate)
Signing Chain:
    1. SHA-256        : 73957d438373217249cf3b01aede381c8337a91acdaeb72
       SHA-1          : 179590f3665fea0aea4f3eea6dee1ddff68f6159
       Common Name       : Developer ID Application: Code 42 Software
       Organization        : Code 42 Software
       Organizational Unit : 9YV9435DHD
       Valid From          : 2017/05/05 08:50:20 -0400
       Valid Until         : 2022/05/06 08:50:20 -0400
```

Basic Commands - key

- santactl fileinfo /Applications/CrashPlan.app/ --key SHA-256 **95a24abf57600e2d2a4695db28322e698d09da3a**
- santactl fileinfo /Applications/CrashPlan.app/ --cert-index 1 --key SHA-256 **73957d4383732181cc8f8637ae36bff91acdaeb72**

Basic Commands - key

- santactl fileinfo /Applications/Firefox.app --key Rule
  Whitelisted (Certificate)

- santactl fileinfo /usr/bin/hostinfo --key Path --key SHA-256 --key Rule
  Path : /usr/bin/hostinfo
  SHA-256: 77aff1c2ca5051ad01fdfac23c6f3844276c
  Rule : Whitelisted (Certificate)

Basic Commands - key

- santactl fileinfo /usr/bin -r --key Path --key SHA-256 --key Rule

  Path   : /usr/bin/cpan
  SHA-256: 77aff1c26f36f3ca50ad01fdfac6f36f323c6f3844276c
  Rule   : Whitelisted (Scope)

  Path   : /usr/bin/libtool
  SHA-256: 690cd467cfa61a35cfcd98af3dee75835a9009218df02
  Rule   : Whitelisted (Certificate)

Basic Commands - rule

- bash# santactl rule --blacklist --path /Applications/Malware.app
- bash# santactl fileinfo --cert-index 1 --key SHA-256 /Applications/Malware.app
- bash# santactl rule --blacklist --certificate --sha256 73957d43837321724 9cf3b01aede381c8337ae91acdaeb

Rule Precedence

- Rules are evaluated most specific to least
  - Binary
  - Certificate
  - Scope

Basic Commands - Download Monitor

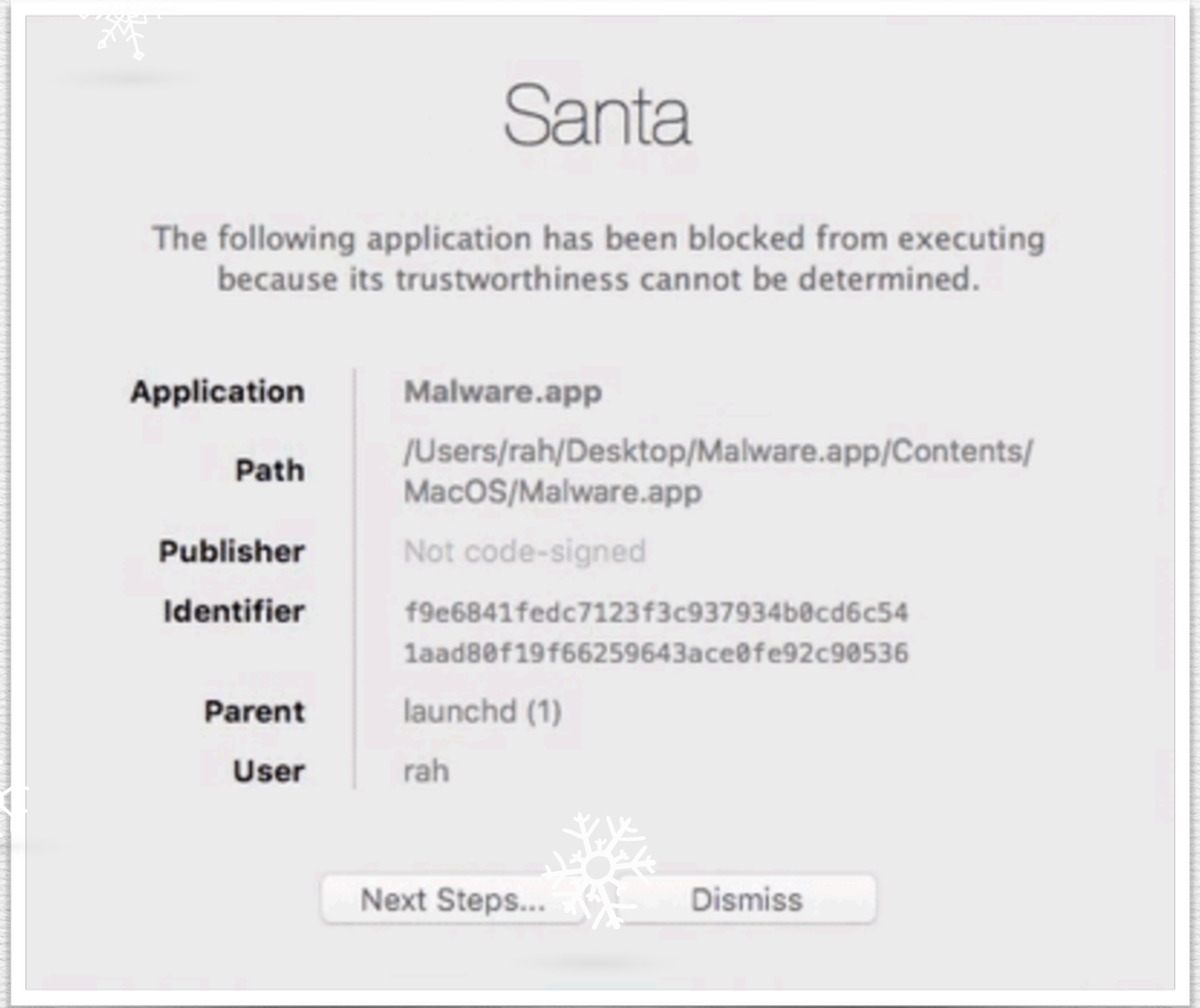
```
bash-3.2# santactl fileinfo ~/Downloads/TeamViewer.dmg --key "Download URL" --key "Download Referrer URL" --key "Download Timestamp"

Download URL          : https://dl.tvcdn.de/download/TeamViewer.dmg

Download Referrer URL: https://www.teamviewer.com/

Download Timestamp   : 2019/02/26 02:23:41 -0500
```

Basic Commands - Status

```
bash-3.2# santactl status
>>> Daemon Info
  Driver Connected          | Yes
  Mode                      | Monitor
  File Logging              | No
  Watchdog CPU Events       | 1  (Peak: 23.85%)
  Watchdog RAM Events       | 0  (Peak: 19.13MB)
 Compiler Rules             | 0
  Transitive Rules          | 0
  Events Pending Upload     | 13
```

```
>>> Kernel Info
  Root cache count          | 216
  Non-root cache count      | 0
>>> Database Info
  Binary Rules              | 0
  Certificate Rules         | 2
  Compiler Rules            | 0
  Transitive Rules          | 0
  Events Pending Upload     | 13
```

Blocked Application



Built In Protection

- To avoid blocking any Apple or Santa binaries, SantaD will create two immutable rules at startup
  - The Signing Cert SantaD is signed with
  - The Signing Cert LaunchD is signed with

Local Log

- /var/db/santa/santa.log

- Local Events
  (EXEC WRITE RENAME DELETE DISKAPPEAR DISKDISAPPEAR)

- Logs can be very large
  (20MB/day on my work desktop computer)

Local Log

[2019-07-09T18:11:42.699Z] I santad: action=EXEC|decision=ALLOW|reason=UNKNOWN|sha256=e959aec0ecb50d8f4d905d2dcdea7cf4afa36ee6a5d7deb5f7a6867b283af2cf|cert_sha256=fea2d342615081eb11d5f4b77ed5d5f272449e50690b60b3bc8d42428077823d|cert_cn=Developer ID Application: Dropbox, Inc. (G7HH3F8CAK)|pid=7155|ppid=1|uid=501|user=todd|gid=20|group=staff|mode=M|path=/Users/todd/Library/Dropbox/DropboxMacUpdate.app/Contents/MacOS/DropboxMacUpdate|args=/Users/todd/Library/Dropbox/DropboxMacUpdate.app/Contents/MacOS/DropboxMacUpdate -check periodic

Local Log

[2019-07-09T15:23:05.522Z] I santad: action=EXEC|
decision=ALLOW|reason=CERT|
sha256=1387da02511996e3f3fd78975c3d32448d3bf42a71ed35c1374ed
e212b33ff8d|
cert_sha256=2aa4b9973b7ba07add447ee4da8b5337c3ee2c3a991911e8
0e7282e8a751fc32|cert_cn=Software Signing|pid=5820|ppid=5813|
uid=501|user=todd|gid=20|group=staff|mode=M|path=/usr/bin/tail|
args=tail -F /var/log/system.log

Local Log

santa.log:[2019-07-08T21:27:58.112Z] I santad: action=DISKAPPEAR|mount=|volume=test6|bsdname=disk2s2|fs=hfs|model=Apple Disk Image|serial=|bus=Virtual Interface|dmgpath=/Users/todd/Documents/Testing6.dmg|appearance=2019-07-08T21:27:58.055Z

Local Log

/var/db/santa/santa.log:[2019-07-08T21:42:39.488Z] I santad: action=DISKDISAPPEAR|mount=|volume=EFI|bsdname=disk2s2

Filesystem Events

Write/Rename/Delete and other events written to local log file.

Great for forensic tracing of Events

Configuration Profile

- Controls many additional settings
  - Regex pattern for whitelist/blacklist (/Volumes)!
- Profiles installed via
  - MDM
  - profiles -i /path/to/config.mobileconfig
  - Double-click the mobile config

Configuration Profile

ClientMode	Integer	1=Monitor 2=Lockdown
WhitelistRegex	String	Regex to whitelist if binary or cert scope doesn't allow execution.
MoreInfoURL	String	URL to open when user clicks "More Info"
EventDetailText	String	Text to show on the button
SyncBaseURL	String	URL of Sync Server

And Many More…

Local or Server

- Servers:
  - Moroz: Simple Go Server written by Victor Vrantchan
  - Upvote: Google AppEngine, integration with VirusTotal
  - Zentral: Centralized service management

Server Events

- Server Events - Blocked or Unknown Events
- Repeat launches (within 5 mins?) not sent
- Whitelisted app launches are not sent to server

Moroz

- Simple Go server
- Very easy to setup and use
- Has Events directory with json file for different events

More on Moroz

https://github.com/groob/moroz

```
/opt/Moroz/moroz
  -event-dir /opt/Moroz/santa_events
  -configs   /opt/Moroz/config/
  -tls-cert  /opt/Moroz/server.crt
  -tls-key   /opt/Moroz/server.key
```

More on Moroz

- Config dir contains
  - Global.toml
  - MachineUUID.toml

- MachineUUID.toml entries will take precedence over anything in global.toml file.

More on Moroz global.toml

```
client_mode = "MONITOR"
# blacklist_regex = “^(?:/tmp)/.*"
# whitelist_regex = "^(?:/Users)/.*"
batch_size = 100
enable_bundles = false
enabled_transitive_whitelisting = true


[[rules]]
rule_type = "CERTIFICATE"
policy = "WHITELIST"
sha256="1007a6677b965d696afad3c40a301ed5f69758bd3317ee3092279740c8878ce4"
custom_msg = “Firefox Allowed!”
```

Moroz - Events

santa_events/<<binarySHA>>/<<MacUUID>>/
<<TimeStamp.json>>

Decision, executing user, filename, path, SHA256, logged in users, parent_name, PID, PPID, and more.

Zentral

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

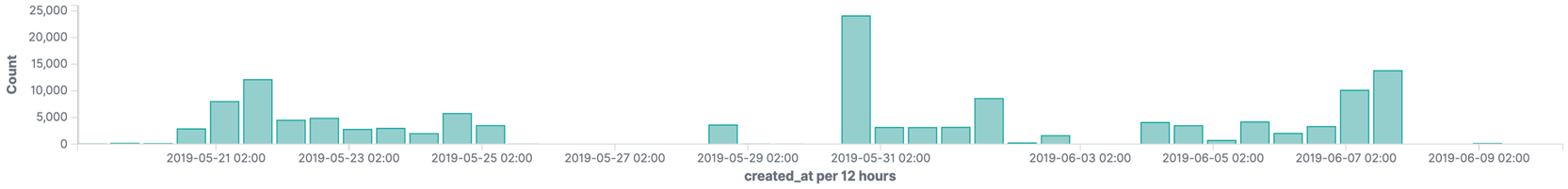
Zentral is a centralized service to manage configurations for osquery's powerful endpoint inventory and security features. Zentral also support Google Santa in a similar way. A build in event tracking, notification and time series event processing will complement these open source technologies.

Zentral

Discover - Kibana

https://zentral.example.org/kibana/app/kibana#/discover?_a=(columns:!(santa_log.action,santa_log.decision,santa_log.args),filters:!(('$state':(store:appState),meta:(alias:!n,disabled:!f,index:'33b...

Discover



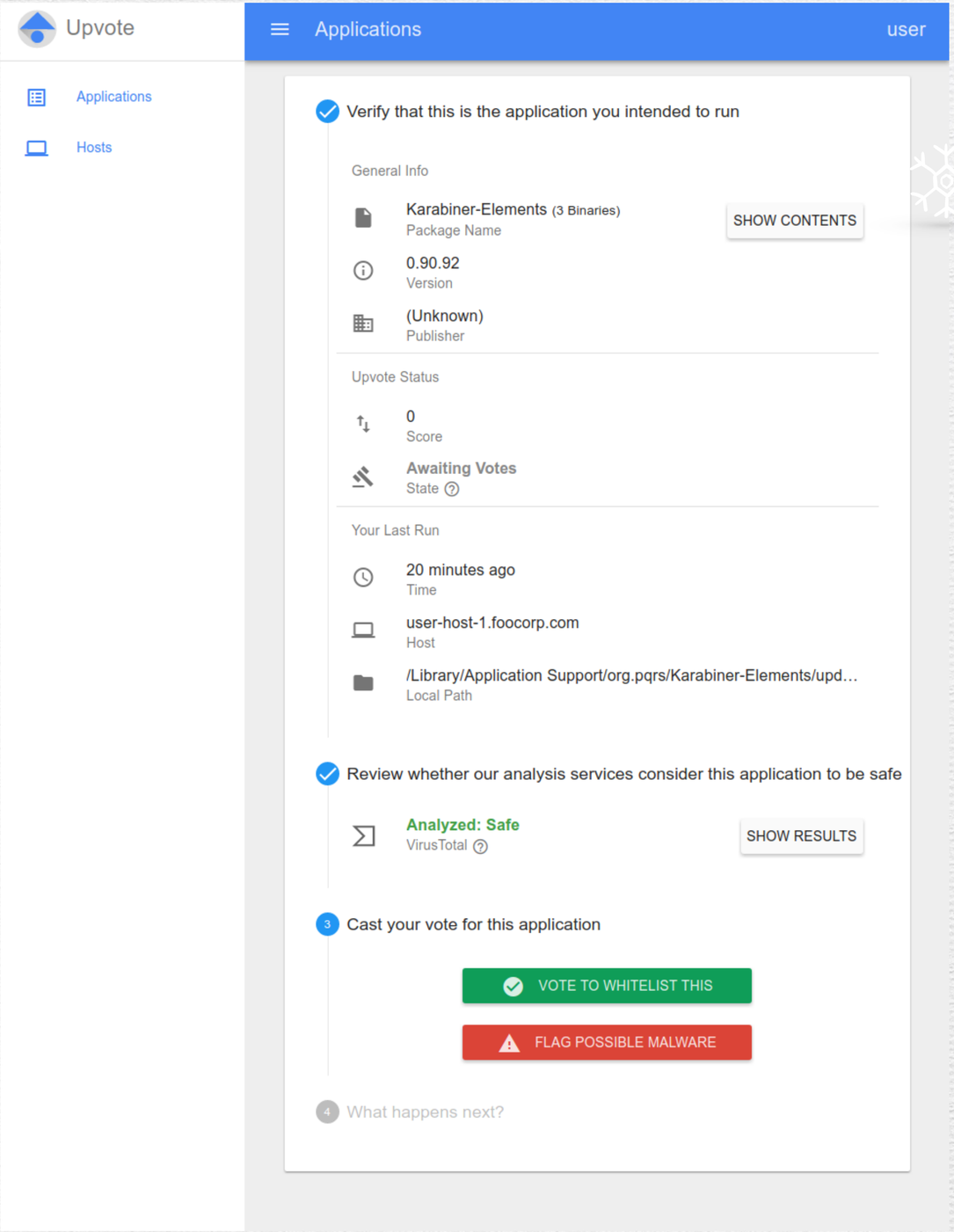
Time	santa_log.action	santa_log.decision	santa_log.args
Jun 9, 2019 @ 09:14:05.691	EXEC	ALLOW	kextcache, -arch, x86_64, -local-root, -all-loaded, -kernel, /System/Library/Kernels/kernel, -prelinked-kernel, /System/Library/PrelinkedKernels/prelinkedkernel, -volume-root, /, /System/Library/Extensions, /Library/Extensions, /AppleInternal/Library/Extensions, /Library/Apple/System/Library/Extensions
Jun 9, 2019 @ 09:14:05.684	EXEC	ALLOW	/usr/sbin/kextcache, -F, -u, /
Jun 9, 2019 @ 09:14:05.681	EXEC	ALLOW	/usr/sbin/kextcache, -F, -u, /
Jun 9, 2019 @ 09:14:05.664	EXEC	ALLOW	/usr/bin/wall, -n
Jun 9, 2019 @ 09:14:05.653	EXEC	ALLOW	sh, -c, /usr/bin/wall, -n
Jun 9, 2019 @ 09:14:05.639	EXEC	ALLOW	sh, -c, /usr/bin/wall, -n
Jun 9, 2019 @ 09:14:05.597	EXEC	ALLOW	/System/Library/CoreServices/sessionlogoutd
Jun 9, 2019 @ 09:13:39.594	EXEC	ALLOW	/bin/launchctl, list, com.facebook.osqueryd
Jun 9, 2019 @ 09:13:06.355	EXEC	ALLOW	/System/Library/PrivateFrameworks/AmbientDisplay.framework/Versions/A/XPCServices/com.apple.AmbientDisplayAgent.xpc/Contents/MacOS/com.apple.AmbientDisplayAgent
Jun 9, 2019 @ 09:13:01.923	EXEC	ALLOW	/usr/libexec/nsurlstoraged, --privileged
Jun 9, 2019 @ 09:12:58.992	EXEC	ALLOW	/System/Library/Frameworks/VideoToolbox.framework/Versions/A/XPCServices/VTDecoderXPCService.xpc/Contents/MacOS/VTDecoderXPCService
Jun 9, 2019 @ 09:12:58.523	EXEC	ALLOW	/usr/sbin/systemsoundserverd
Jun 9, 2019 @ 09:12:58.491	EXEC	ALLOW	/System/Library/Frameworks/LocalAuthentication.framework/Support/coreauthd
Jun 9, 2019 @ 09:12:58.401	EXEC	ALLOW	/System/Library/PrivateFrameworks/SystemAdministration.framework/Resources/activateSettings

Upvote

https://github.com/google/upvote

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.

--Blatantly stolen from Github Description



VirusTotal is a binary reputation aggregator that can be used to inform trust decisions. The API provides analysis results from many anti-virus and application scanners and is free to use up to a certain usage limit (4 req/min).

Thank You!

?