Google

Santa's Got A Brand New Bag

Matt White, Pete Markowsky / 2023-10-12

Agenda

- What is Santa?
- Deployment at Google
- Making a Modern Santa
- What's New?
- Better Detection & Response
- Getting Involved

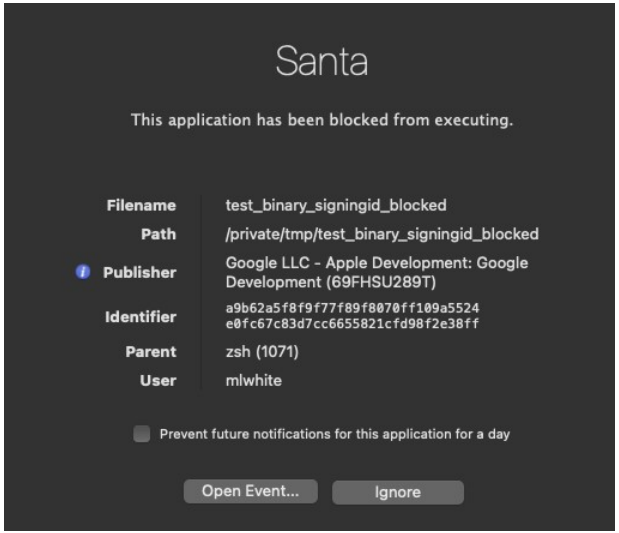
What Is Santa?

What is Santa?

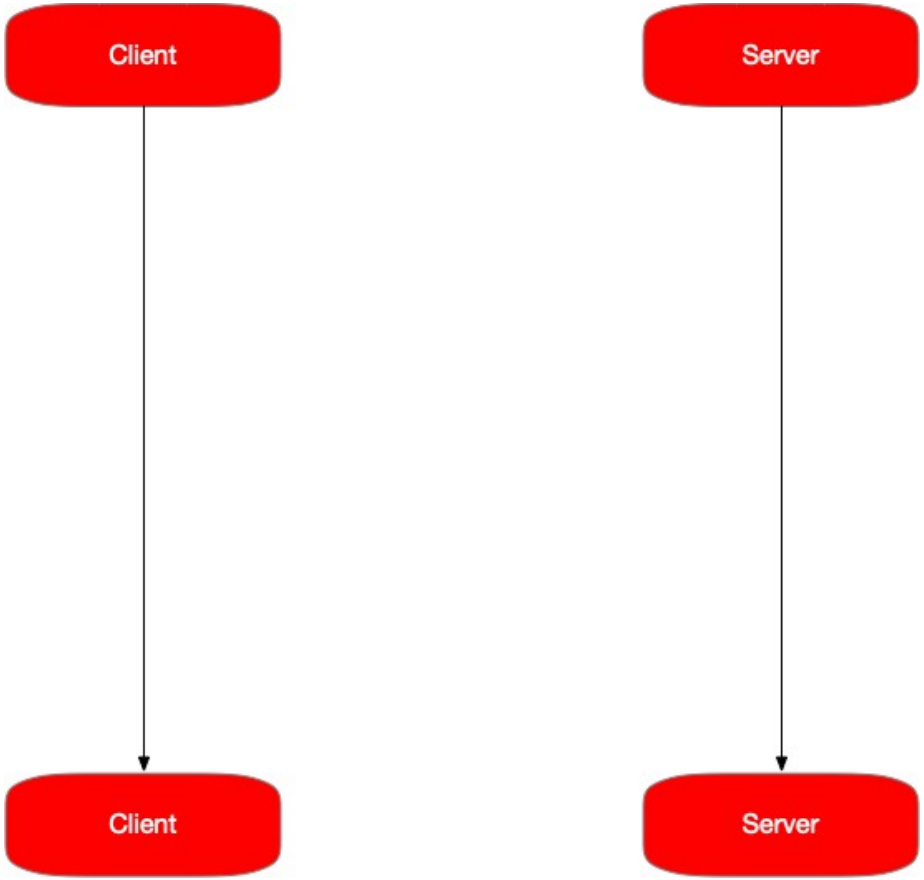
- Policy enforcement
  - Binary and file access authorization
  - USB mass storage protections
- Endpoint telemetry
  - Processes, File operations, Disk events
- Sync protocol

Binary Authorization

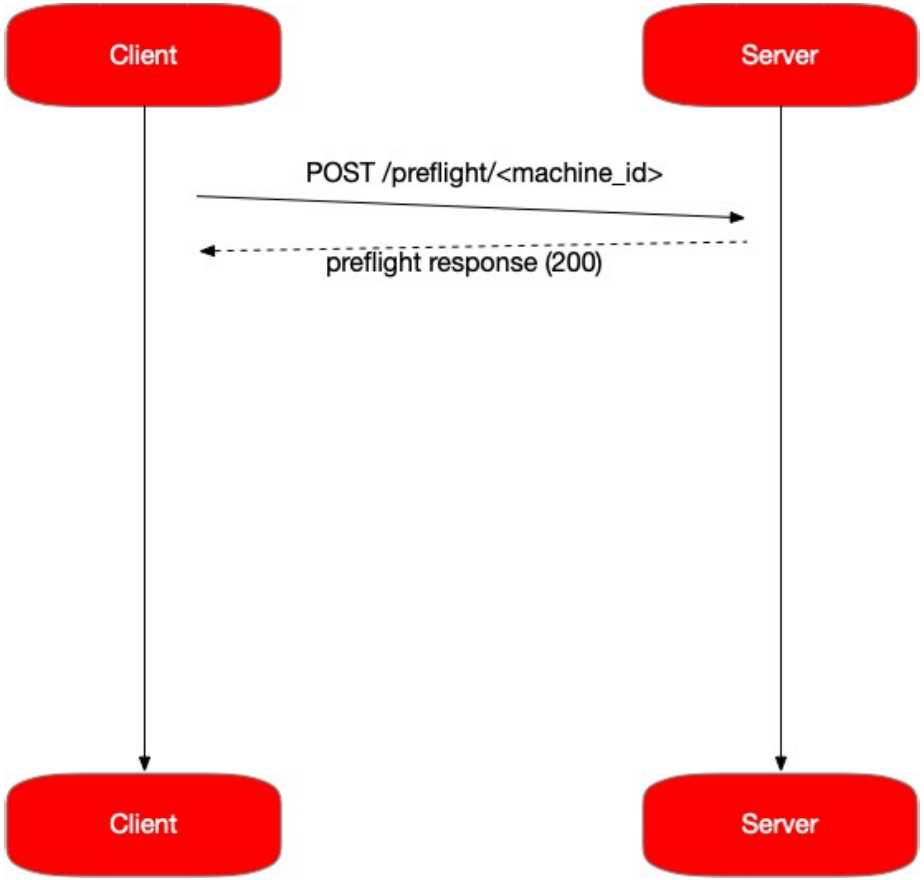
- All executions are evaluated against policy
- Supported rule types:
  - Binary Hash, Certificate Hash, Signing ID, Team ID
- Transitive allowlisting
- Lockdown Mode vs. Monitor Mode



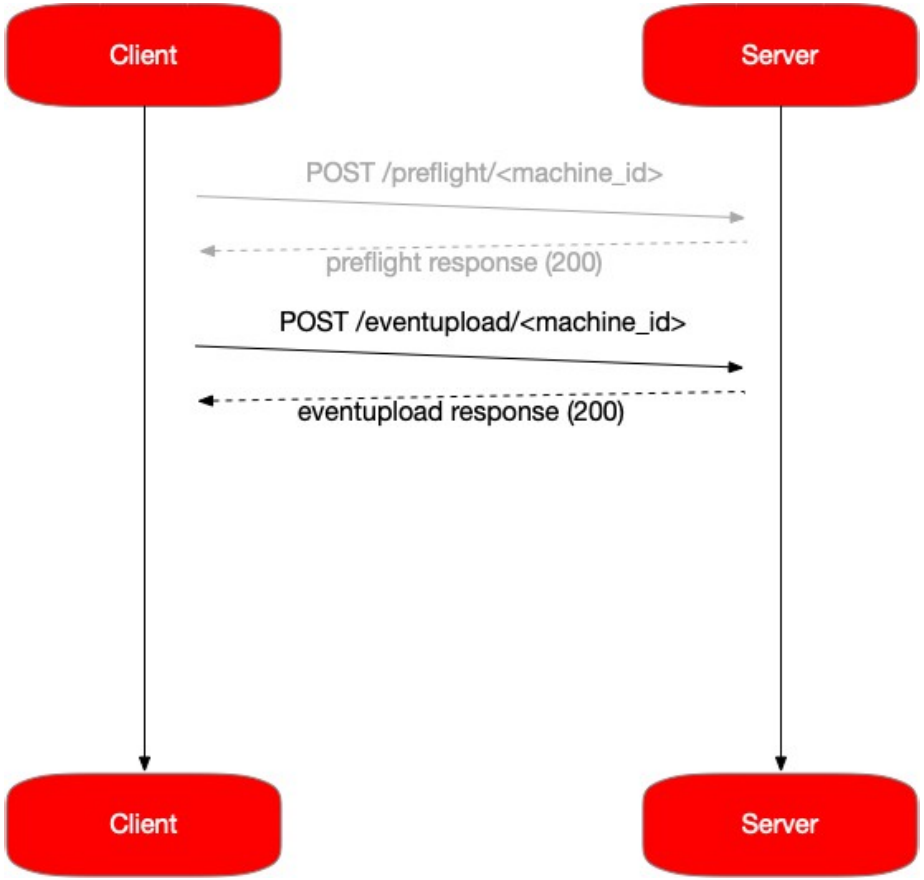
Synchronization



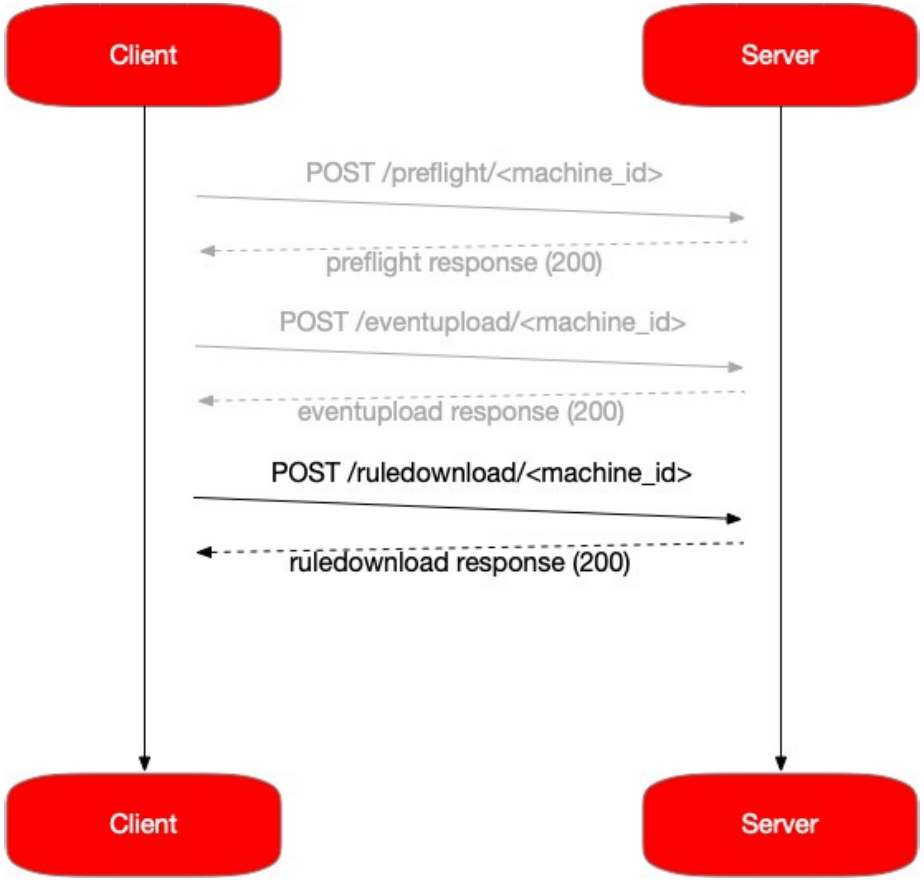
Synchronization



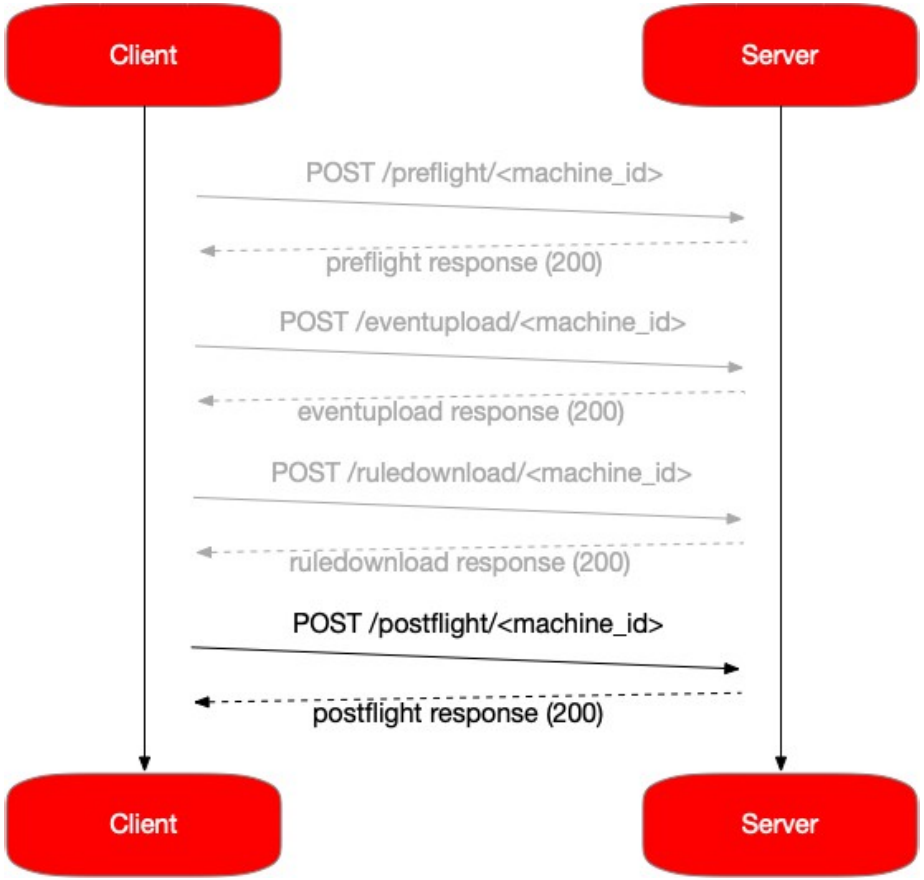
Synchronization



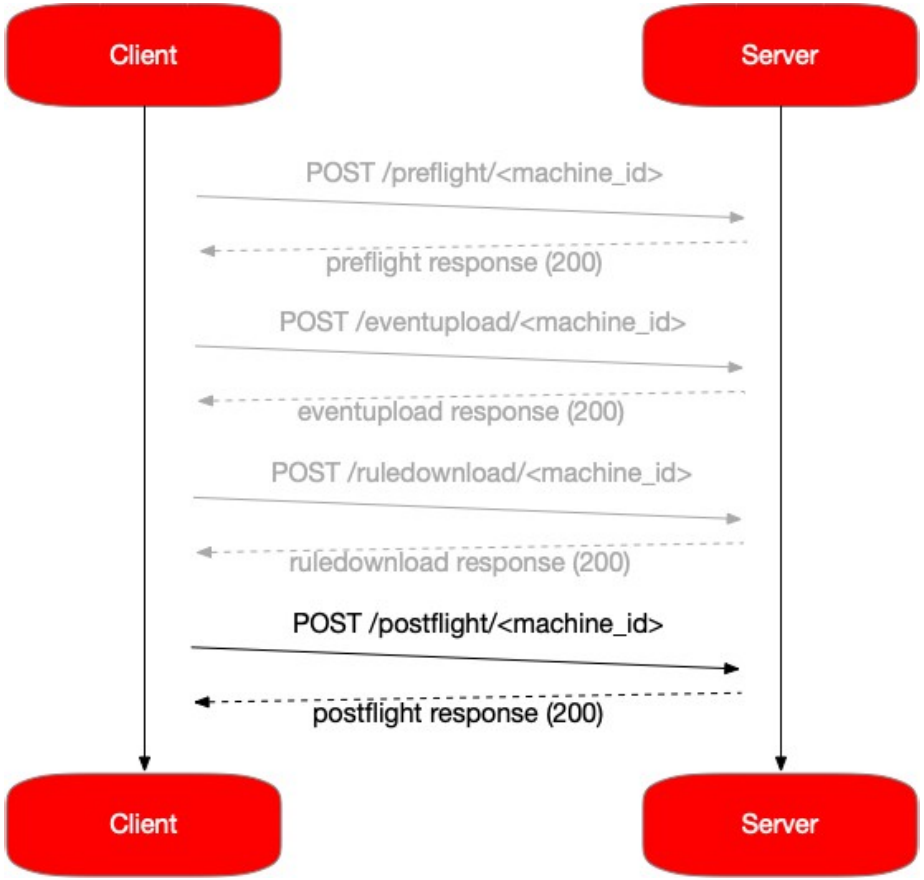
Synchronization



Synchronization

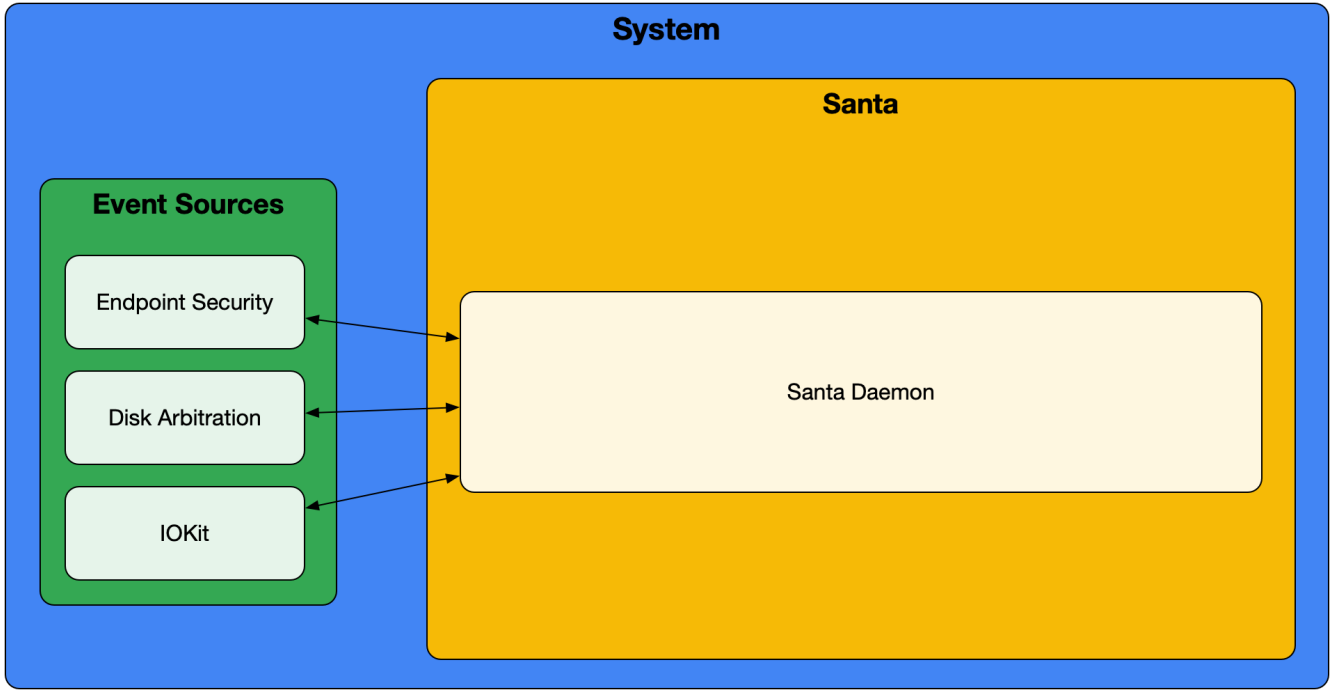


Synchronization

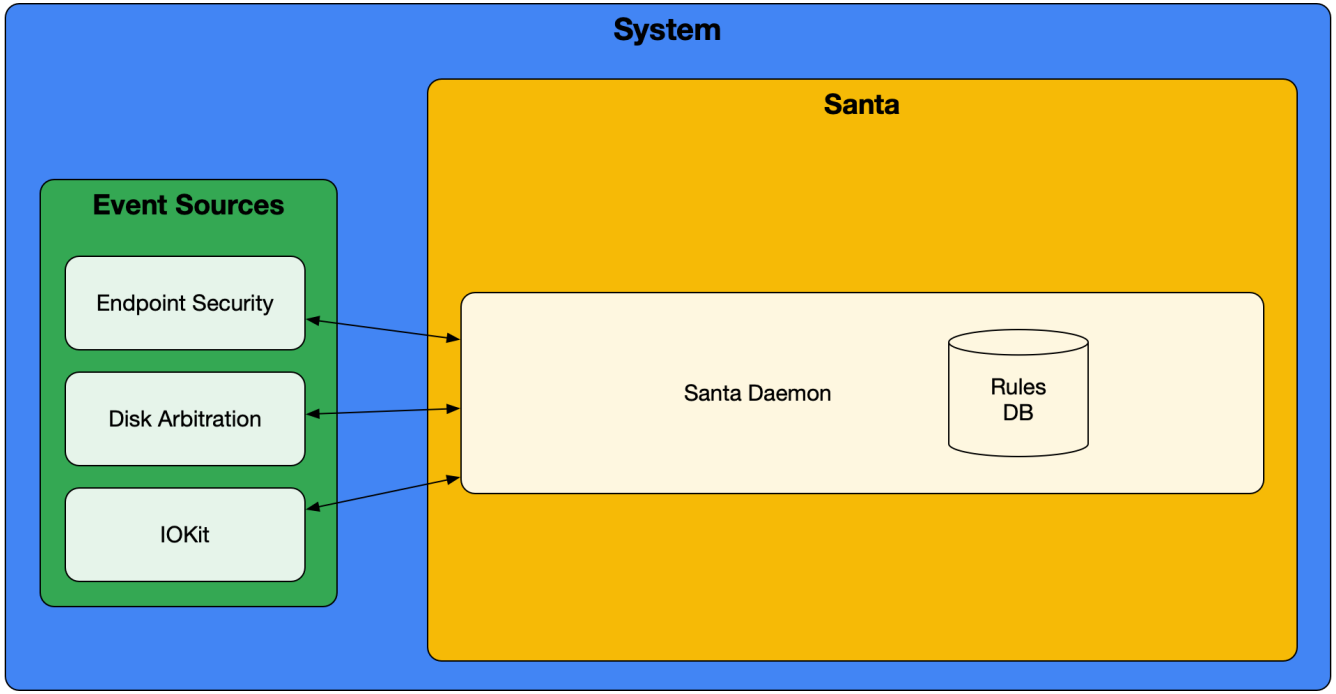


Santa Architecture

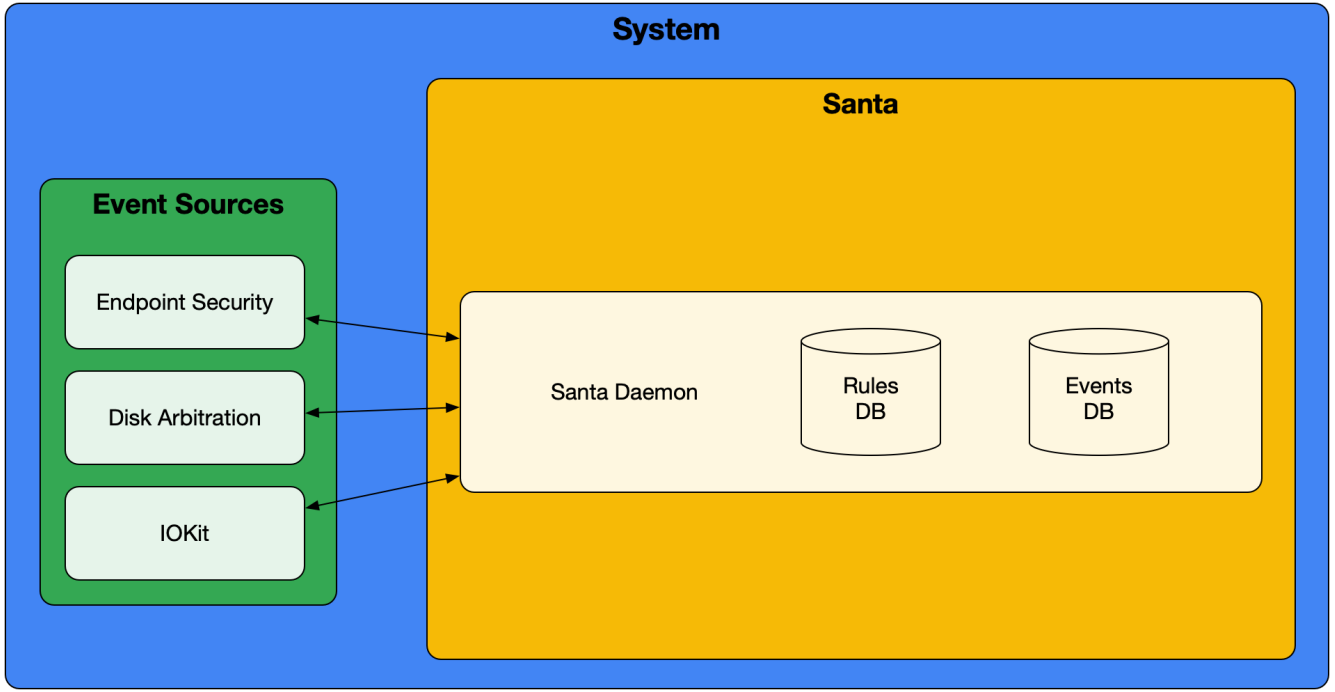
Santa Architecture



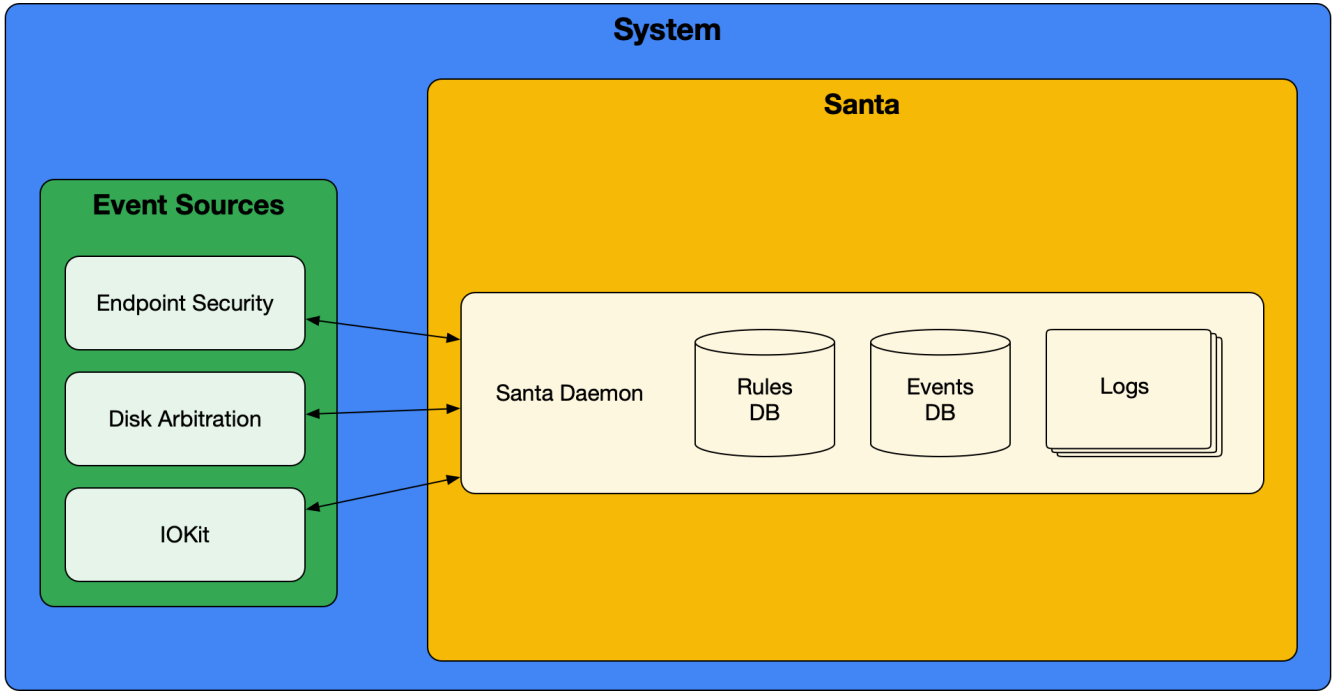
Santa Architecture



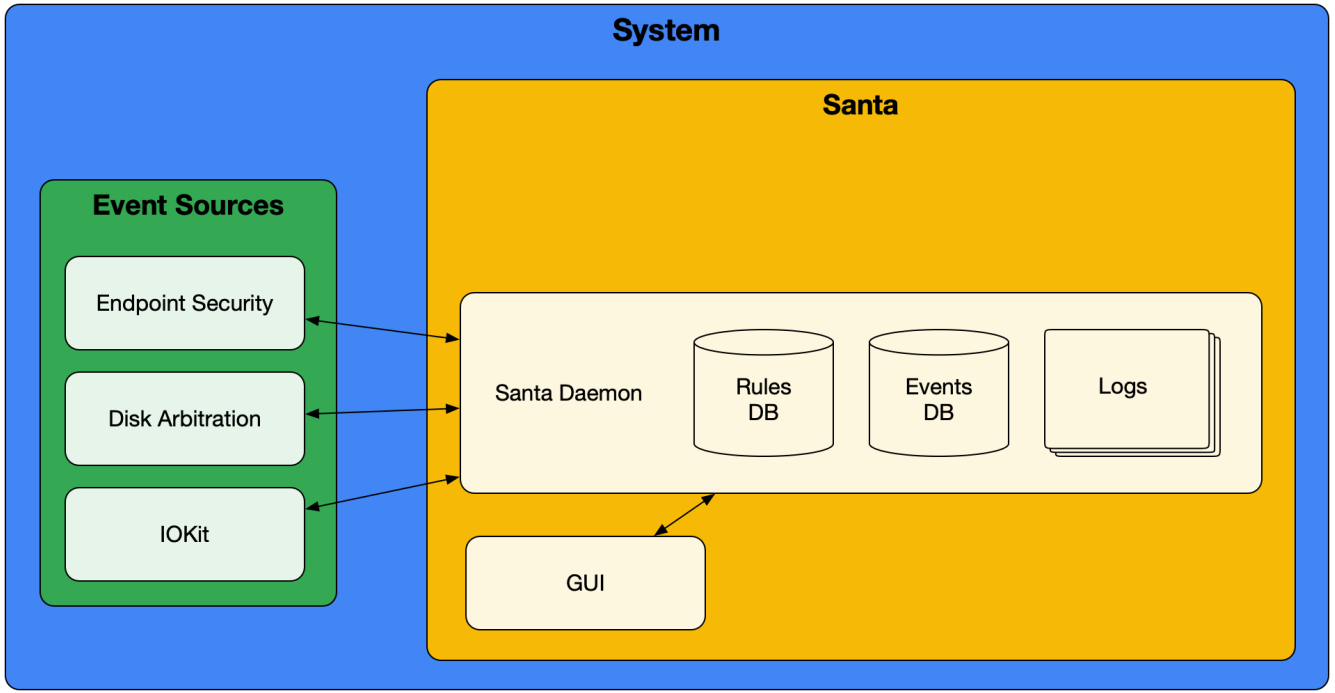
Santa Architecture



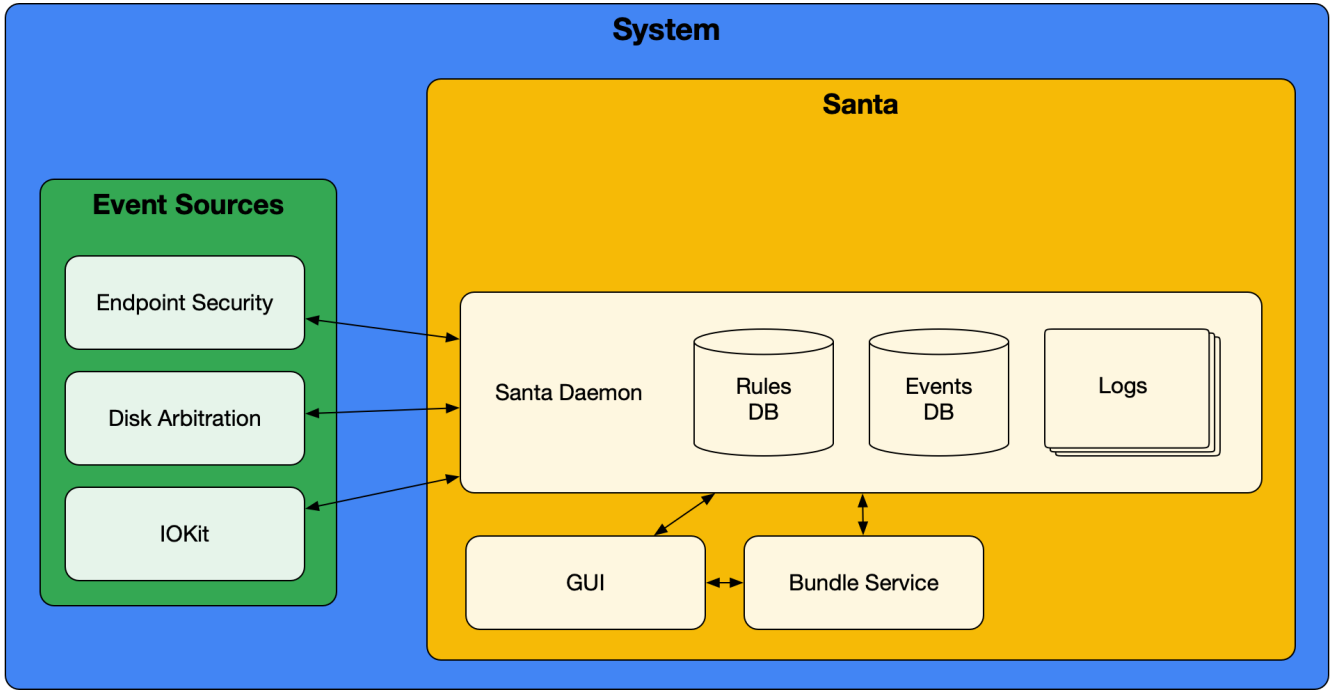
Santa Architecture



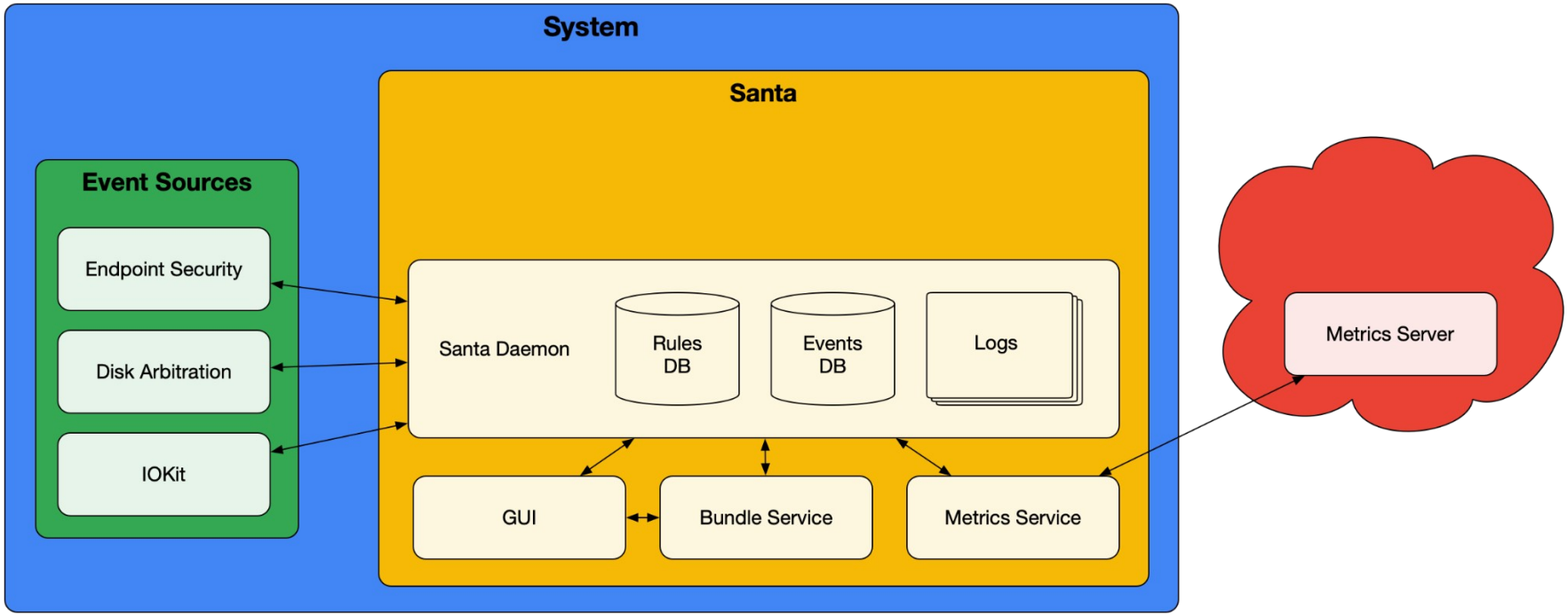
Santa Architecture



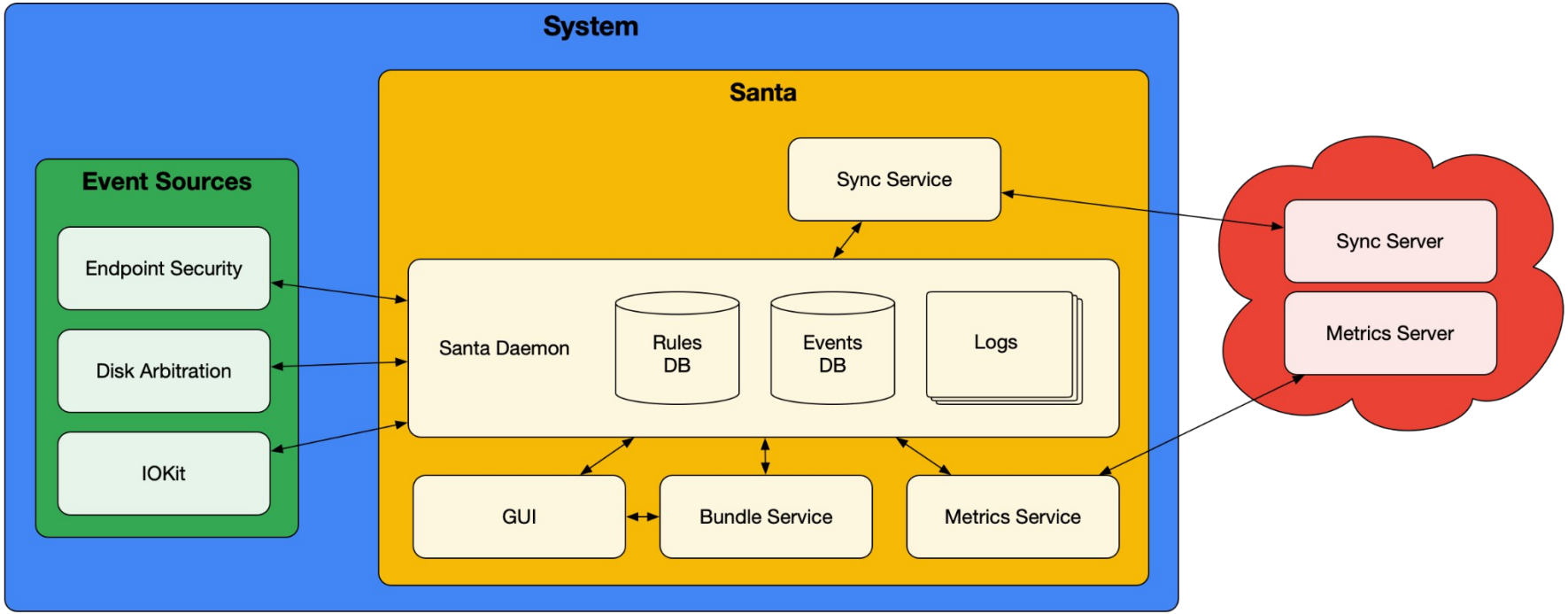
Santa Architecture



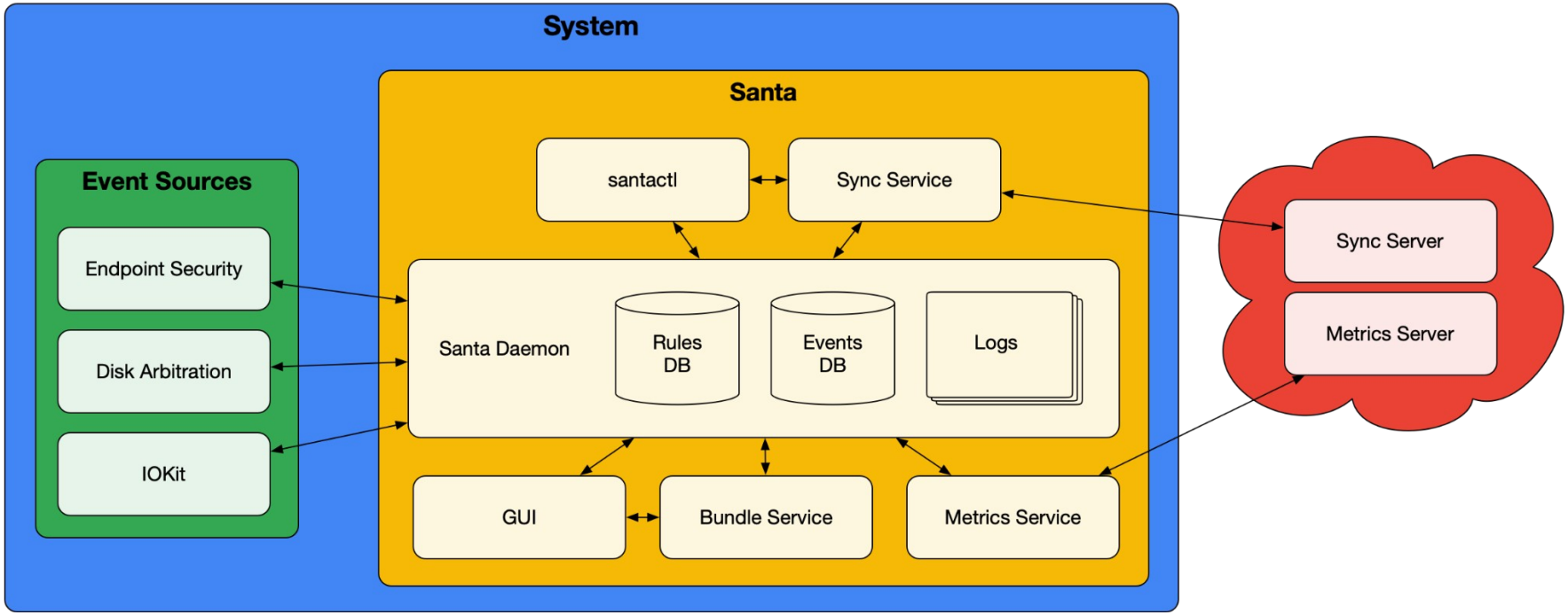
Santa Architecture



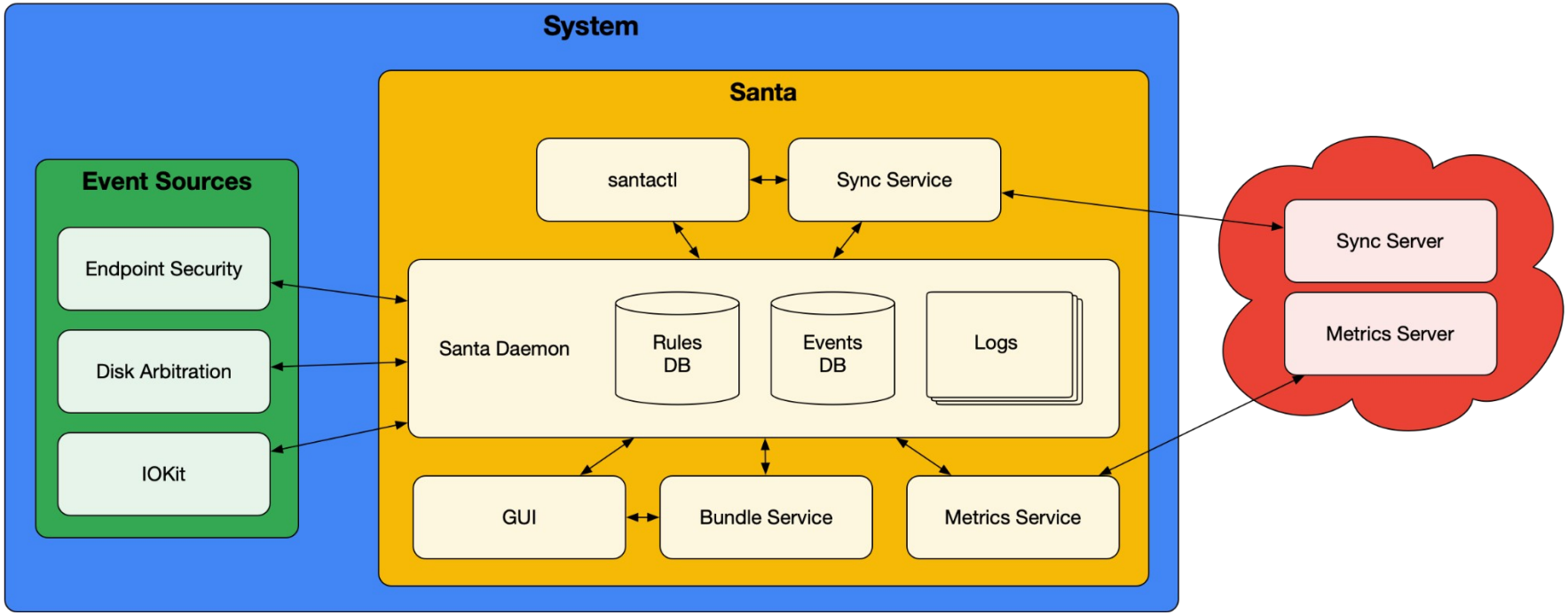
Santa Architecture



Santa Architecture



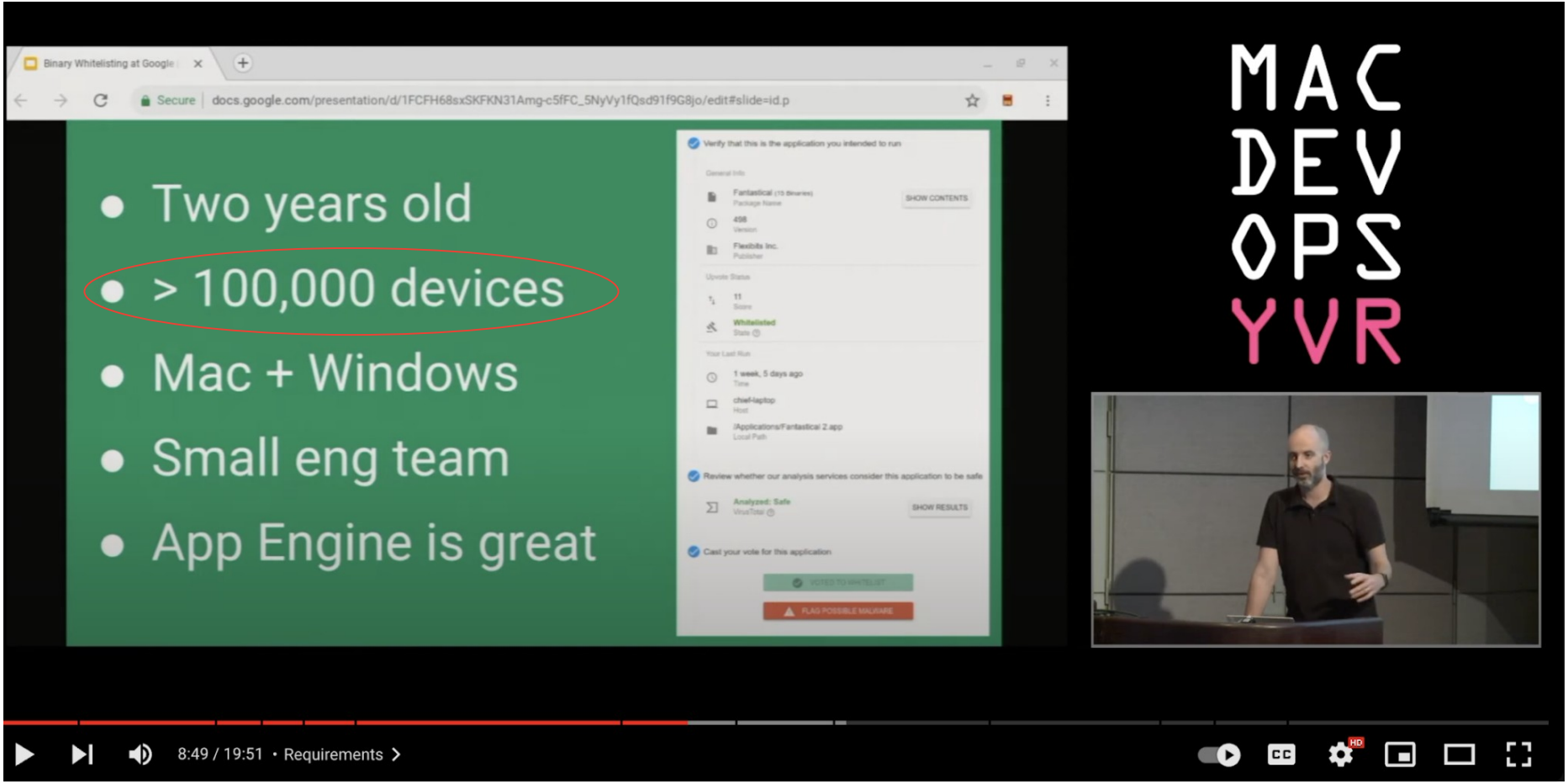
Santa Architecture



Deployment at Google

Deployment @Google

- Development done entirely in open source
- Build in house
- Binaries deployed via custom package manager
- Configuration managed via MDM

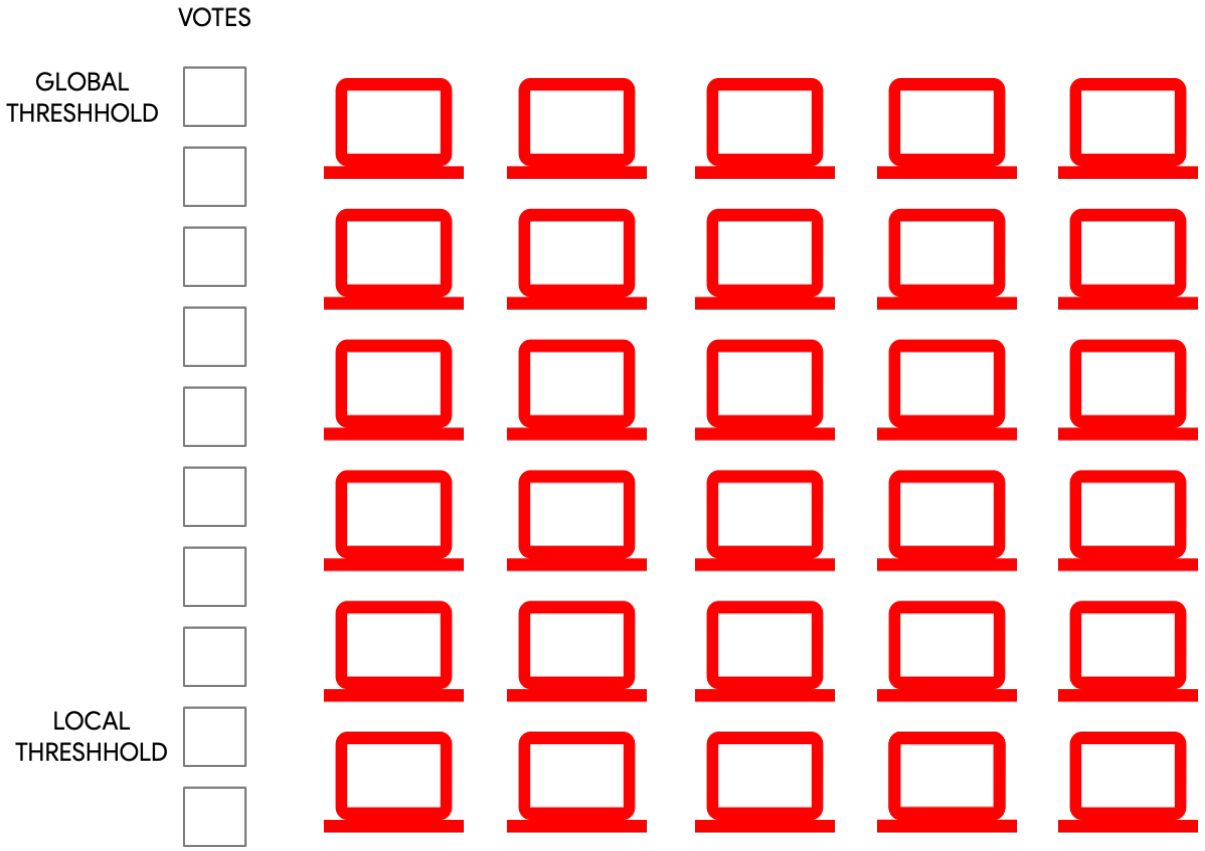

Binary Whitelisting at Google
Secure
docs.google.com/presentation/d/1FCFH68sxSKFKN31Amg-c5fFC_5NyVy1fQsd91f9G8jo/edit#slide=id.p
Two years old
> 100,000 devices
Mac + Windows
Small eng team
App Engine is great
Verify that this is the application you intended to run
Fantastical
SHOW CONTENTS
498
Flexibits Inc.
11
Whitelisted
1 week, 5 days ago
chief-laptop
/Applications/Fantastical 2.app
Review whether our analysis services consider this application to be safe
Analyzed: Safe
SHOW RESULTS
Cast your vote for this application
FLAG POSSIBLE MALWARE
MAC
DEV
OPS
YVR
8:49 / 19:51 • Requirements

Rule Management

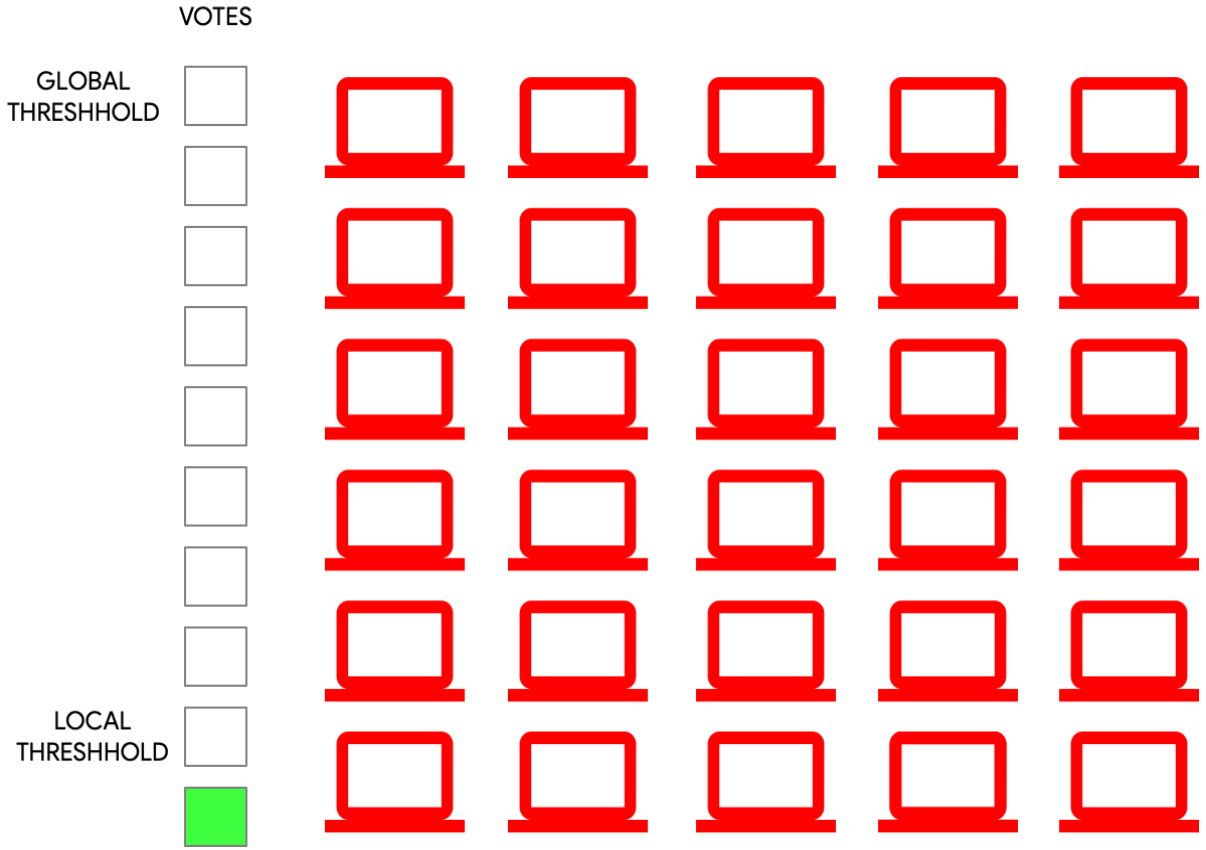
- Most endpoints run in Lockdown mode (default deny)
- Maintaining allowlists not feasible at scale
- Social voting at Google
- First presented by Matt Doyle at MacDevOps YVR

  https://www.youtube.com/watch?v=zUvzTaeOVd8

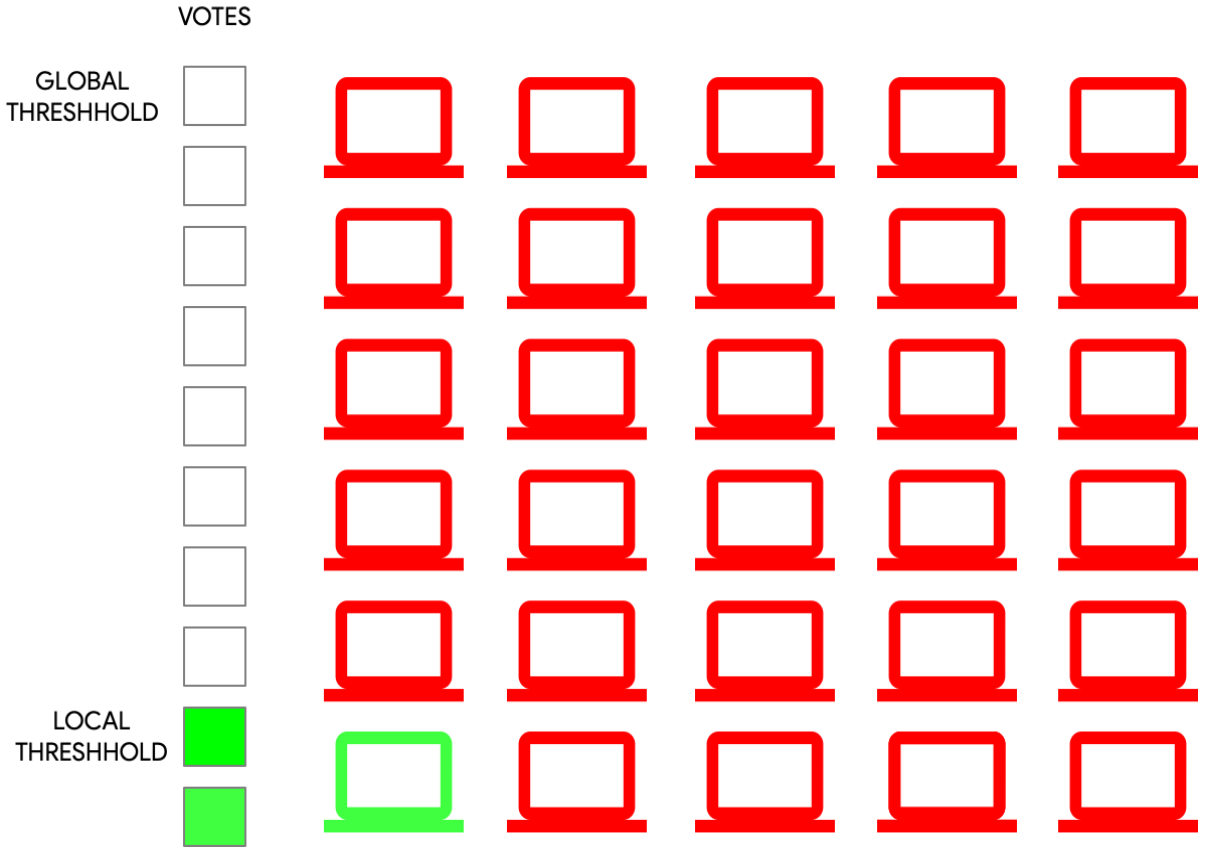
Social Voting



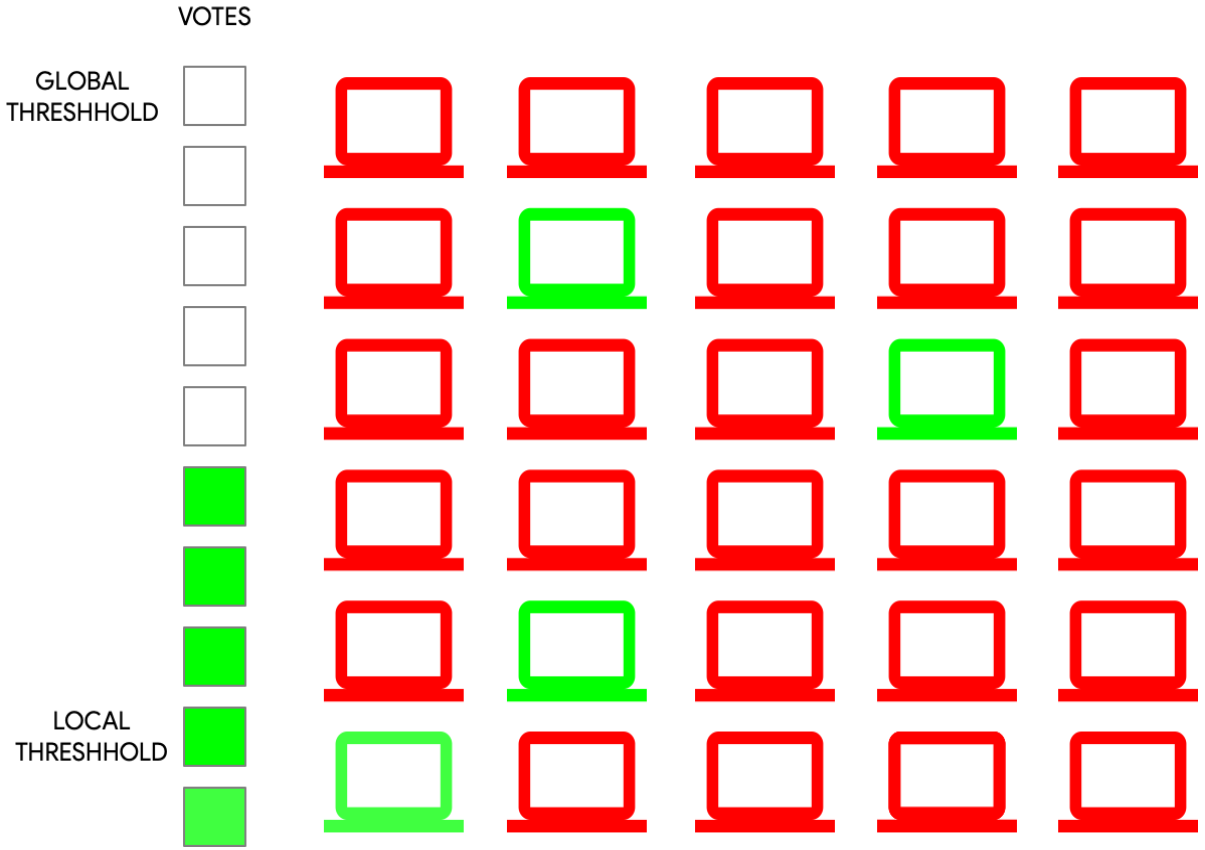
Social Voting



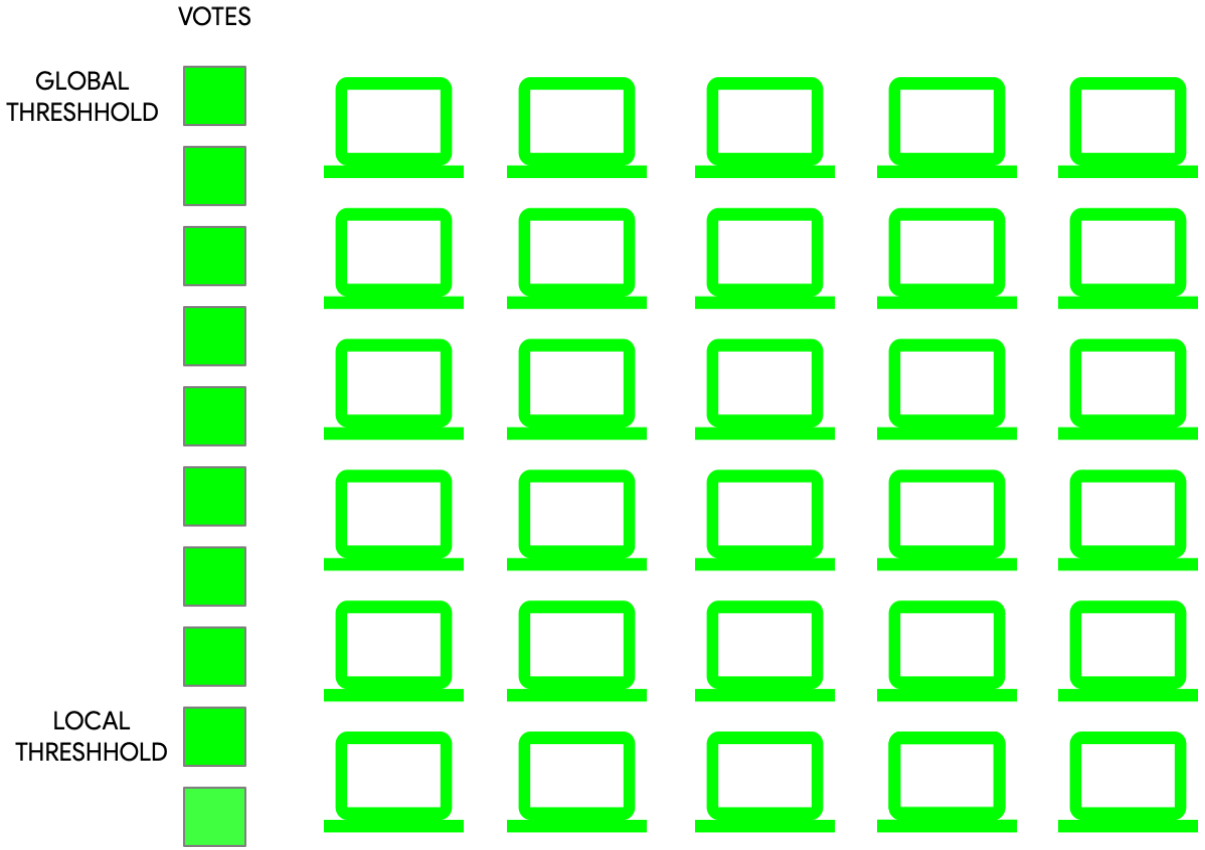
Social Voting



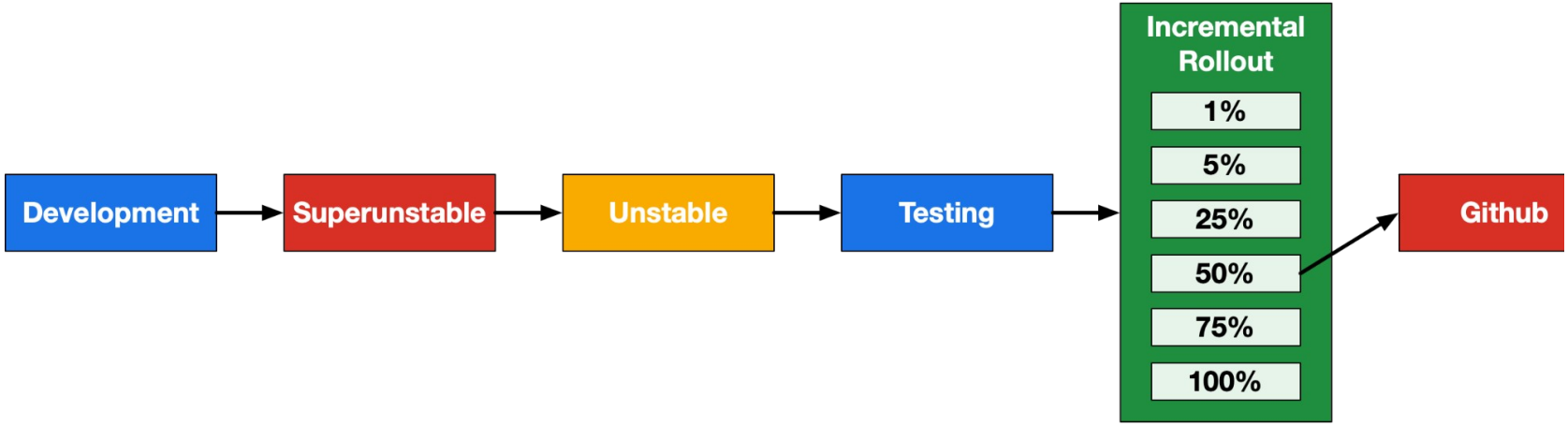
Social Voting



Social Voting



Typical Release Process



Making a Modern Santa

Transitioning to a Dedicated Team for macOS

- Santa originally a 20% project
    - @russellhancox & @tburgin
- Team formed in mid-late 2021 with a macOS endpoints focus

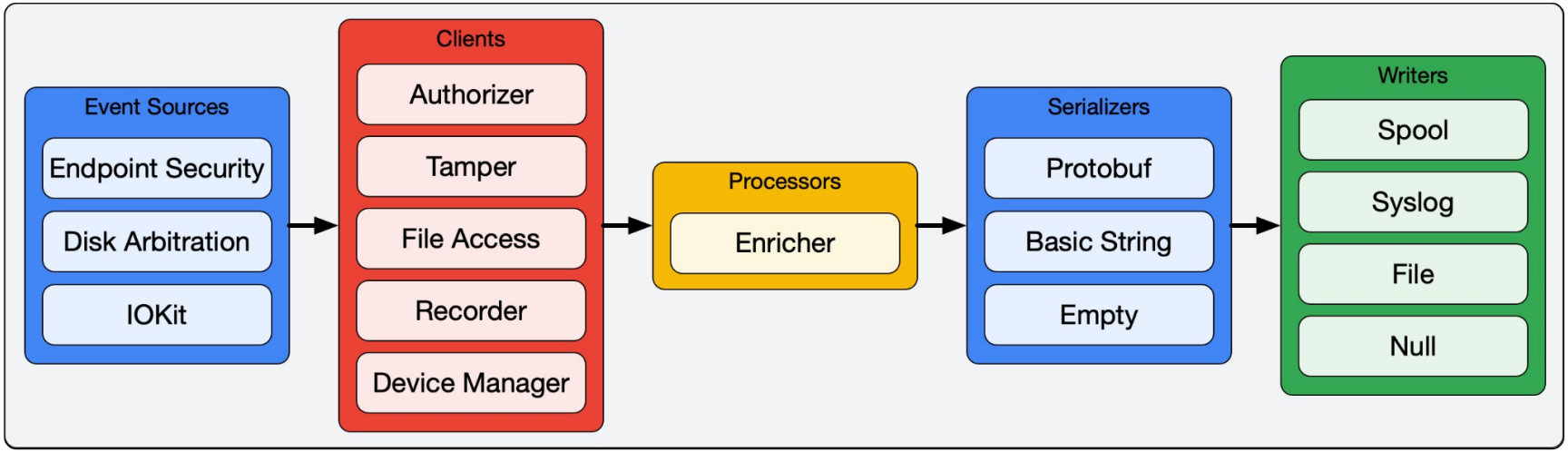
Adopting EndpointSecurity APIs

- Originally a kext-based solution
- Began adopting ES late 2019, macOS 10.15
- ES events translated into existing structures and data flows

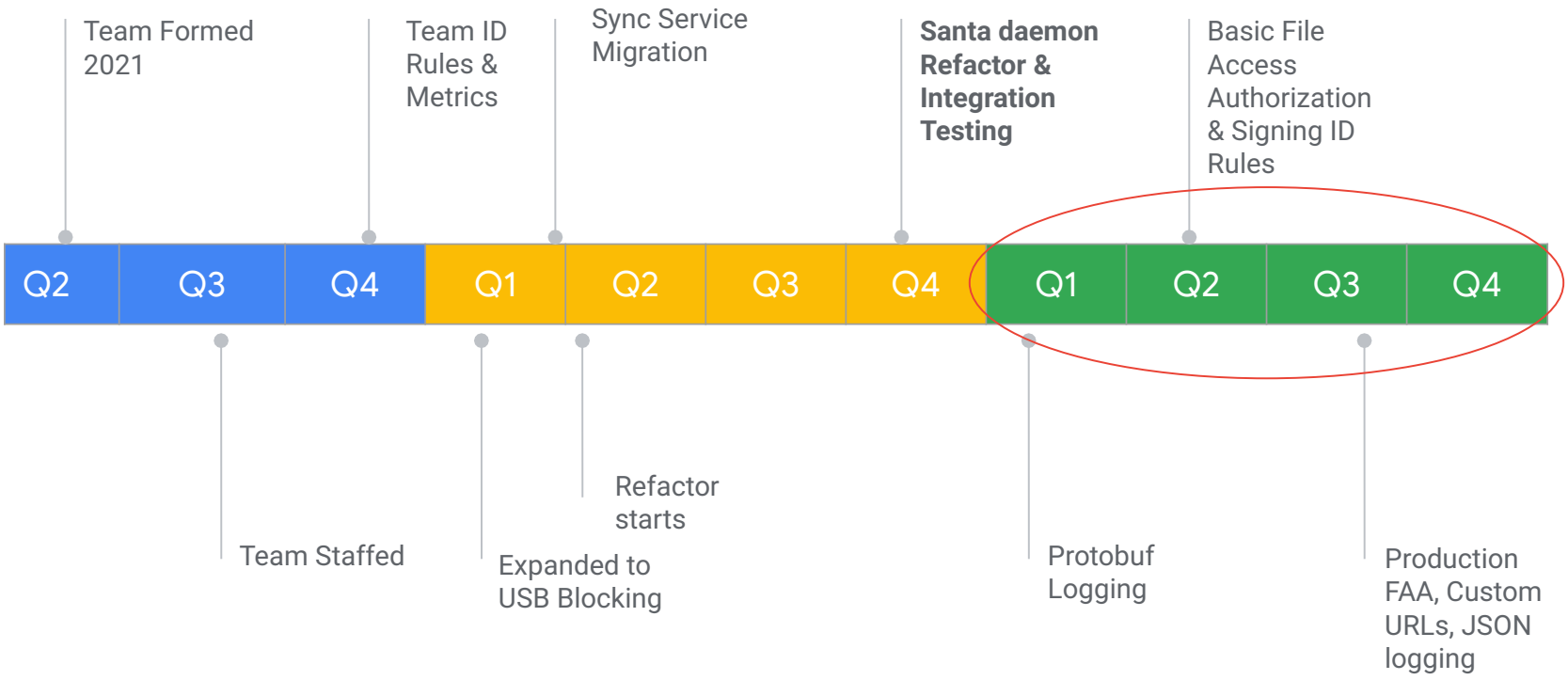
The Need to Redesign

- Performance concerns for new features
- Dropping kext support
- Reducing reliance on Objective-C

Rearchitecting Santa



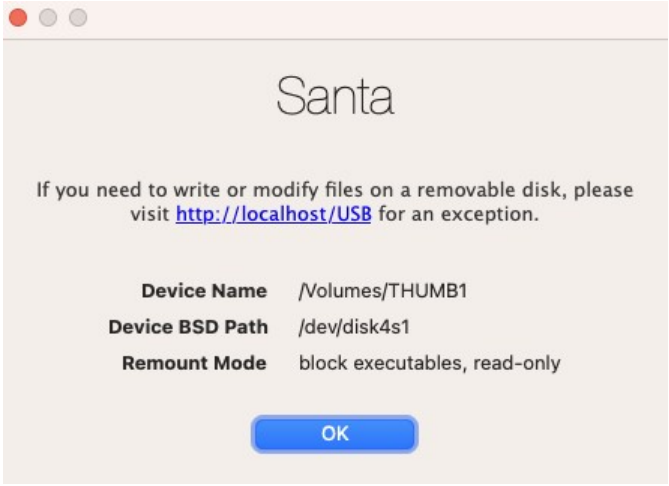
Recent Timeline of Major Features



What's New?

USB Mass Storage Restrictions

- Blocking USB mass storage devices
- Forcing mount flags
- Exception flow via sync protocol



File Access Authorization (FAA)

- Evaluate all file access attempts against policy
- Required OS changes
- Policy overview

File Access Authorization (FAA)

- Evaluate all file access attempts against policy
- Required OS changes
- Policy overview
  - Watch Items

```
<key>ChromeCookiesRule</key>
<dict>
  <key>Paths</key>
  <array>
    <dict>
      <key>Path</key>
      <string>/Users/*/Library/Application Support/Google/Chrome/*/Cookies</string>
      <key>IsPrefix</key>
      <true/>
    </dict>
    ...
  </array>
  ...
</dict>
```

File Access Authorization (FAA)

- Evaluate all file access attempts against policy
- Required OS changes
- Policy overview
  - Watch Items
  - Options

```
<key>ChromeCookiesRule</key>
<dict>
  <key>Paths</key>
  <array>...</array>
  <key>Options</key>
  <dict>
    <key>AllowReadAccess</key>
    <false/>
    <key>AuditOnly</key>
    <false/>
    ...
  </dict>
  ...
</dict>
```

File Access Authorization (FAA)

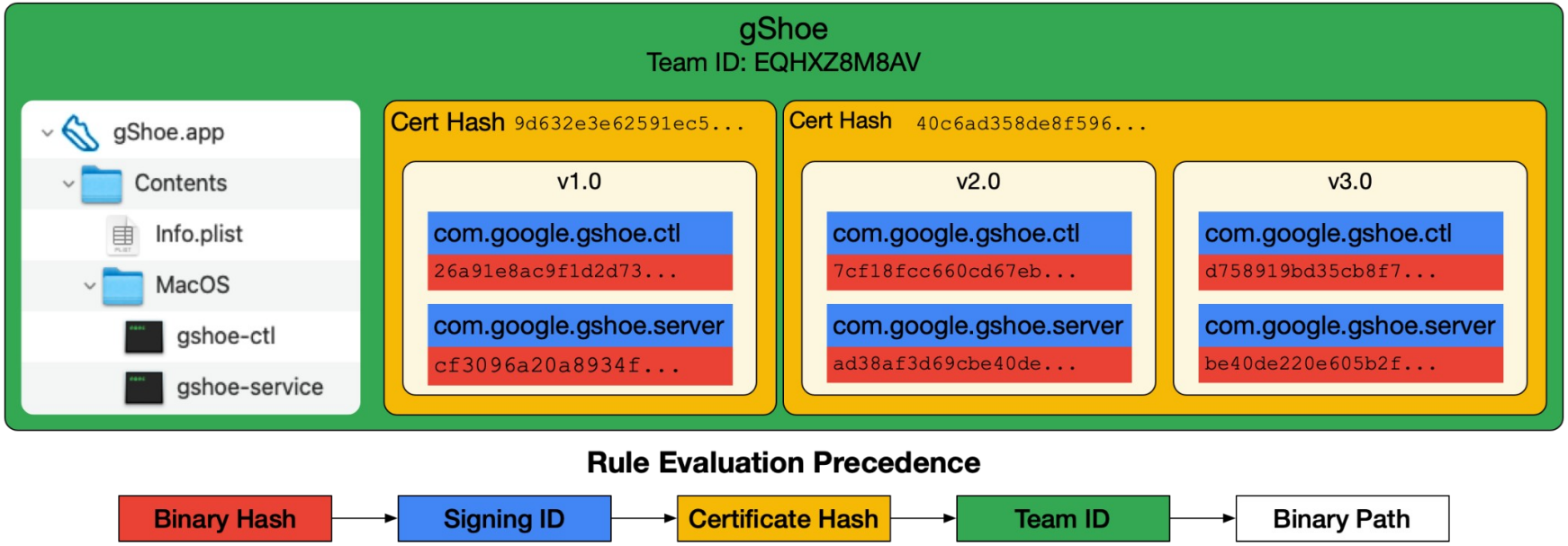
- Evaluate all file access attempts against policy
- Required OS changes
- Policy overview
  - Watch Items
  - Options
  - Exceptions

```
<key>ChromeCookiesRule</key>
<dict>
  <key>Paths</key>
  <array>...</array>
  <key>Options</key>
  <dict>...</dict>
  <key>Processes</key>
  <array>
    <dict>
      <key>TeamID</key>
      <string>EQHXZ8M8AV</string>
      <key>SigningID</key>
      <string>com.google.Chrome</string>
    </dict>
    <dict>
      <key>SigningID</key>
      <string>com.apple.mds</string>
      <key>PlatformBinary</key>
      <true/>
    </dict>
  </array>
</dict>
```

New Rule Types & Rule Precedence

- Team ID
- Signing ID

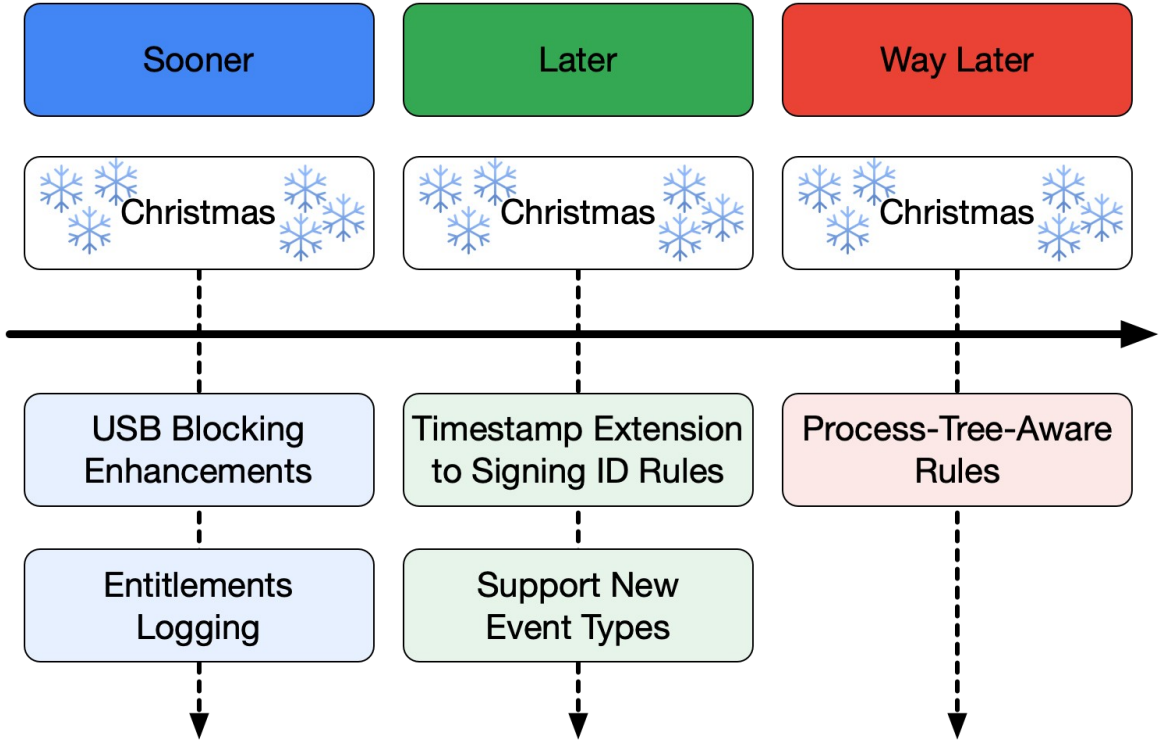
New Rule Types & Rule Precedence



Miscellaneous

- Ways to configure rules
  - Static rules
  - JSON rule import/export
- Per-rule Custom URLs
- Distributed Notifications

Coming Attractions



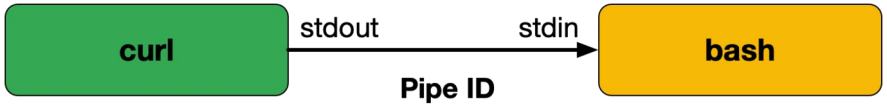
Better Detection & Response

Logging Enhancements

- Structured logging via Protobuf and JSON
- Added new fields to telemetry
- Enrichment data and most ES event data

Powerful Detection Primitives

- Better process grouping (process group/session IDs)
- setuid
- File descriptor info
  - `curl | bash`, Sockets
- Environment vars
- Code signing flags

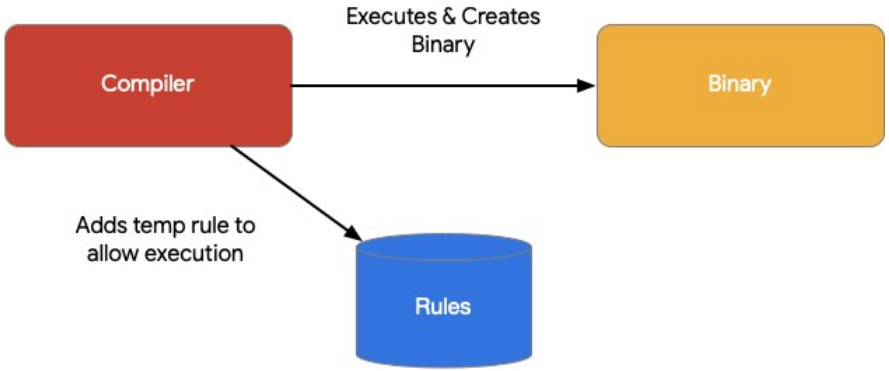


“Tripwire” FAA Rules

- Watch / Lockdown creds
  - Bearer tokens, browser cookies, honey tokens
- Watch / Lockdown config modifications
  - SSH authorized_keys files, sudoers, pam
- Filter by code signing info to avoid false positives

More Livable Lockdown

- Better toolchain support
- Easier to administer transitive allowlisting



Getting Involved

Santa Community

- santa.dev
- github.com/google/santa
- Discussions / Issues / PRs
- Sync service contributions