NORTH POLE SECURITY

Santa Past, Present, And Future

A Christmas Carol

Nice To Meet You!

PETE MARKOWSKY
Led all first party security agent development at **Google**, including Santa. Previously co-founded **Capsule8** Linux Cloud EDR company

MATT WHITE
Previous Santa project lead at **Google**. Original author and lead of the **Apple** Endpoint Security Framework

Today's Agenda

1. What Is Santa?
2. Ghost Of Santa Past
3. Ghost Of Santa Present
4. Ghost Of Santa Yet To Come

What Is Santa?

What Is Santa?

- An Open Source macOS Security Agent
- Policy enforcement
  - Application allowlisting, file access control, USB media control
- Endpoint telemetry

What Is Santa?

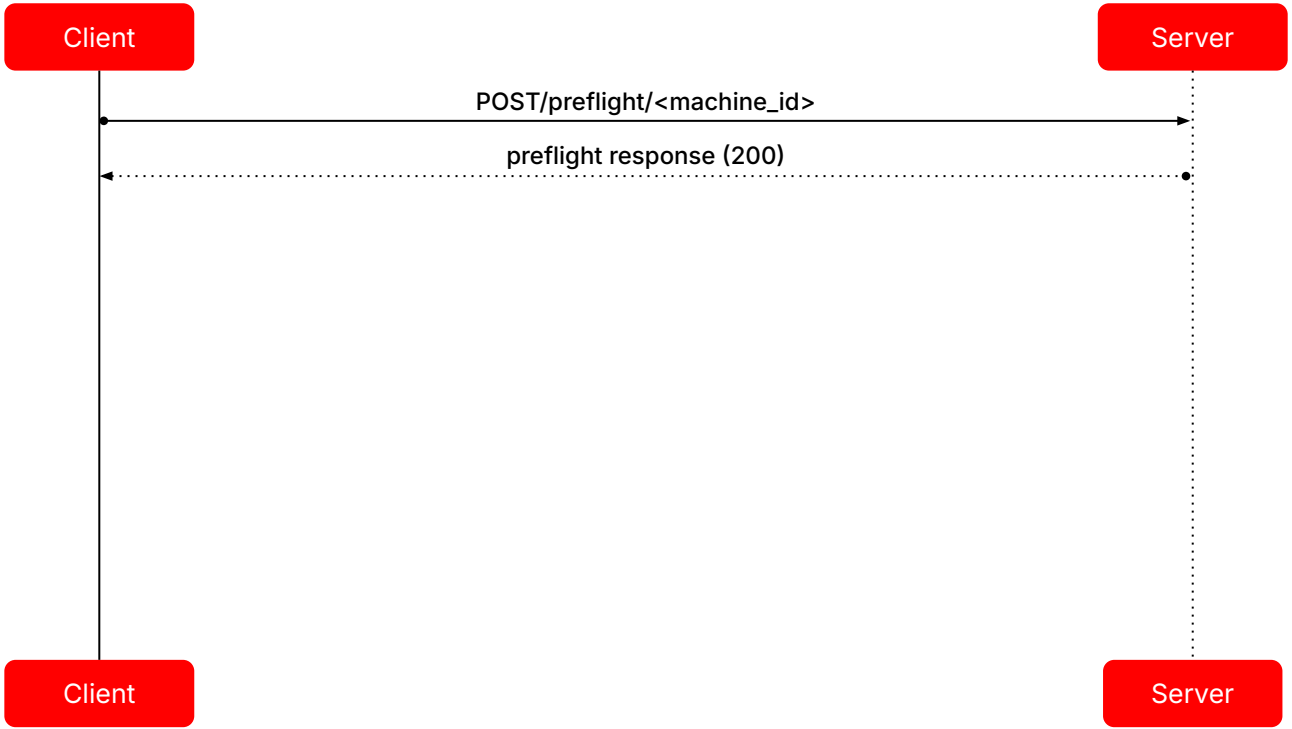
- Performant & Safe
- Effective & Can Be Deployed Next To EDR
- Designed for guard rail style security (social voting)

Guard Rail Security

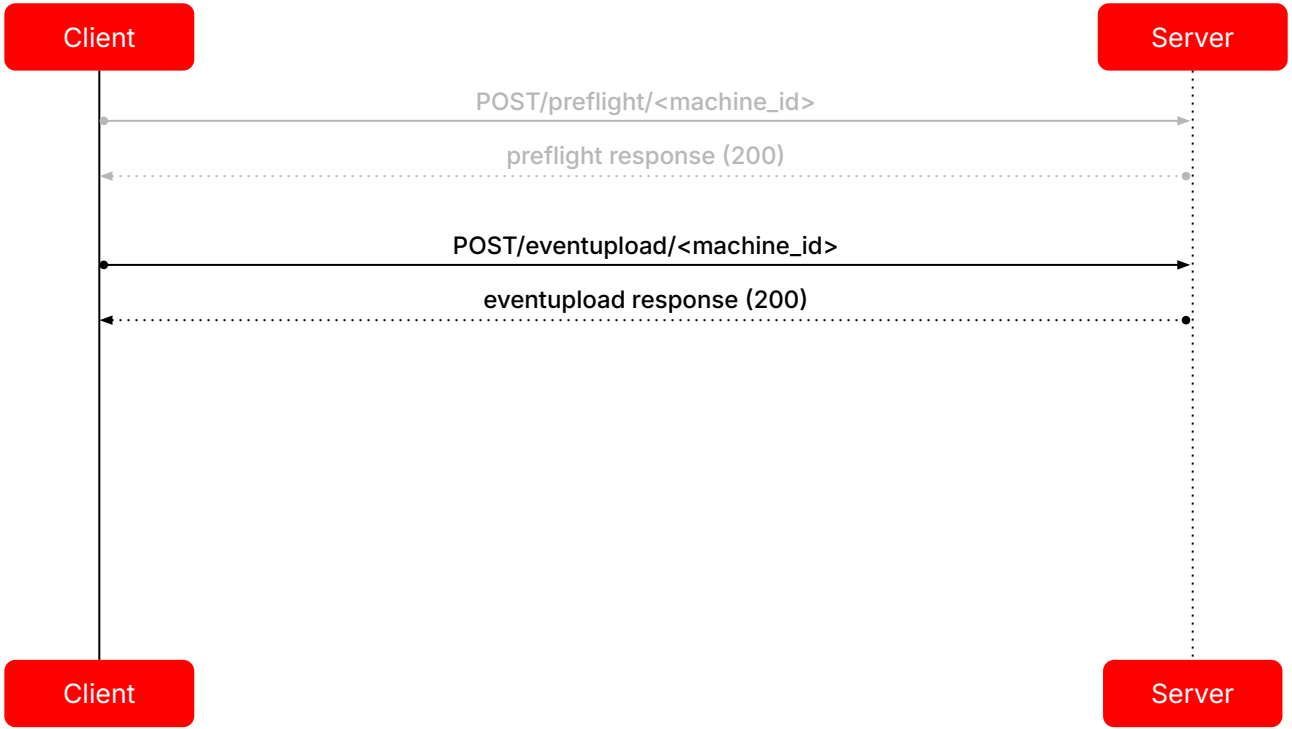
- Allow security to define the line of what's risky via a risk engine
- Enforcement tools supply context for risk engine to check requests against the line
- Bespoke tools help users safely approve low-risk requests, or alert security
- Tools need to be responsive
- Process is incremental & impact is monitored

Synchronization

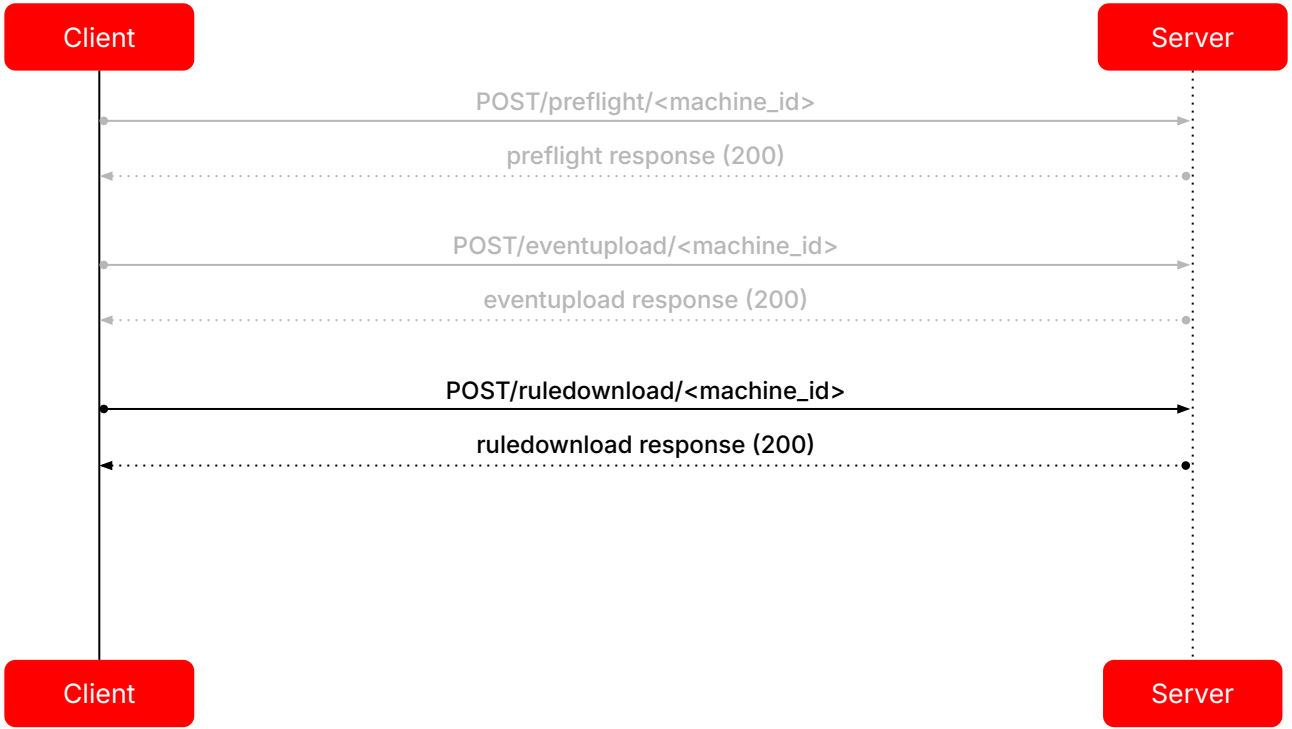
Synchronization



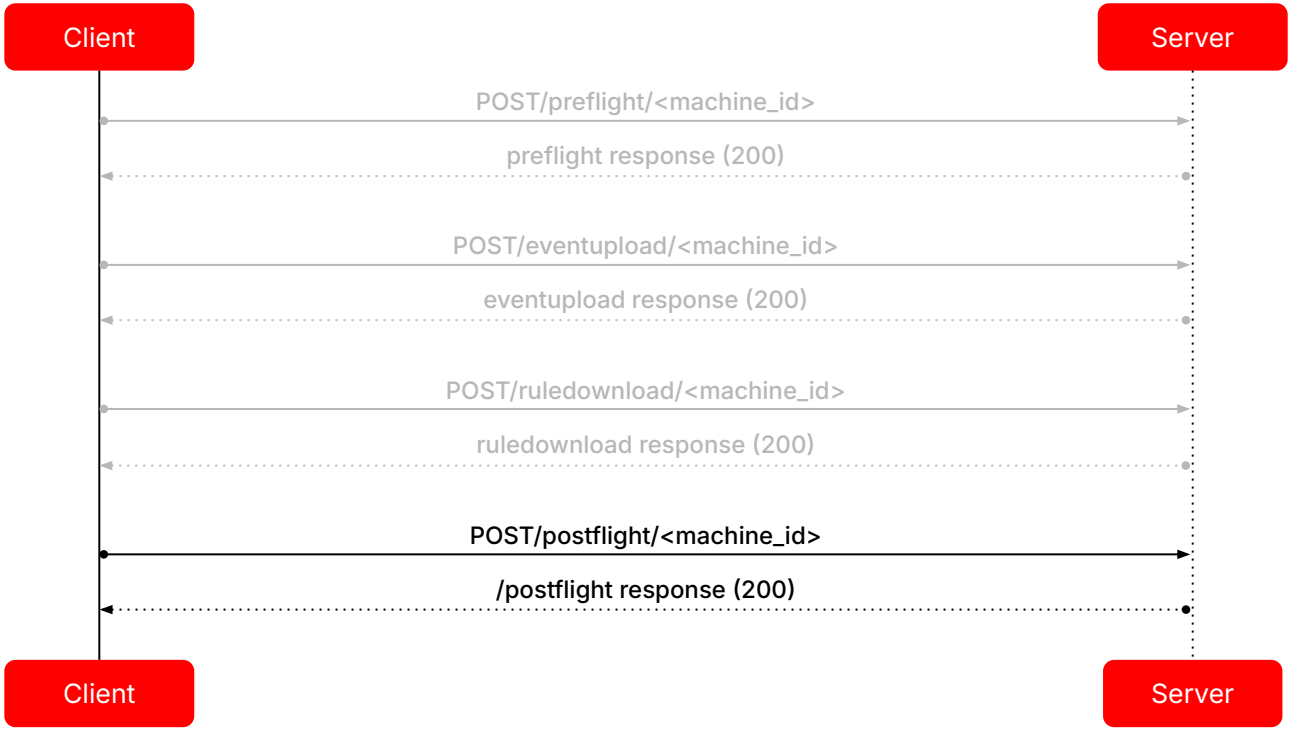
Synchronization



Synchronization



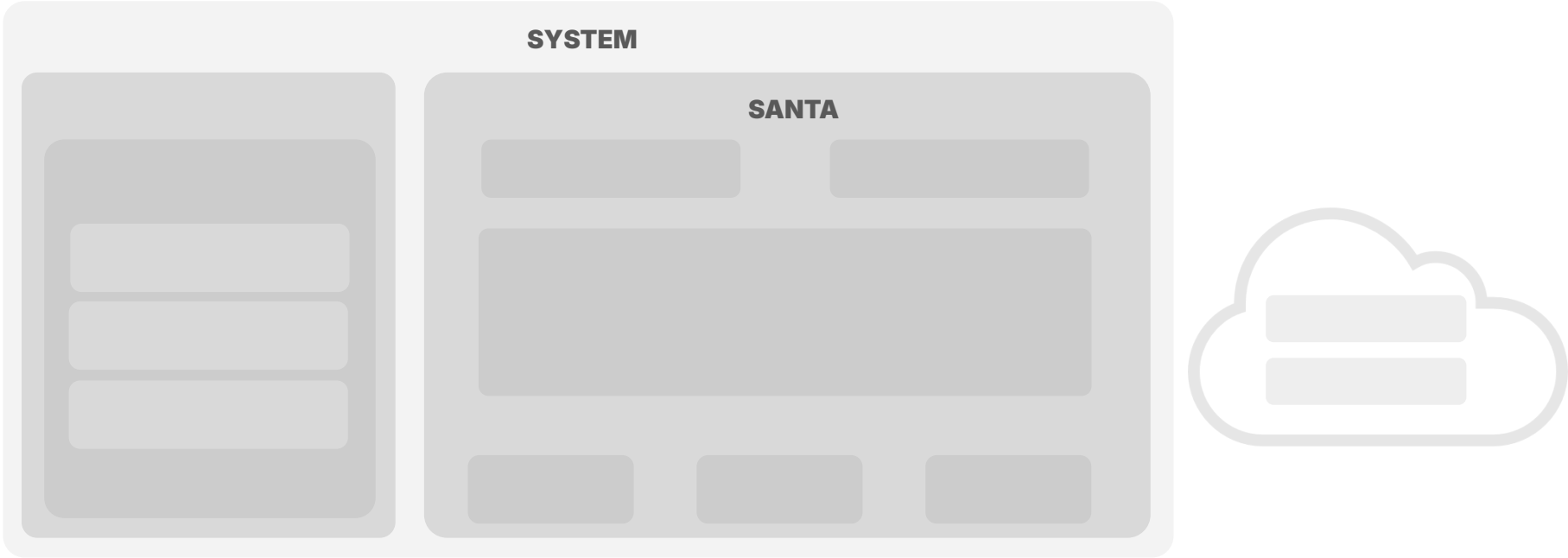
Synchronization



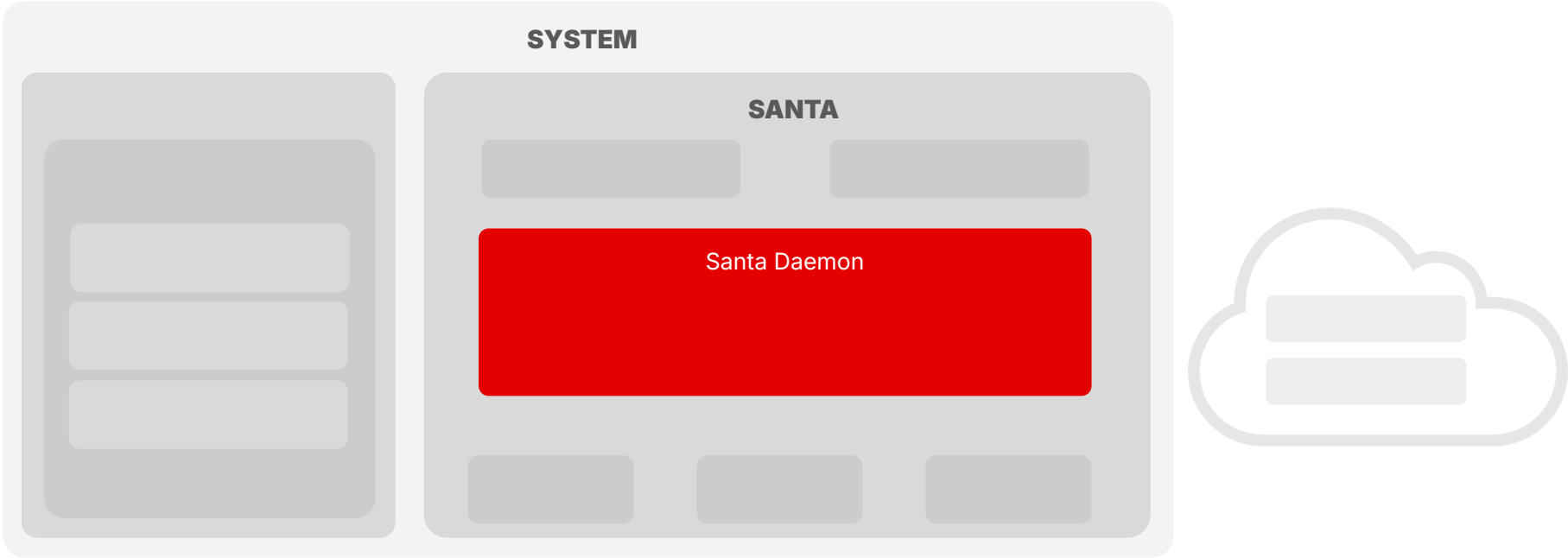
What Is Santa

Architecture

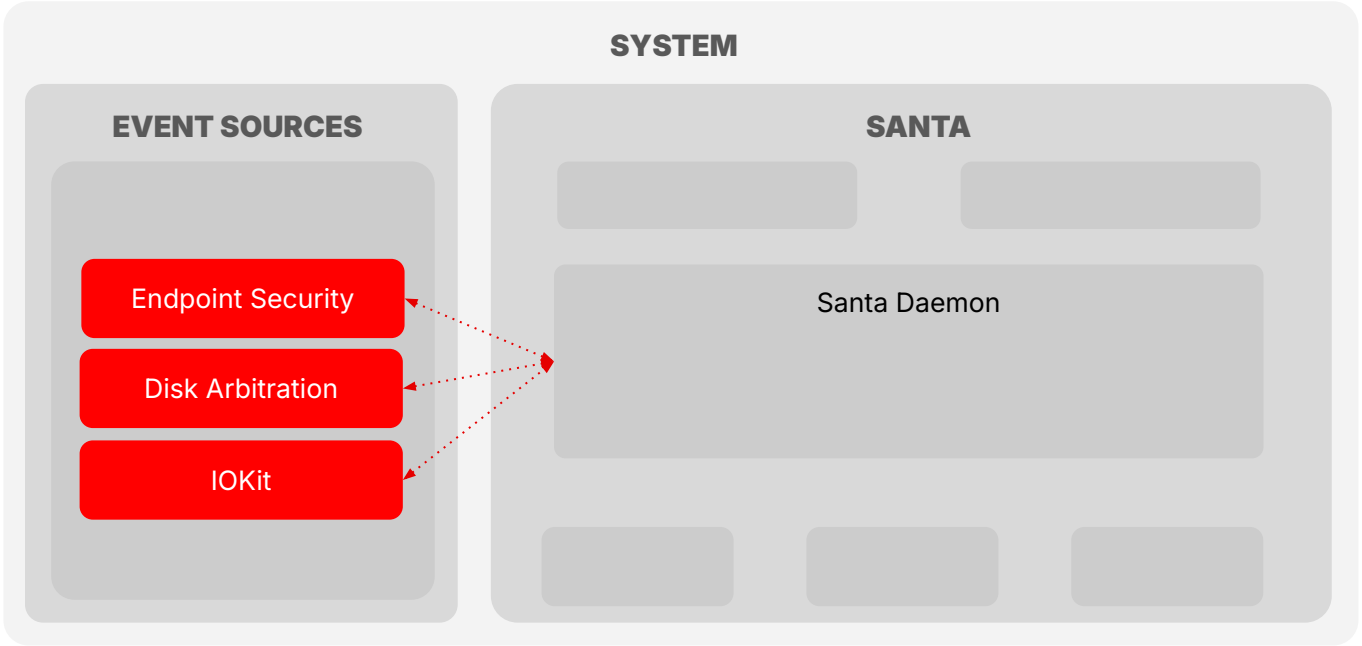
Santa Architecture



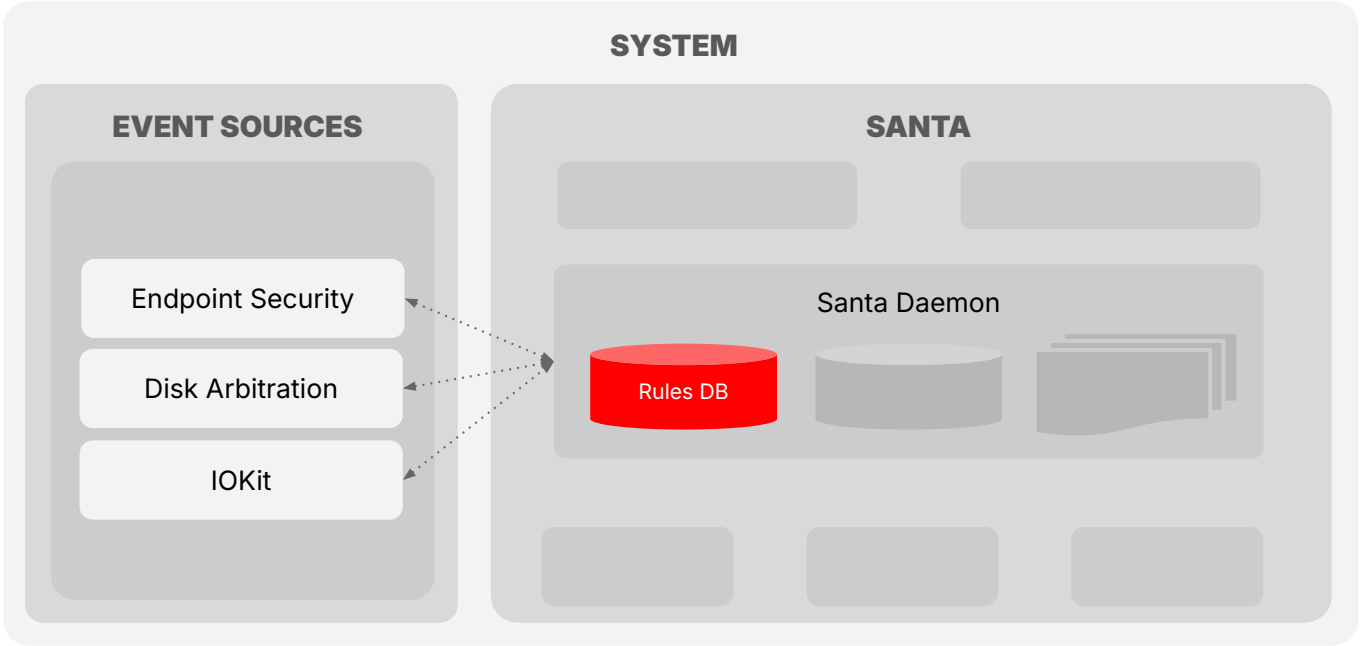
Santa Architecture



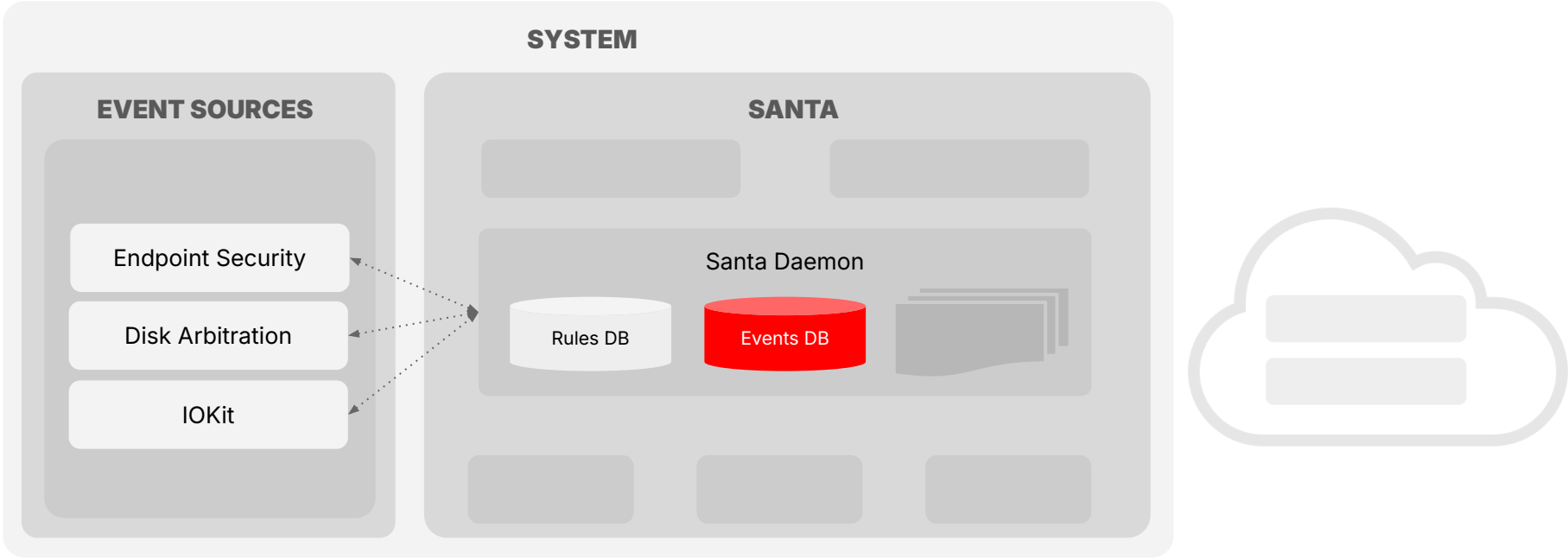
Santa Architecture



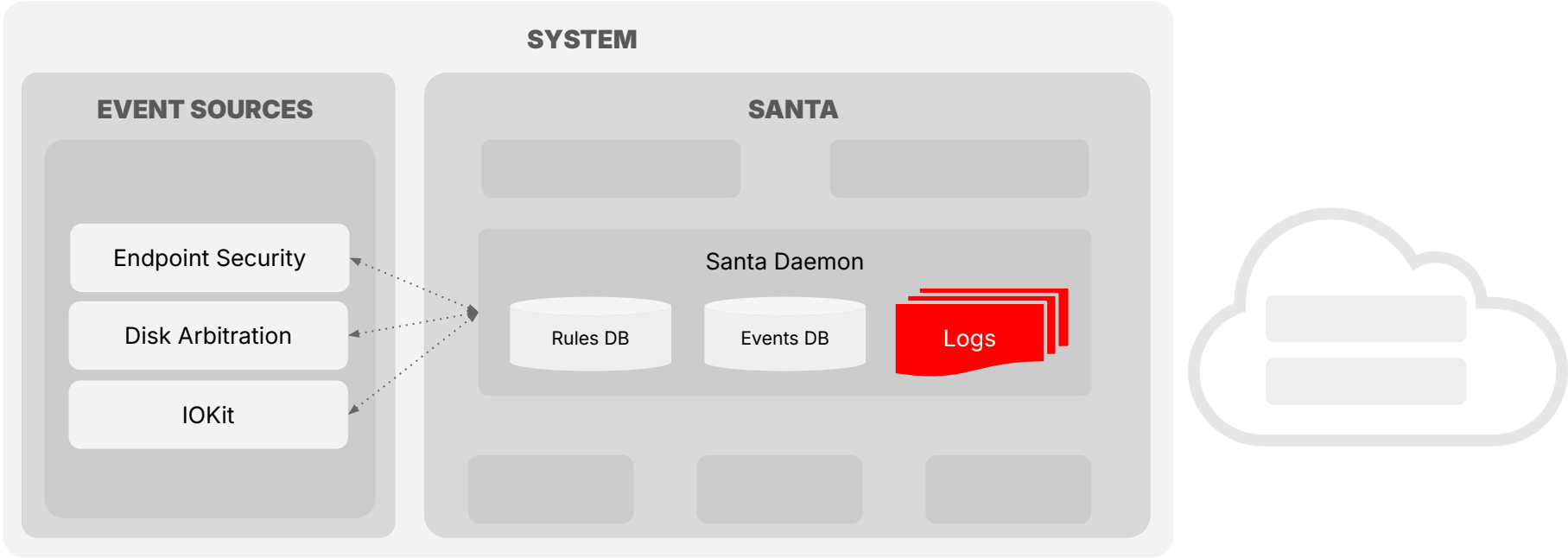
Santa Architecture



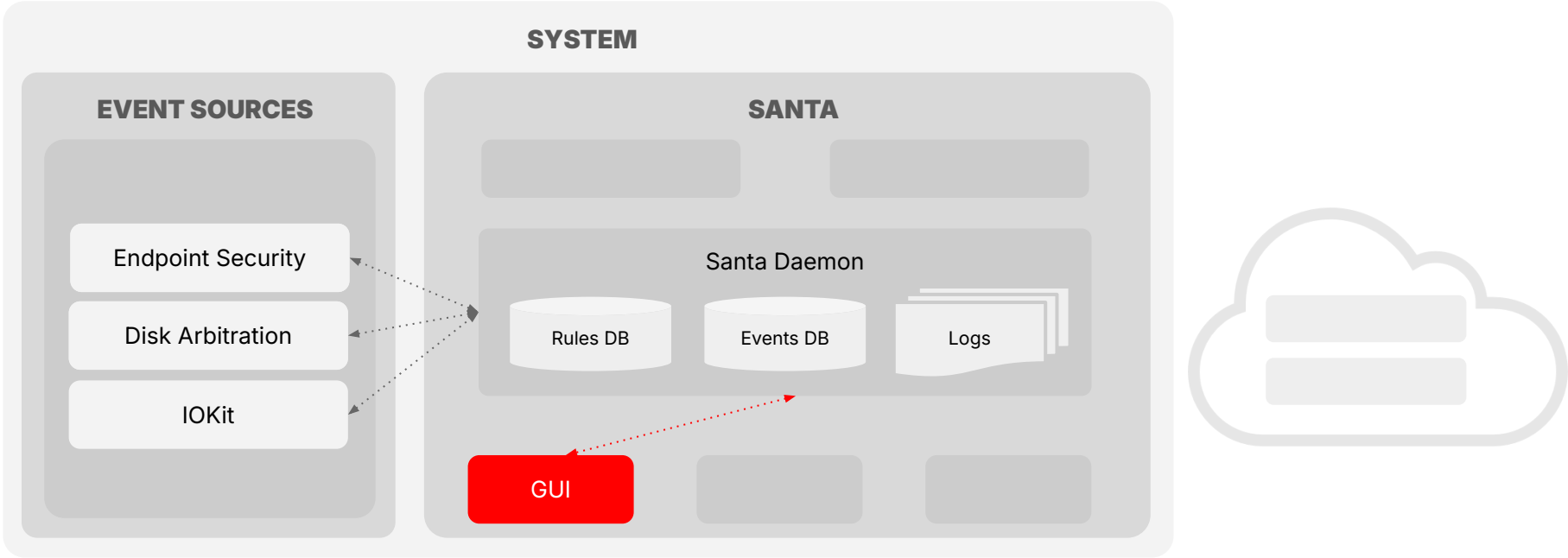
Santa Architecture



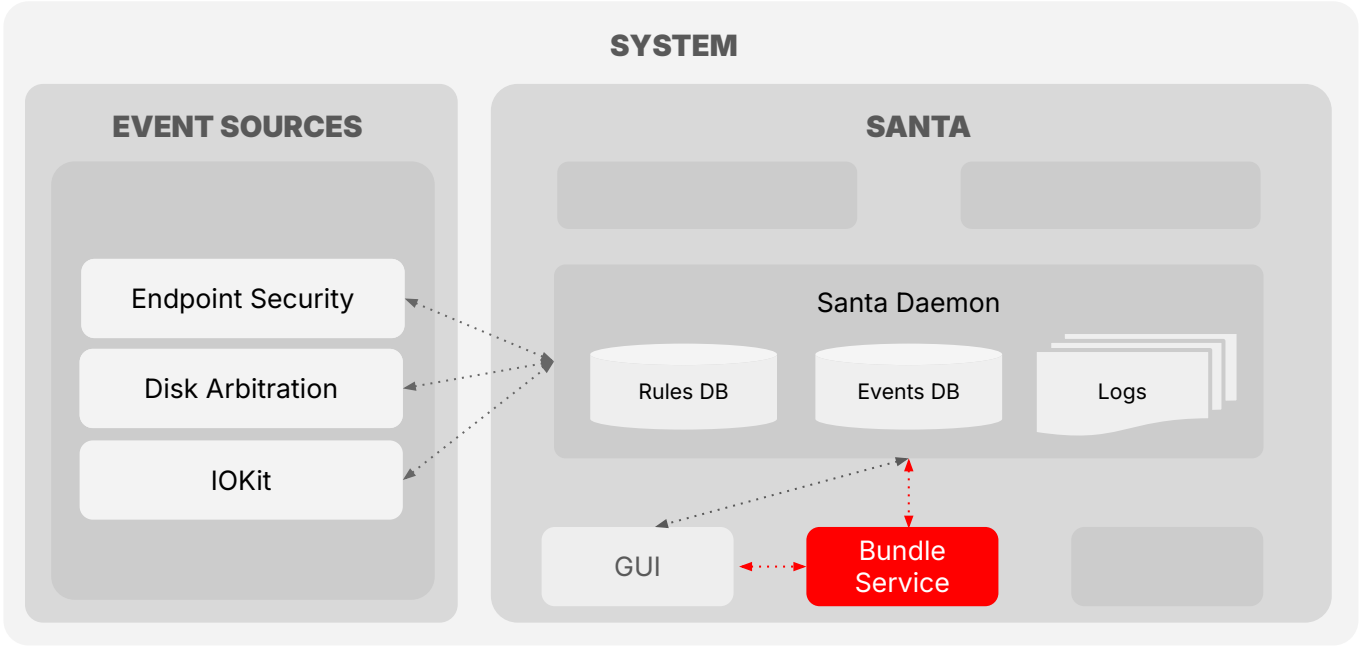
Santa Architecture



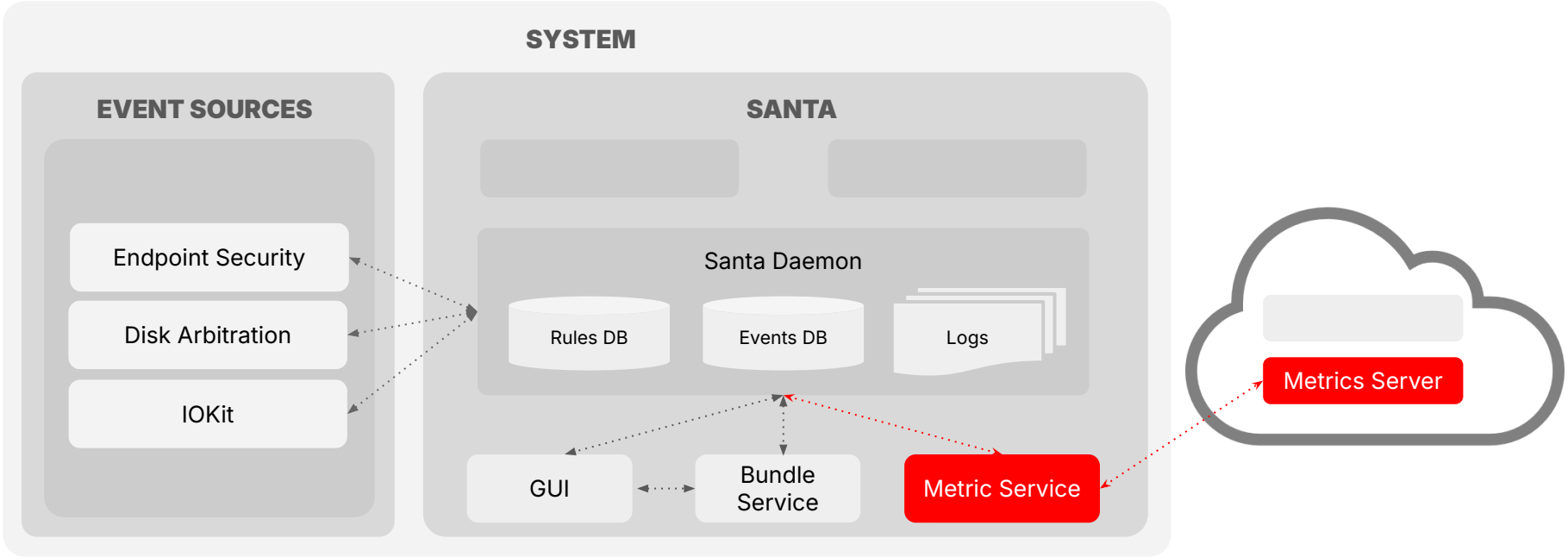
Santa Architecture



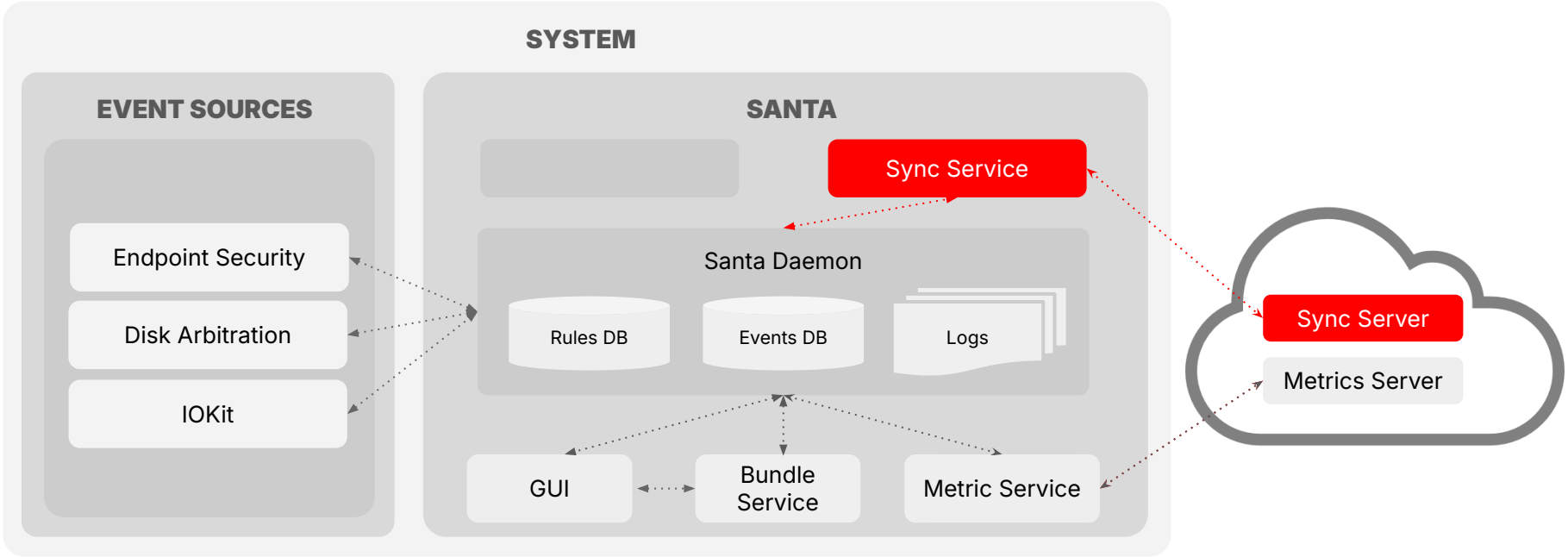
Santa Architecture



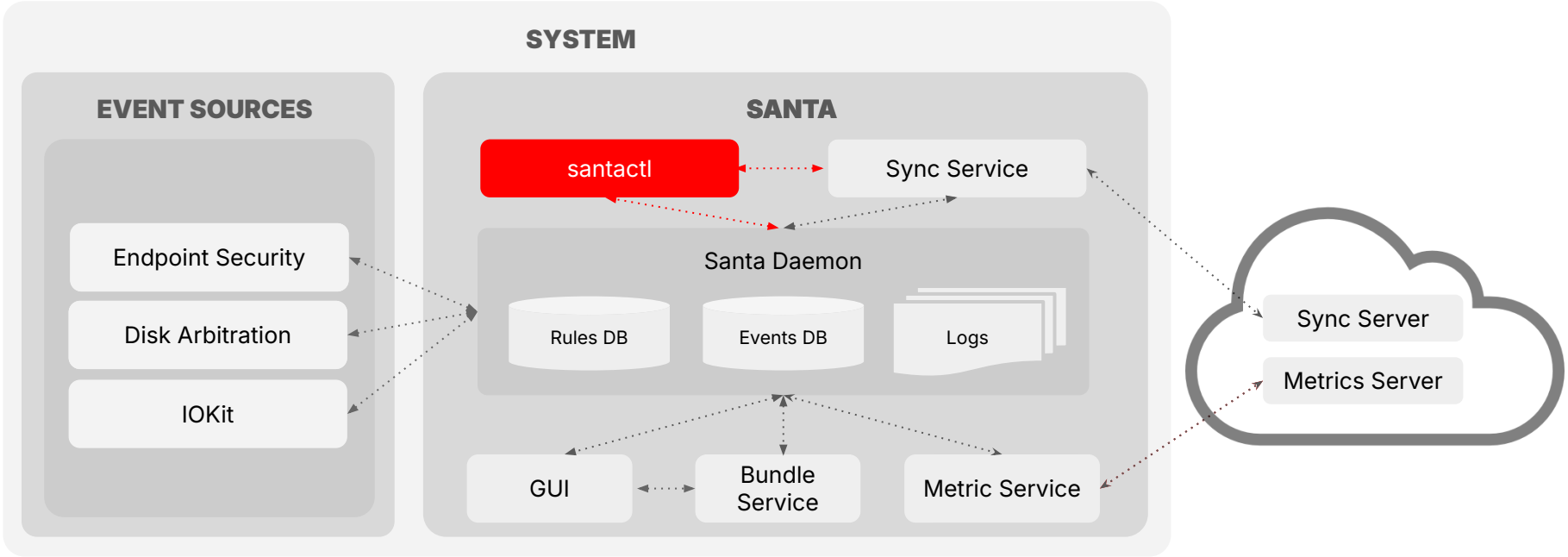
Santa Architecture



Santa Architecture



Santa Architecture



Ghost Of Santa Past

NORTH POLE SECURITY

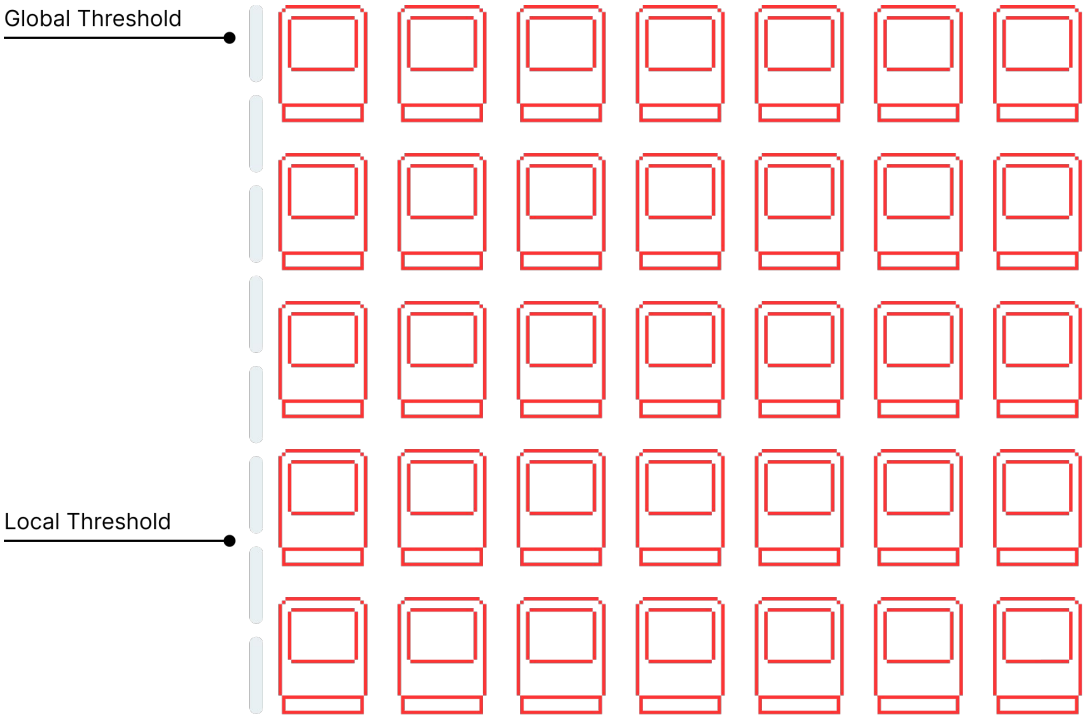
Deployment At Google

- Agent development done entirely in open source
- Built via in house build system
- Binaries deployed via custom package manager
- Configuration managed via MDM

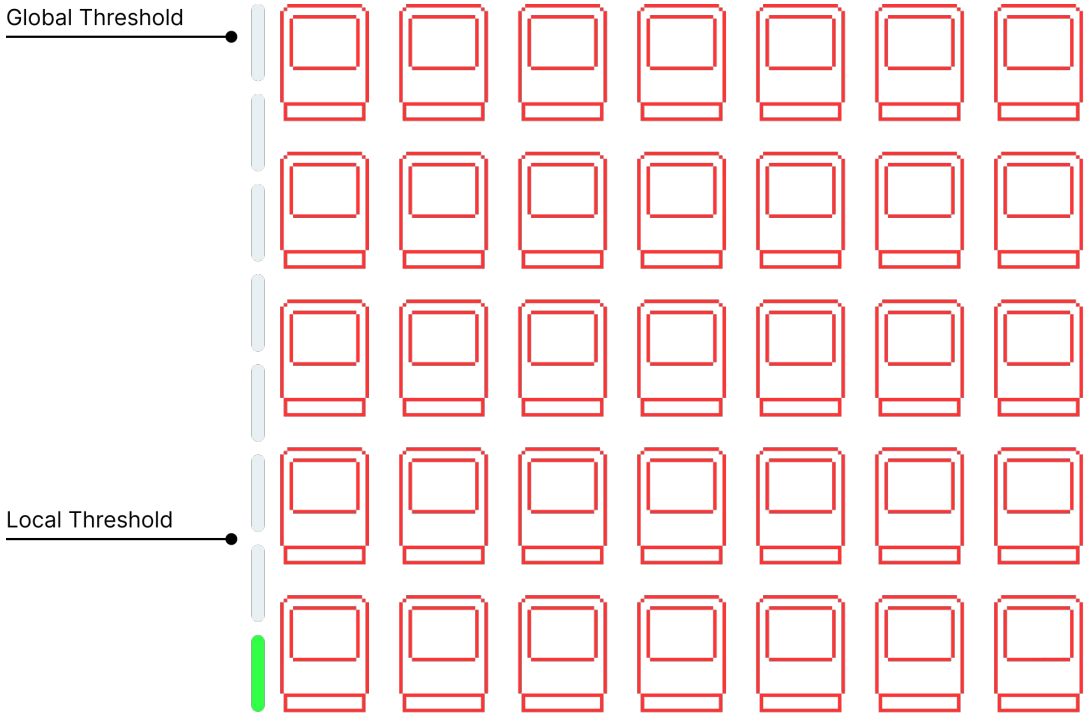
Rule Management

- Most endpoints run in default deny mode (Lockdown mode)
- Maintaining allowlists not feasible at scale
- Social voting
- First presented at MacDevOps YVR ‘18

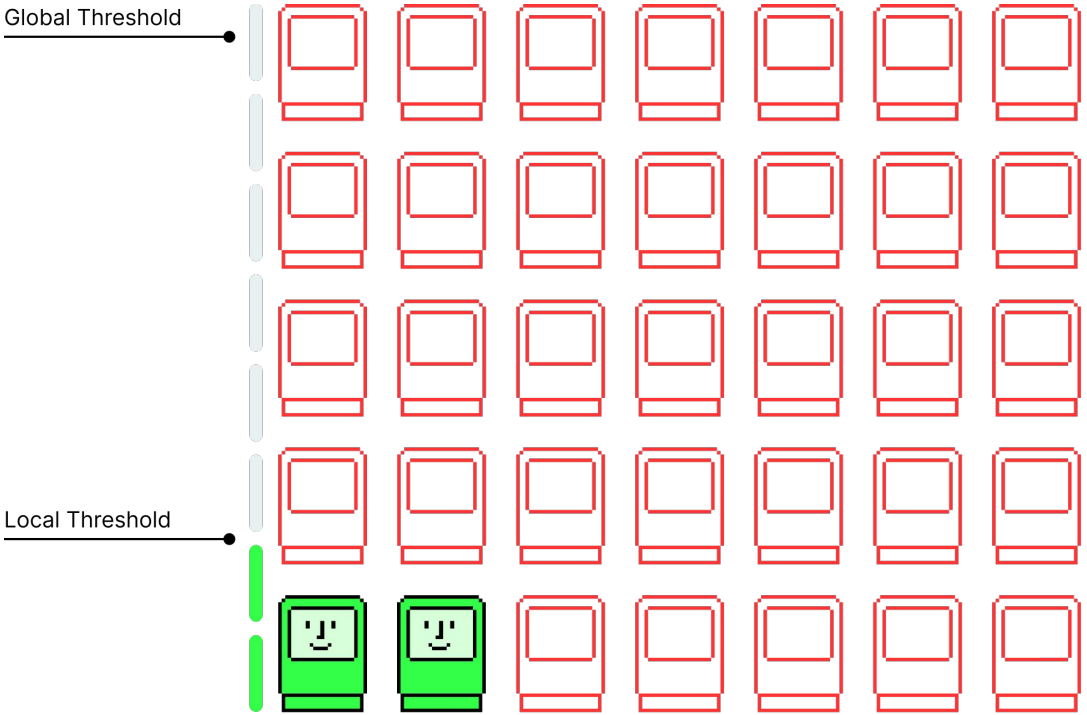
Social Voting



Social Voting

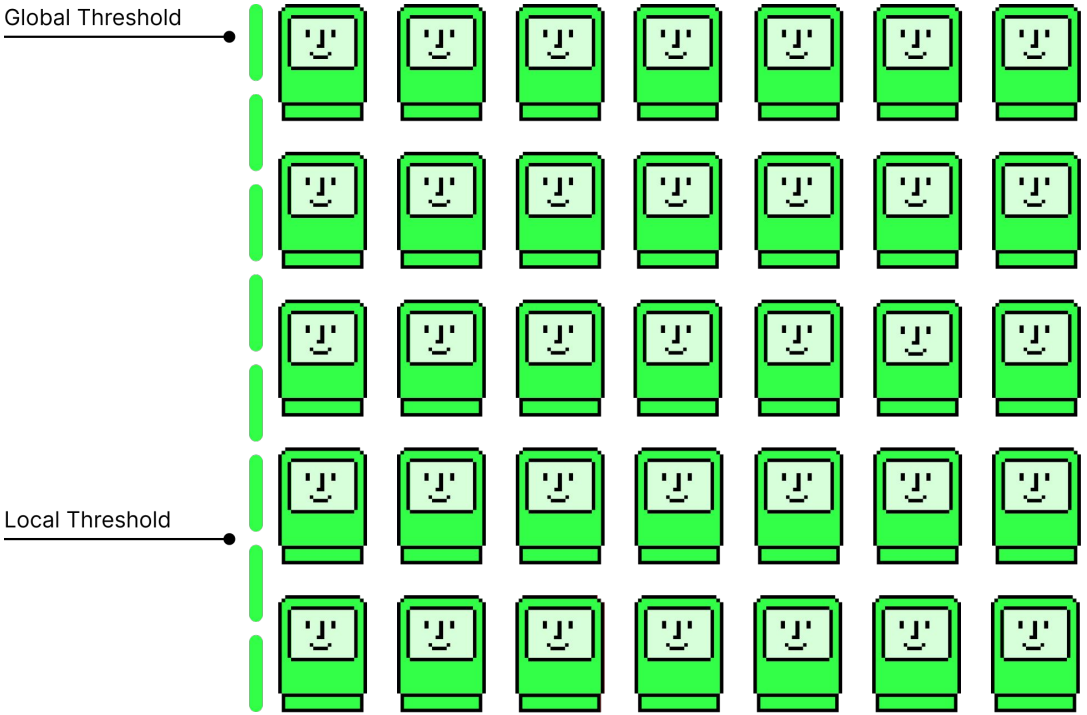


Social Voting

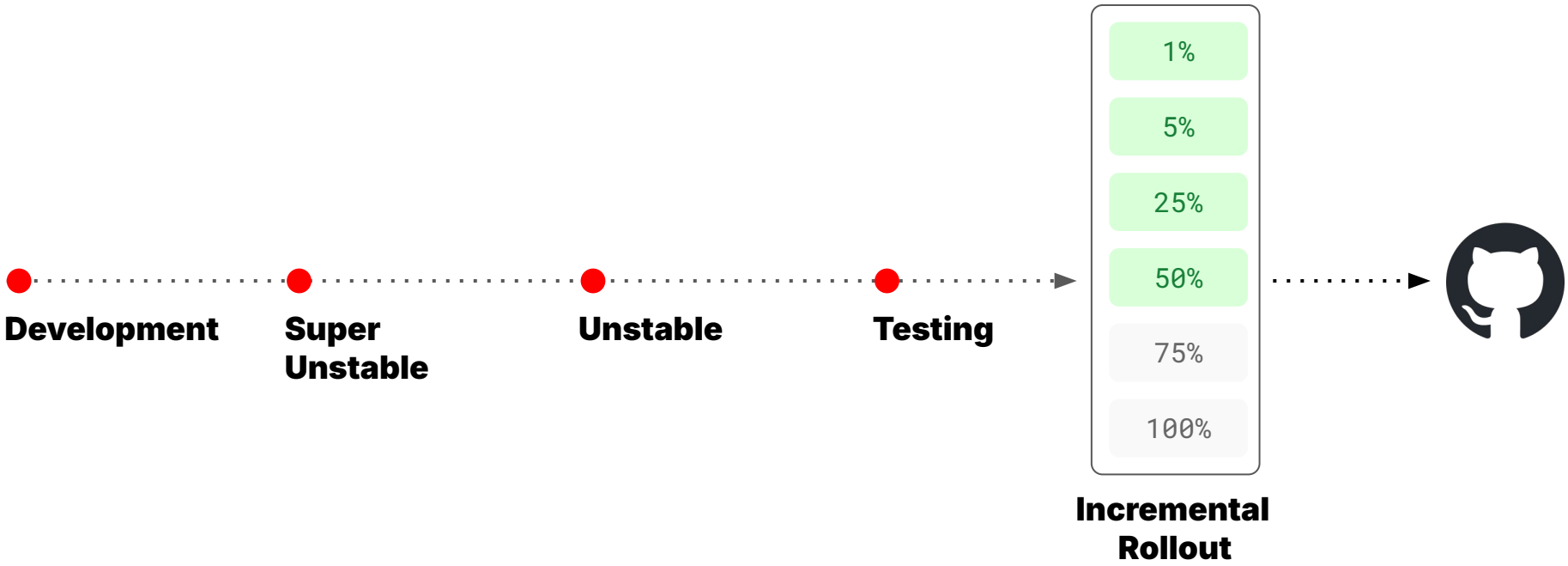


Social Voting

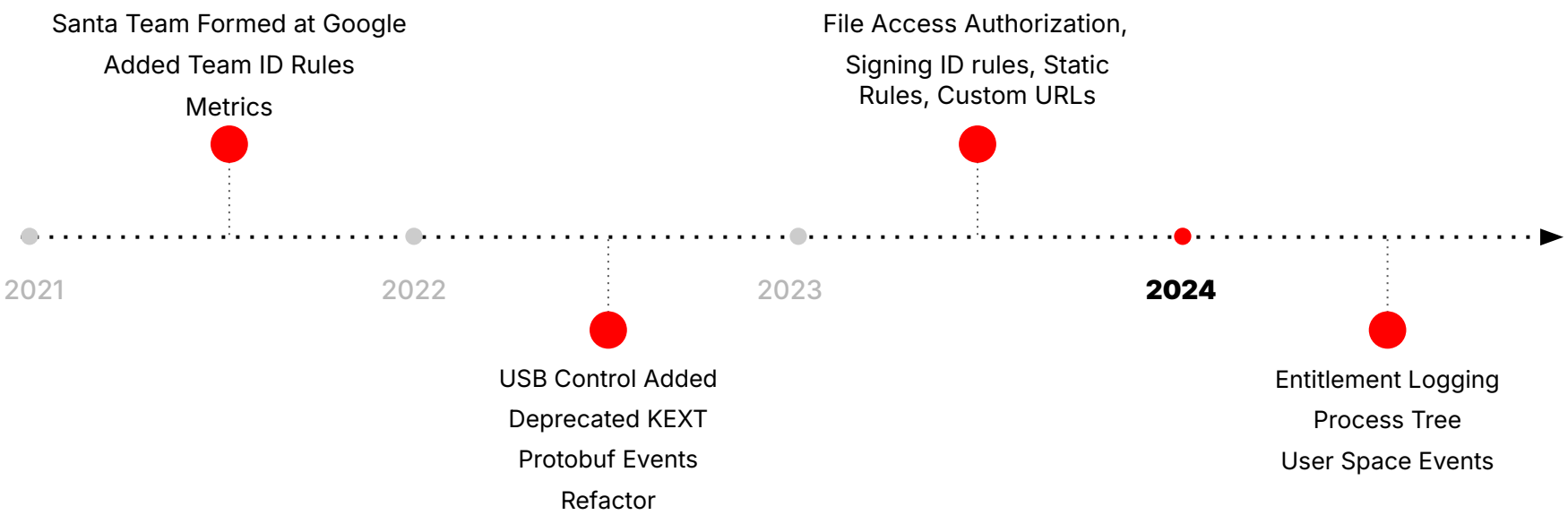
Social Voting



Typical Release Process



History of Santa



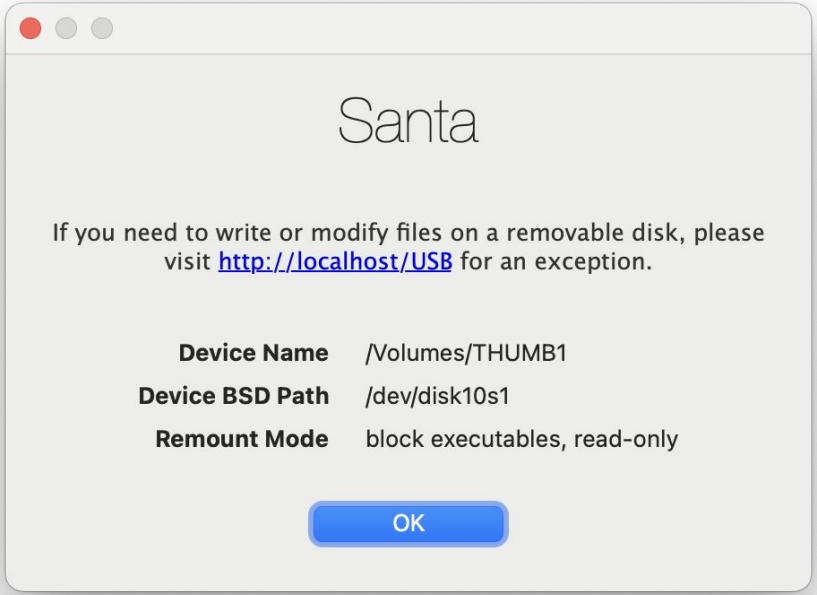
Ghost Of Santa Present

NORTH POLE SECURITY

Ghost Of Santa Present

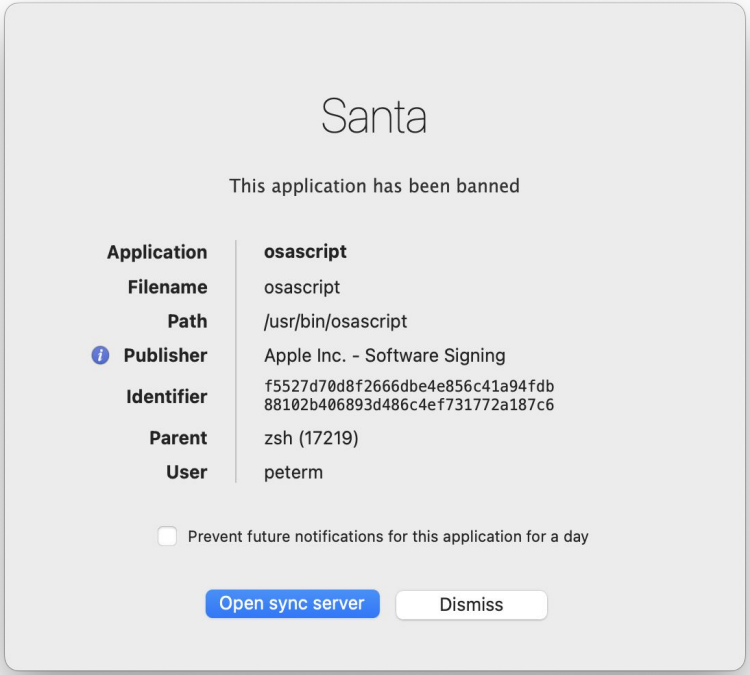
Authorizations

USB Mass Storage Restrictions



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

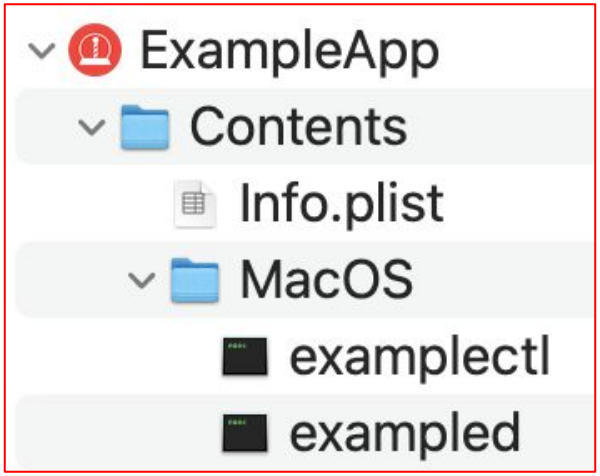
Binary Authorization



- All executions are evaluated against policy
- **Supported Rule types:**
  - CDHash, Binary Hash, Singing ID, Certificate Hash, Team ID
- Transitive allowlisting
- Lockdown Mode vs. Monitor Mode

Rule Types and Precedence

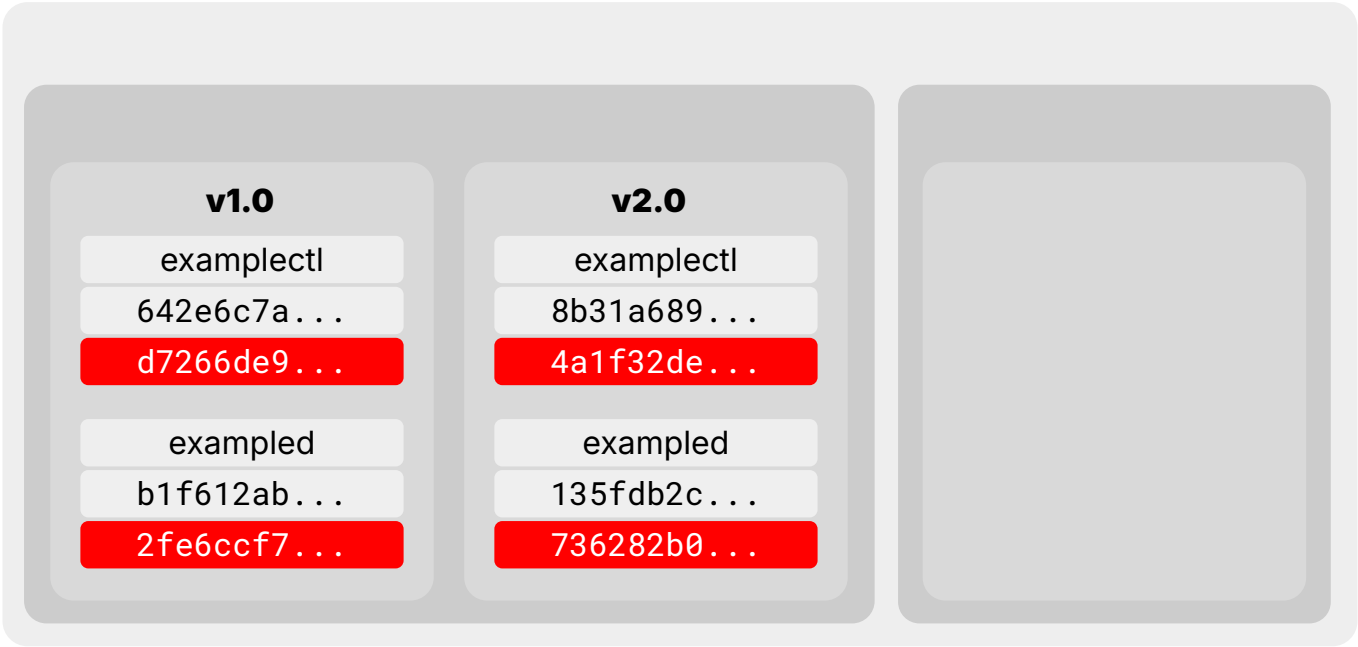
Rule Types and Precedence



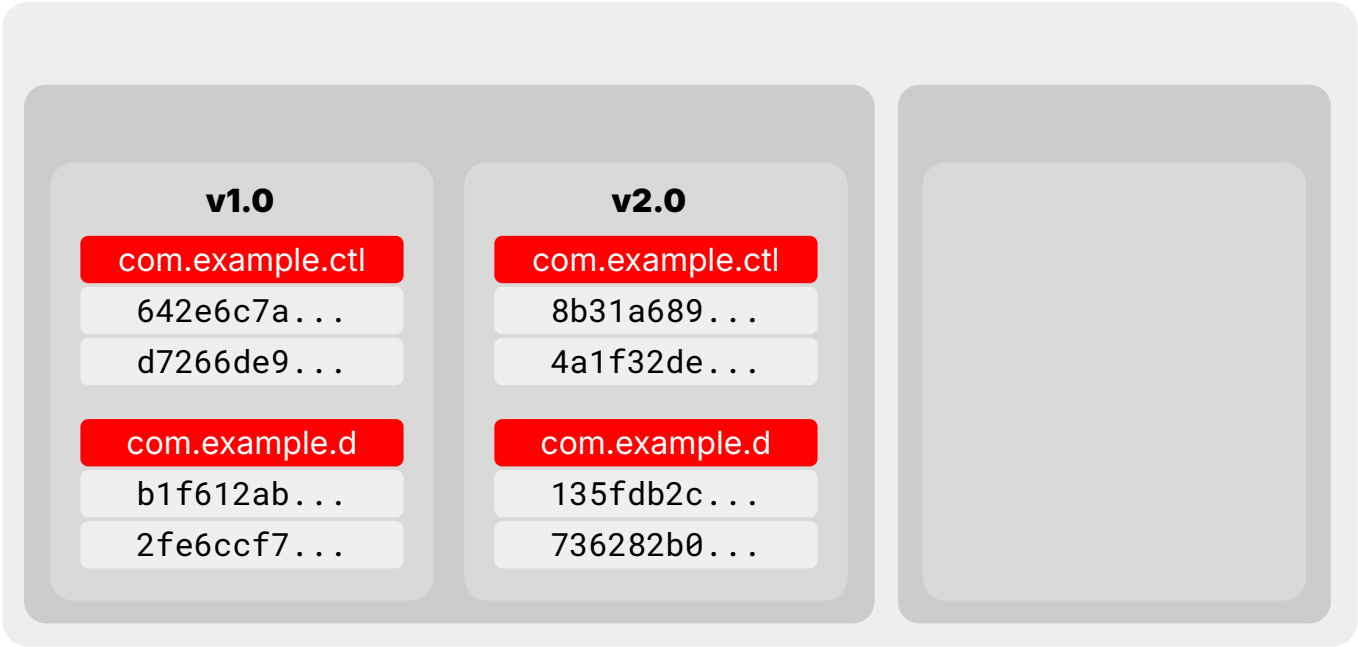
CDHash · Binary Hash · Signing ID · Cert Hash · Team ID · Path Regex

Rule Types and Precedence

Rule Types and Precedence

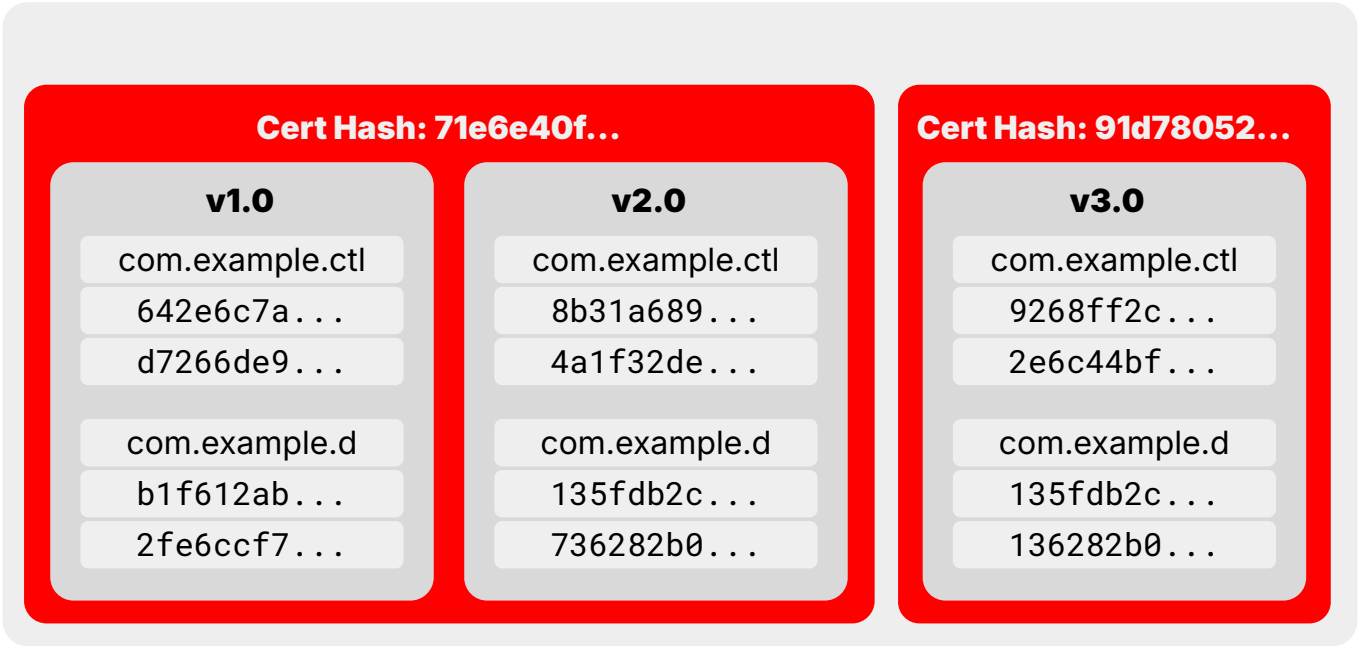


Rule Types and Precedence



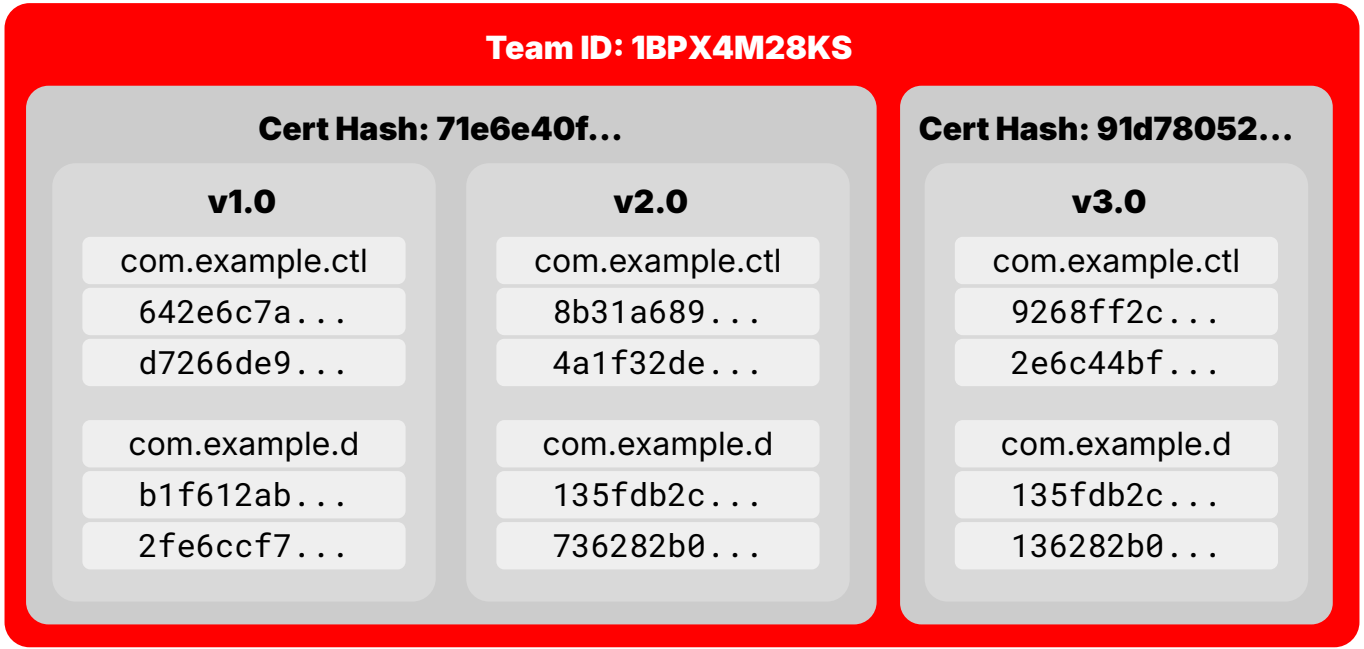
CDHash · Binary Hash · **Signing ID** · Cert Hash · Team ID · Path Regex

Rule Types and Precedence



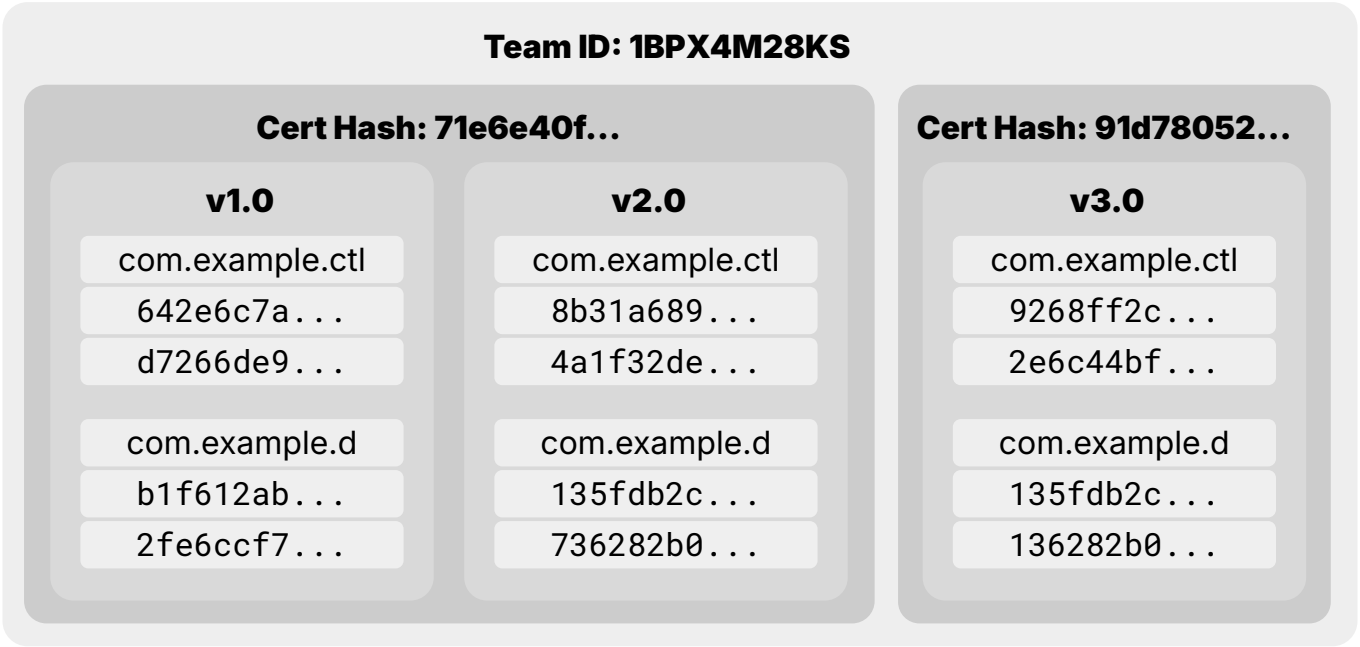
CDHash · Binary Hash · Signing ID · **Cert Hash** · Team ID · Path Regex

Rule Types and Precedence



CDHash · Binary Hash · Signing ID · Cert Hash · **Team ID** · Path Regex

Rule Types and Precedence

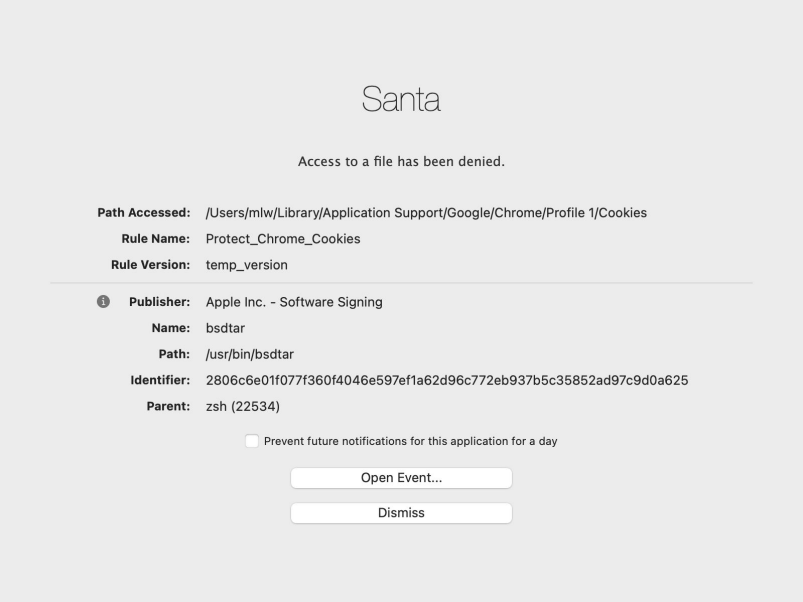


CDHash | Binary Hash | Signing ID | Cert Hash | Team ID | **Path Regex**

Rule Types and Precedence

- `santactl rule --allow --teamid --identifier EXAMPLETID`
- ```
  santactl rule --block \
                --signingid \
                --identifier EXAMPLETID:com.example.cloud-storage
  ```
  ```

File Access Authorization (FAA)

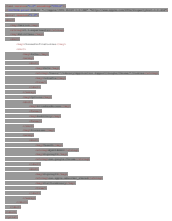


- Evaluate all file access attempts against policy
- Required OS changes (thanks Apple!)
- Rich policy options
  - Docs on northpole.dev

FAA Policy Example

```
<plist version="1.0">
<dict>
   <key>Version</key>
   <string>v0.1-experimental</string>
   <key>WatchItems</key>
   <dict>
      ...
   </dict>
</dict>
</plist>
```

FAA Policy Example



```
<key>ChromeProfileCookies</key>
<dict>
     ...
</dict>
```

FAA Policy Example

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

FAA Policy Example

```
<key>Options</key>
<dict>
    <key>AllowReadAccess</key>
    <false/>
    <key>AuditOnly</key>
    <false/>
</dict>
```

FAA Policy Example

```
<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.mdworker_shared</string>
        <key>PlatformBinary</key>
        <true/>
    </dict>
</array>
```

"Tripwire" FAA Rules

Watch / Lockdown cred files
Bearer tokens, browser cookies, honey tokens

Watch / Lockdown config modifications
SSH authorized_keys files, sudoers, pam

Rich configurations for defining exceptions

Ghost Of Santa Present

Telemetry

NORTH POLE SECURITY

Events

- Process lifecycle
- File operations
- Process meta events
- Mounts
- User space events
  - User Login Events

Logging Enhancements

File & Syslog

```
[2024-09-14T01:29:58.820Z] I santad:
action=EXEC|decision=ALLOW|reason=BINARY|explain=critical system
binary|sha256=4e10cd6f…|cert_sha256=d84db96a…|cert_cn=Software
Signing|pid=18909|pidversion=304830|ppid=1|uid=0|user=root|gid=0|
group=wheel|mode=M|path=/usr/libexec/xpcproxy|args=xpcproxy
com.google.santa.syncservice
```

Logging Enhancements

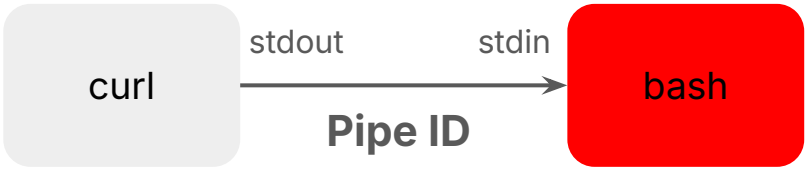
Protobuf & JSON


```
{"event_time":"2024-09-27T00:57:03.054743778Z","processed_time":"2024-09-27T00:57:03.096101Z","execution":{"instigator":{"id":{"pid":7994,"pidversion":436479},"parent_id":{"pid":57102,"pidversion":284557},"original_parent_pid":57102,"group_
id":7994,"session_id":28399,"effective_user":{"uid":501,"name":"peterm"},"effective_group":{"gid":20,"name":"staff"},"real_user":{"uid":501,"name":"peterm"},"real_group":{"gid":20,"name":"staff"},"executable":{"path":"/bin/zsh","truncated":
false}},"target":{"id":{"pid":7994,"pidversion":436480},"parent_id":{"pid":57102,"pidversion":284557},"responsible_id":{"pid":2365,"pidversion":6391},"original_parent_pid":57102,"group_id":7994,"session_id":28399,"effective_user":{"uid":501
,"name":"peterm"},"effective_group":{"gid":20,"name":"staff"},"real_user":{"uid":501,"name":"peterm"},"real_group":{"gid":20,"name":"staff"},"is_platform_binary":true,"is_es_client":false,"code_signature":{"cdhash":"1EZGz93Itz42b0XPw7GOZ/Fe
i/g=","signing_id":"com.apple.osascript"},"cs_flags":570509825,"executable":{"path":"/usr/bin/osascript","truncated":false,"stat":{"dev":16777229,"mode":33261,"nlink":1,"ino":"1152921500312492734","user":{"uid":0,"name":"root"},"group":{"gi
d":0,"name":"wheel"},"rdev":0,"access_time":"2024-09-05T20:54:17Z","modification_time":"2024-09-05T20:54:17Z","change_time":"2024-09-05T20:54:17Z","birth_time":"2024-09-05T20:54:17Z","size":"175776","blocks":"72","blksize":4096,"flags":5243
20,"gen":0},"hash":{"type":"HASH_ALGO_SHA256","hash":"f5527d70d8f2666dbe4e856c41a94fdb88102b406893d486c4ef731772a187c6"}},"tty":{"path":"/dev/ttys005","truncated":false},"start_time":"2024-09-27T00:57:03.049288Z"},"working_directory":{"path
":"/private/var/db/santa","truncated":false,"stat":{"dev":16777229,"mode":16877,"nlink":21,"ino":"14878140","user":{"uid":0,"name":"root"},"group":{"gid":0,"name":"wheel"},"rdev":0,"access_time":"2024-09-27T00:56:06.676415236Z","modificatio
n_time":"2024-09-27T00:30:14.966649278Z","change_time":"2024-09-27T00:30:14.966649278Z","birth_time":"2023-10-07T00:07:28.968760732Z","size":"672","blocks":"0","blksize":4096,"flags":0,"gen":0}},"args":["b3Nhc2NyaXB0"],"envs":["VEVSTV9QUk9H
UkFNPUFwcGxlX1Rlcm1pbmFs","U0hFTEw9L2Jpbi96c2g=","VEVSTT14dGVybS0yNTZjb2xvcg==","VE1QRElSPS92YXIvZm9sZGVycy9tcC9saHF5ZDZoZDdzNzVoX21maGxzdjJna3cwMDAwZ24vVC8=","VEVSTV9QUk9HUkFNX1ZFUlNJT049NDU0LjE=","VEVSTV9TRVNTSU9OX01EPUFEOEUzRUQ1LURERjYtN
EZBNy04OTZCLUQzNzlDQUIwODJCNQ==","VVNFUj1wZXRlcm0=","U1NIX0FVVEhfU09DSz0vcHJpdmF0ZS90bXAvY29tLmFwcGxlLmxhdW5jaGQucGdKV055MEhaOS9MaXN0ZW5lcnM=","UEFUSD0vVXNlcnMvcGV0ZXJtLy5nZW0vcnVieS8zLjMuNS9iaW46L1VzZXJzL3BldGVybS8ucnViaWVzL3J1YnktMy4zLjUv
bGliL3J1YnkvZ2Vtcy8zLjMuMC9iaW46L1VzZXJzL3BldGVybS8ucnViaWVzL3J1YnktMy4zLjUvYmluOi9vcHQvaG9tZWJyZXcvYmluOi9vcHQvaG9tZWJyZXcvc2JpbjovdXNyL2xvY2FsL2dvL2JpbjovTGlicmFyeS9GcmFtZXdvcmtzL1B5dGhvbi5mcmFtZXdvcmsvVmVyc2lvbnMvMy40L2JpbjovdXNyL2xvY2FsL2JpbjovdXNyL2xvY2FsL01hY0dQRzIvYmluOi9vc2Vycy9wZXRlcm0vYmluOi9c3IvbG9jYWwvQ2VsbGFyL2xsdm0vMy41LjAvYmluOi9vc2Vycy9wZXRlcm0vc2F0L2Jpbjovb3B0L2phaWxicmVha3Rvb2xzLzovVXNlcnMvcGV0ZXJt","T
GF1bmNoSW5zdGFuY2VJRD1CRkEyRUIyMi0xNjI1LTQwNDItQTMyQi00MERCNTYwNjFGRkY=","X19DRkJ1bmRsZUlkZW50aWZpZXI9Y29tLmFwcGxlLlRlcm1pbmFs","UFdEPS92YXIvZGIvc2FudGE=","WFBDX0ZMQUdTPTB4MA==","WFBDX1NFU1ZJQ0VfTkFNRT0w","U0hMVkw9Mg==","SE9NRT0vVXNlcnMvcGV
0ZXJt","TE9HTkFNRT1wZXRlcm0=","U0VDVVJJVFlTRVNTSU9OSUQ9MTg2YWI=","T0xEUFdEPS9Vc2Vycy9wZXRlcm0vc3JjL3NhbnRh","SE9NRUJSRVdfUFJFRklYPS9vcHQvaG9tZWJyZXc=","SE9NRUJSRVdfQ0VMTEFSPS9vcHQvaG9tZWJyZXcvQ2VsbGFy","SE9NRUJSRVdfUkVQT1NJVE9SWT0vb3B0L2hvb
WVicmV3","SU5GT1BBVEg9L29wdC9ob21lYnJldy9zaGFyZS9pbmZvOi9vcHQvaG9tZWJyZXcvc2hhcmUvaW5mb3B0L2hvbWVicmV3L3NoYXJlL2luZm86","R09QQVRIPS9Vc2Vycy9wZXRlcm0vc3JjL2dvX3dvcmtzcGFjZQ==","RURJVE9SPXZpbQ==","UEFHRVI9bGVzcw==","SE9TVD1yYWdnZWQ=","SE9
NRUJSRVdfTk9fQU5BTFlUSUNTPTE=","RU5WPWJsaXR6ZW4udGVjaA==","UlVCWV9ST09UPS9Vc2Vycy9wZXRlcm0vLnJ1Ymllcy9ydWJ5LTMuMy41","UlVCWU9QVD0=","UlVCWV9FTkdJTkU9cnVieQ==","UlVCWV9WRVJTSU9OPTMuMy41","R0VNX1JPT1Q9L1VzZXJzL3BldGVybS8ucnViaWVzL3J1YnktMy4zLj
UvbGliL3J1YnkvZ2Vtcy8zLjMuMA==","R0VNX0hPTUU9L1VzZXJzL3BldGVybS8uZ2VtL3J1YnkvMy4zLjU=","R0VNX1BBVEg9L1VzZXJzL3BldGVybS8uZ2VtL3J1YnkvMy4zLjU6L1VzZXJzL3BldGVybS8ucnViaWVzL3J1YnktMy4zLjUvbGliL3J1YnkvZ2Vtcy8zLjMuMA==","TEFORz1lbl9VUy5VVEYtOA==
","Xz0vdXNyL2Jpbi9vc2FzY3JpcHQ="],"fds":[{"fd":0,"fd_type":"FD_TYPE_VNODE"},{"fd":1,"fd_type":"FD_TYPE_VNODE"},{"fd":2,"fd_type":"FD_TYPE_VNODE"}],"fd_list_truncated":false,"decision":"DECISION_DENY","reason":"REASON_SIGNING_ID","mode":"MOD
E_MONITOR","certificate_info":{"hash":{"type":"HASH_ALGO_SHA256","hash":"d84db96af8c2e60ac4c851a21ec460f6f84e0235beb17d24a78712b9b021ed57"},"common_name":"Software
Signing"},"entitlement_info":{"entitlements_filtered":false,"entitlements":[{"key":"com.apple.developer.notificationcenter-identifiers","value":"[\"com.apple.ScriptEditor2\"]"},{"key":"com.apple.private.tcc.allow-prompting","value":"[\"kTCC
ServiceAll\"]"}]}}}
```

Powerful Detection Primitives

Examples

- Process grouping (group/session IDs)
- Usernames
- Process args & environment vars
- setuid
- File descriptor info
- Mount remote address
- Events tied to user activity
- Entitlements



Use Case: Infostealers

1

Initial Access

T1566.001:
Phishing: Spearphishing Attachment

The malware cannot run until the risk engine and other users approve it

2

Persistence

T1543.004:
Create or Modify System Process: Launch Daemon

T1543.001:
Create or Modify System Process: Launch Agent

Santa's file access authorization prevents applications from installing LaunchDaemons or LaunchAgents.

Social voting also prevents any second stage malware from executing

3

Lateral Movement

T1552.004:
Unsecured Credentials: Private Keys

4

Data Exfiltration

T1539:
Steal Web Session Cookie

Santa's file access authorization detects and prevents read access to sensitive credentials
Santa's telemetry records all process executions and configured file system operations

Ghost Of Santa Present

Integrations

Rule Level Customization

`custom_msg`

Lets you customize the message users see per rule

`custom_url`

Lets you control where the open button directs the user

Distributed Notifications

Published on blocked executions
Dictionary of event information

santa-dndump
https://github.com/northpolesec/santa-dndump

Distributed Notifications

Rule Configuration

Static rules
configure rules via MDM

Sync Service
via Sync Protocol

Command Line
rule command & JSON rule import/export

Ghost Of Santa Yet To Come

We're The Team That Made Santa Work At Google

Pete Markowsky
CEO
Led all first party security agent development at Google, including Santa

Russell Hancox
Founding Engineer
One of the two original authors of Santa

Tom Burgin
Founding Engineer
One of the two original authors of Santa

Matt White
Founding Engineer
Led Santa development

We Are Forking Santa!

Our Commitment

- Santa will stay open
- Remain compatible with the sync protocol
- Increased involvement with the community

Join us
github.com/northpolesec/santa

Standalone Santa (Beta)

Even More Presents To Come



Sooner

- Standalone Santa (Beta)
- Telemetry event filtering
- More telemetry events

Later

- Process-based FAA rules
- On demand monitor mode
- Process-Tree-Aware Rules
- Fast path exec authorization

Way Later

- File content checks
- USB blocking enhancements
- Complex policies
- Improved transitive allowlisting

Join Our Santa Community

github.com/northpolesec/santa

northpole.dev - docs

Mac Admins — #santa

Other discussions, issues, PRs, we're happy to help!

Thank You!

NORTH POLE SECURITY