More Value, Less work: Automating Security with Bit9 Platform

Tim Smith

Product Manager, Bit9 Platform

Bit9 + CARBON BLACK

ARM YOUR ENDPOINTS.

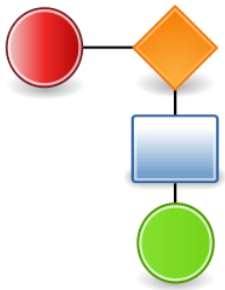
Today's Goals

1. Discuss the value of automation within Bit9

2. Look at automation use cases

3. Learn how it's done

The Value of Automation



Simplifies workflows

Reduces FTE Costs

Speeds Time-to-Value

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

Bit9 Automation – What's Possible

Value at all Enforcement Levels

- Stop and prevent malware execution
- System lockdown
- Analyze unknown and 'gray' files
- Process approval requests
- Drive security policy

Automate Banning of Malware

End-User Friction: *None*
Admin Effort: *None*

Challenge: ***Preexisting malware***

Bit9: ***Terminates running instances and blocks future executions***

Upon initialization
- Ban all existing files deemed Malicious by SRS
- Terminate running instances of these files
- Enable further investigation

Benefits
- Ensure sanitized environment
- Identify attacks already in progress
- Immediate time-to-value

Challenge: ***Newly-arriving malware***

Bit9: ***Blocks malware within moments of it arriving***

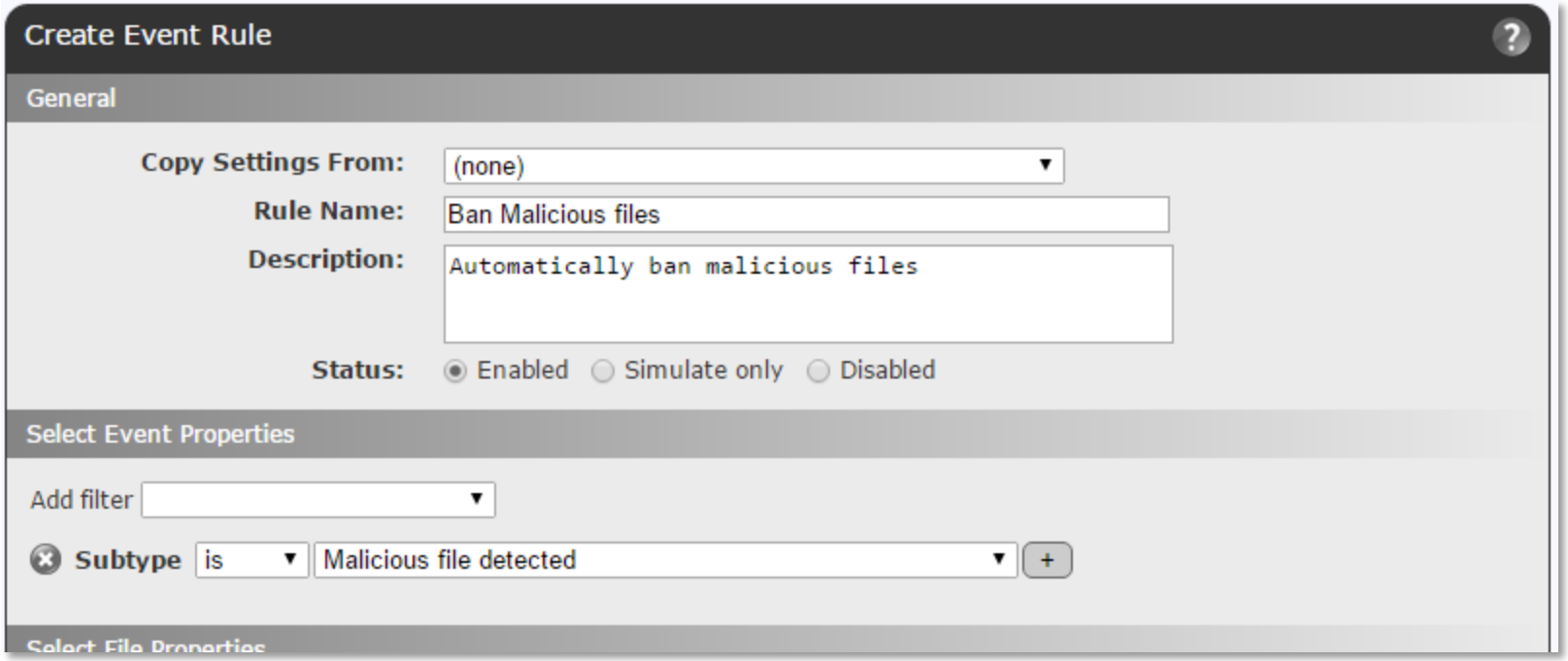
Upon arrival
- Ban newly arriving files deemed Malicious by SRS
- Terminate running instances of these file
- Enable further investigation

Benefits
- Provides rapid first-level of protection
- Unites multiple forms of detection (Sandbox, VT, SRS)
- Immediate time to value

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

How to Automatically Ban Malware

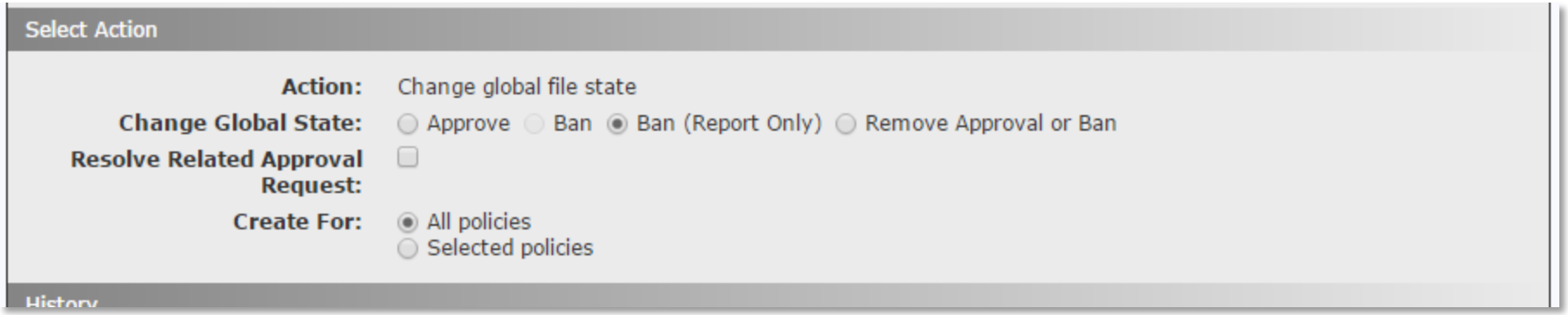
- Create a new Event rule based on “[Sample] Report Malicious files”
- Give the rule a new name like “Ban Malicious Files”
- Enable the Rule
- Keep the subtype as “Malicious file detected”



Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

How to Automatically Ban Malware

- Action remains “Change global file state”
- Alter “Change Global State” to “Ban.”

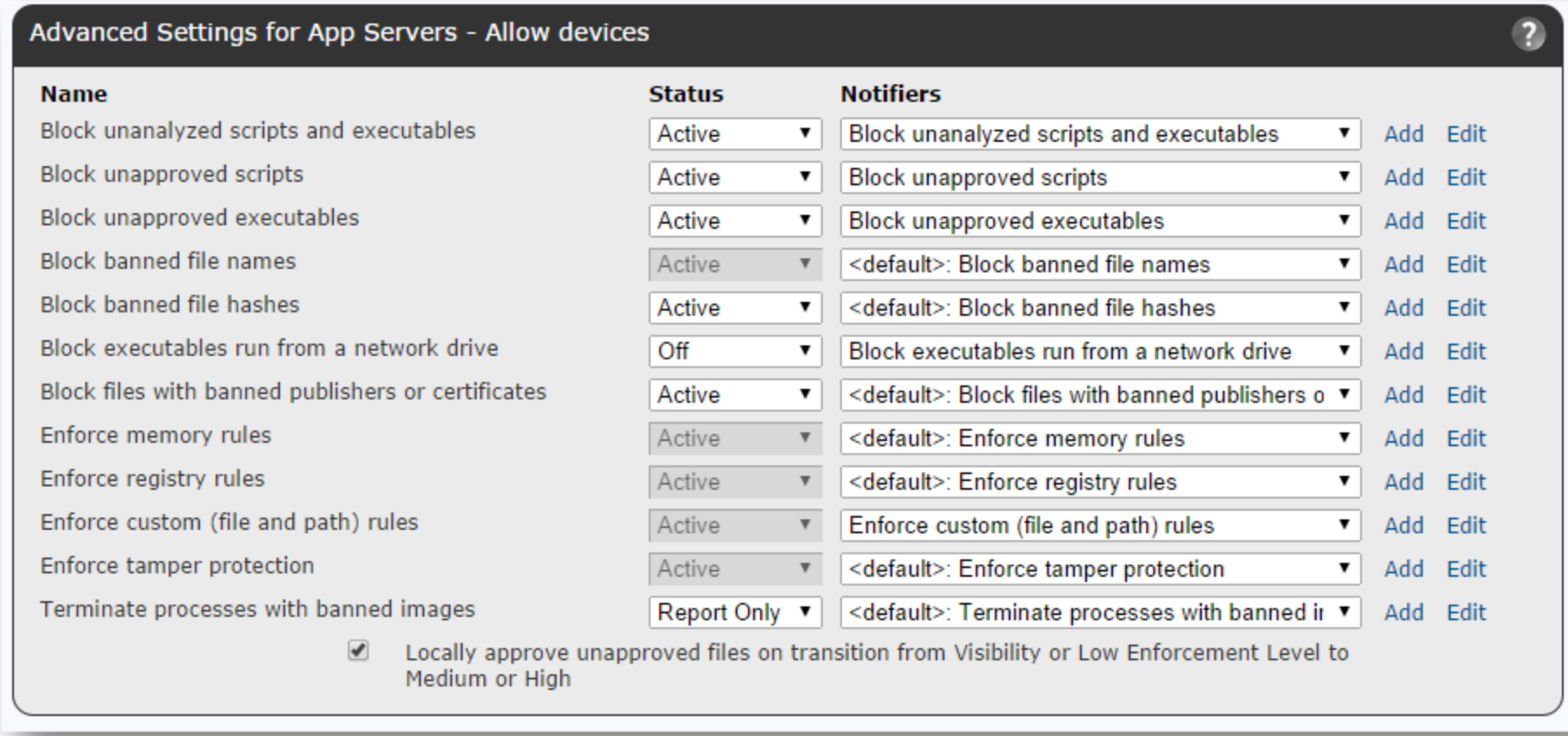


- Ban files via Event Rules is not enabled out of the box
- Go to shepherd_config.php to enable
  - Define property AllowBansFromEventRules
  - Set value to true

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

How to Automatically Ban Malware

- **Edit each policy and click the Advanced tab. Under "Terminate processes with banned images" change that to Active if it is not already.**



Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

Automating File Analysis

Challenge: Determining risk and status of files

Bit9: Multiple options:

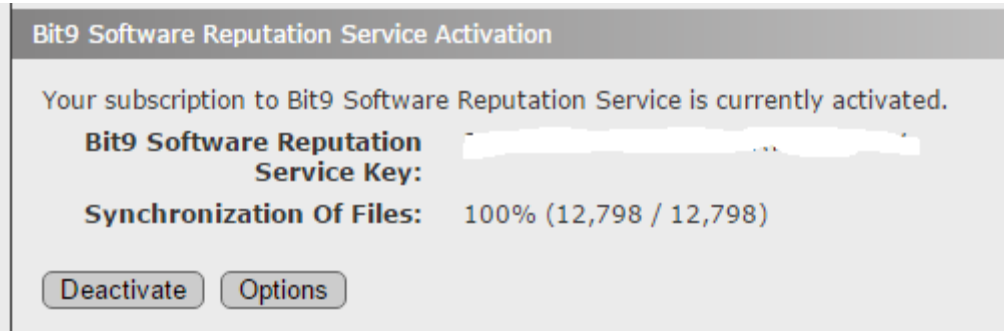
1) ***File hashes unknown to SRS can be passed to VirusTotal – opt in***
2) ***Bit9 can upload and submit files to any 3rd-party for binary analysis***

- **File arrives on endpoint**
  - SRS reputation is not conclusive or is unknown
  - Unknown hashes can automatically be submitted to VirusTotal

  and
  - Bit9 can submit files to 3rd-party 'detonation' solution
  - Result can drive automated response – approval, ban, system lockdown

How to Enable VirusTotal File Hash Lookup

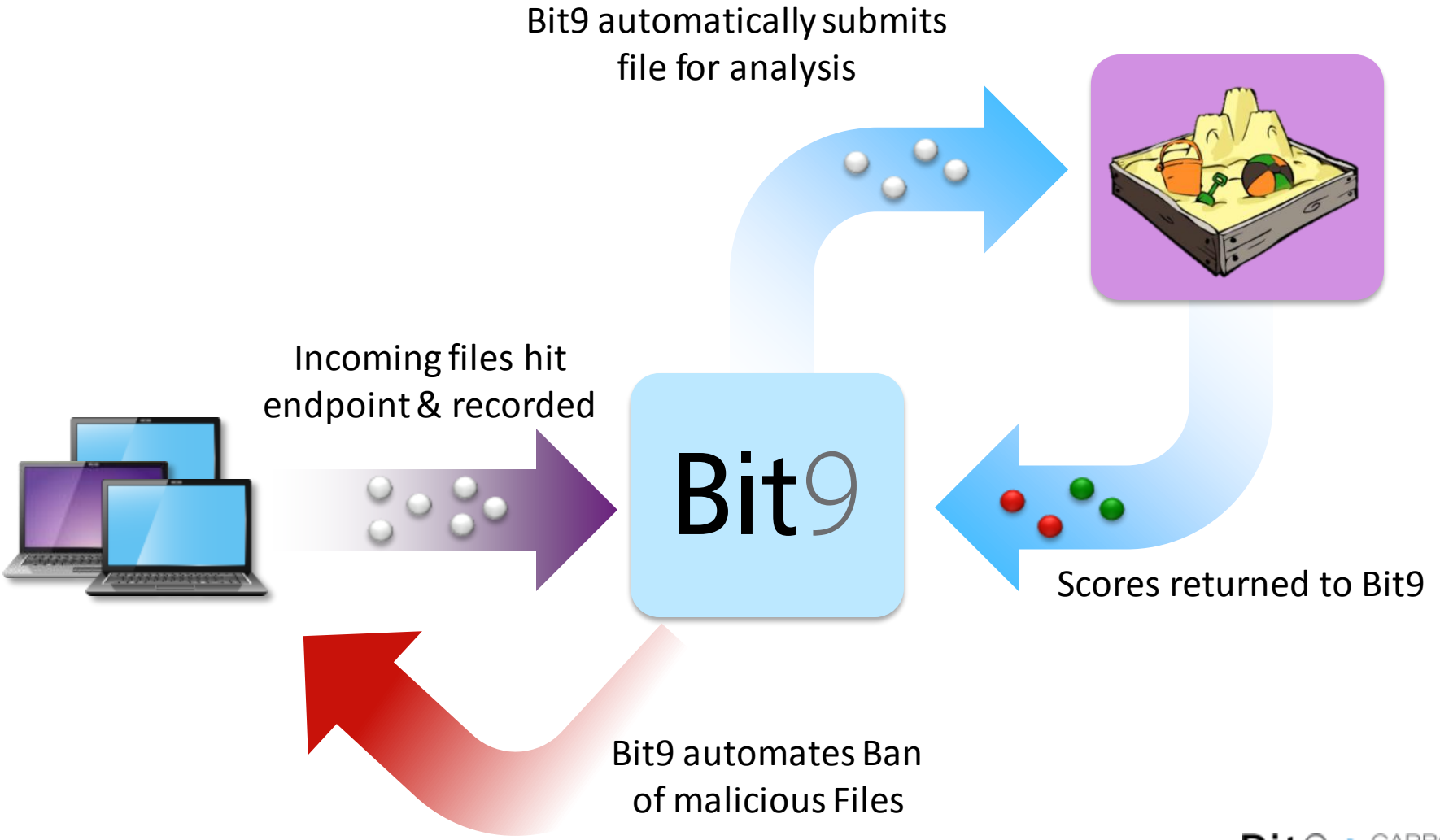
- From the System Configuration page, select the Licensing tab, and hit the SRS Options button.



- When the SRS webpage opens, make sure “Enable VirusTotal Lookup” is checked.

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

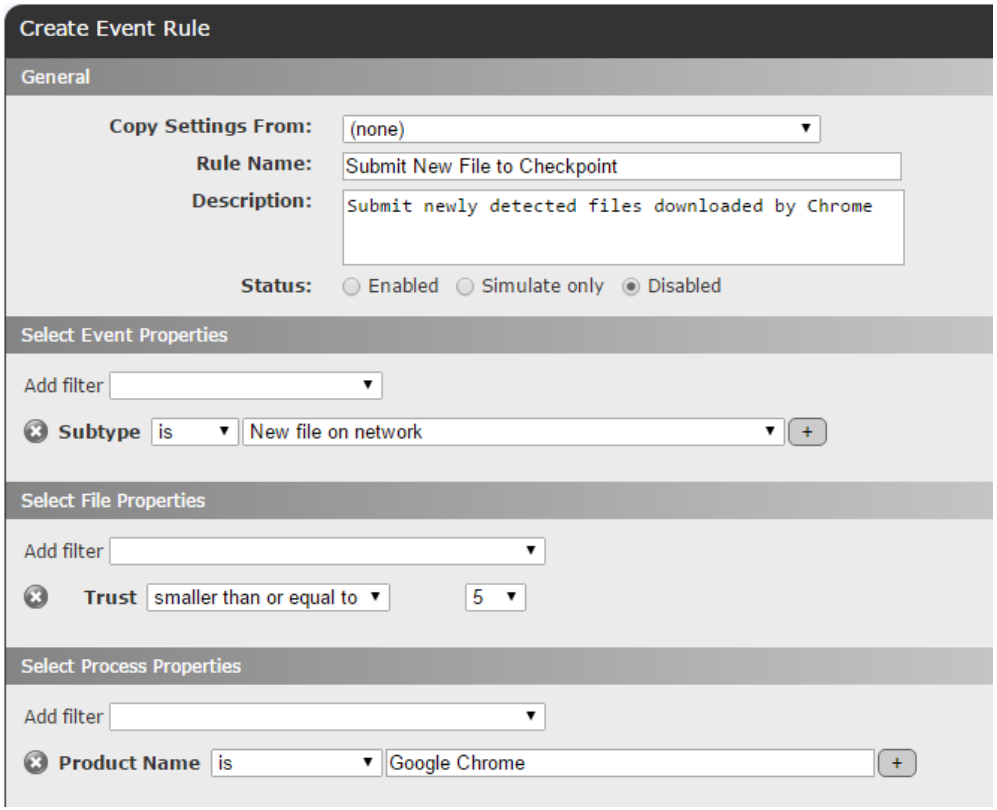
Automating Bans off File Analysis



Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

How to Submit Files to 3rd Parties

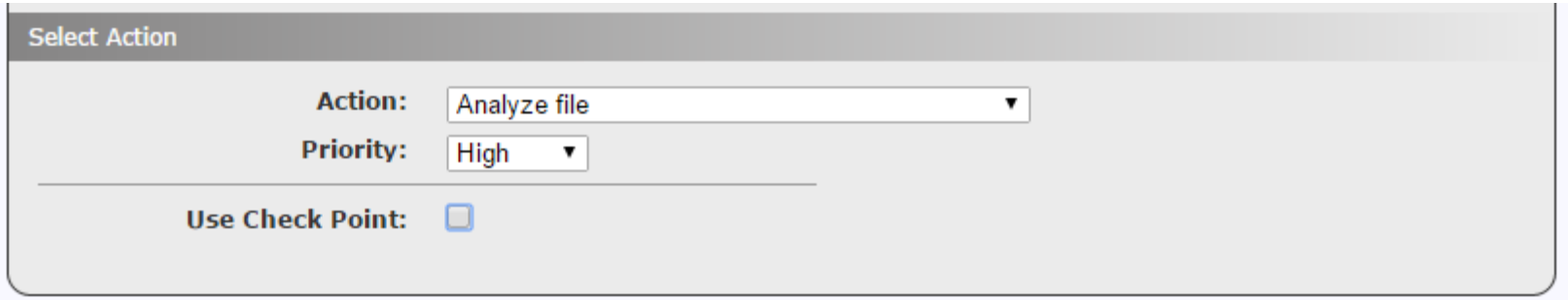
- Create a new Event rule called “Submit New File to …” and the name of your 3rd party detonation service.
- Event Properties: Subtype = “New File on Network”
- File Properties: Trust <= 5
- Could also add the process that generated the file like Chrome



Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

How to Submit Files to 3rd Parties

- Action = Analyze File
- When selected, parameters for configured Connectors appear.



Using your existing malware ban Event rule, newly analyzed malicious files will be banned.

Automating Approval Request Management

Challenge: ***Limited resources to manage Bit9 in High Enforcement***

Bit9: ***Automates management of user requests for file approvals***

Upon receipt of Approval Request

- Approve/ban the file based on reputation
- Have files analyzed then approve/ban based on verdict
- Close the request – notify the user of the response

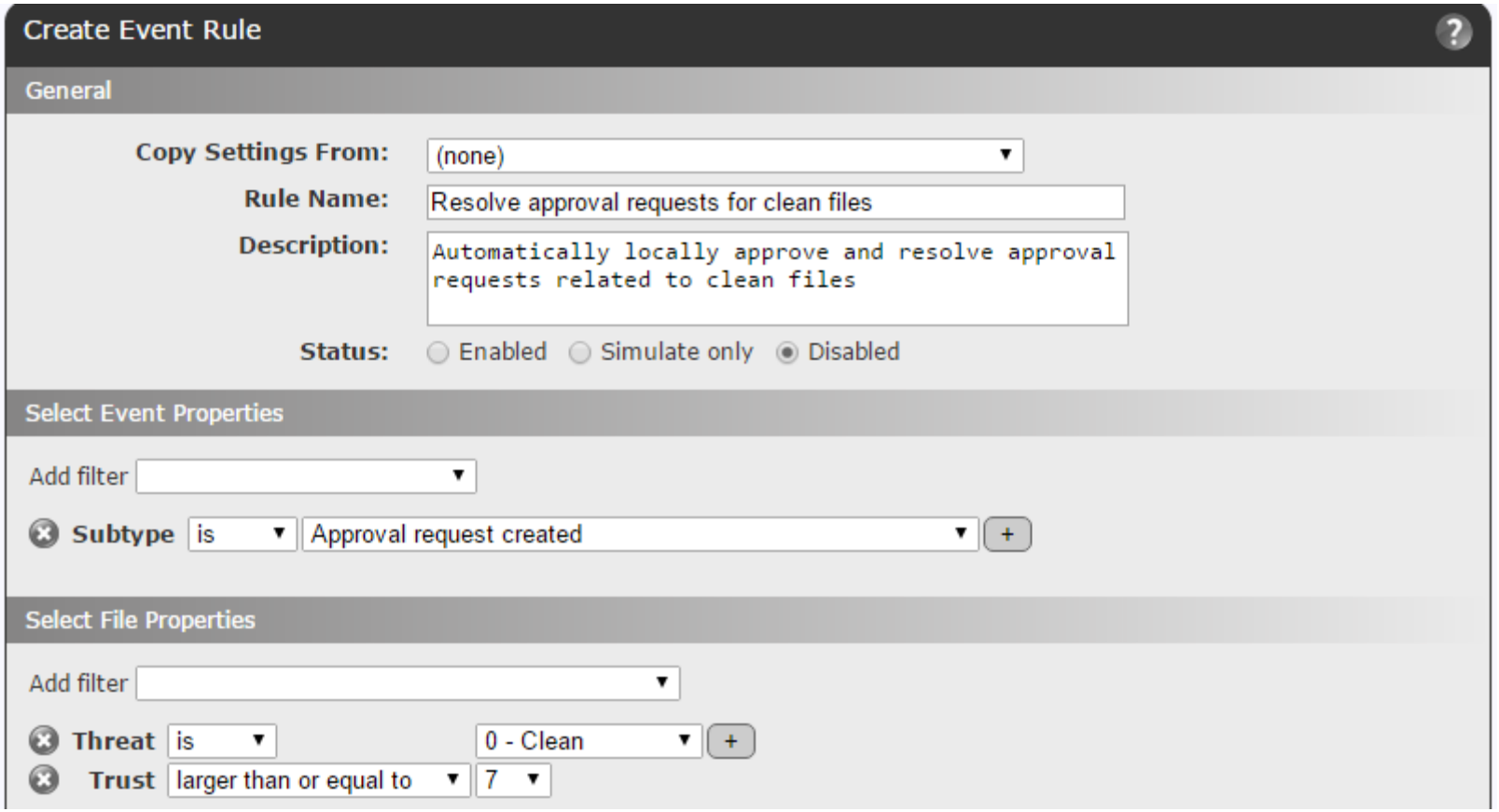
Benefits

- Reduced administrative costs
- Simplifies High Enforcement
- Quicker response

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

How to Automate Approval Requests

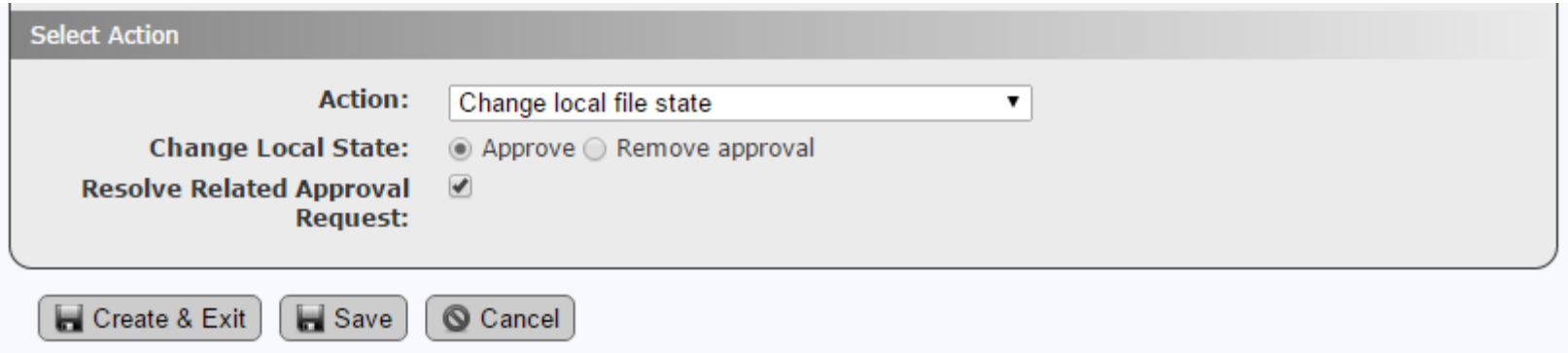
- **Event Properties: Subtype = “Approval request created”**
- **File Properties: Trust = “0 – Clean” and Trust >= 7**



Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

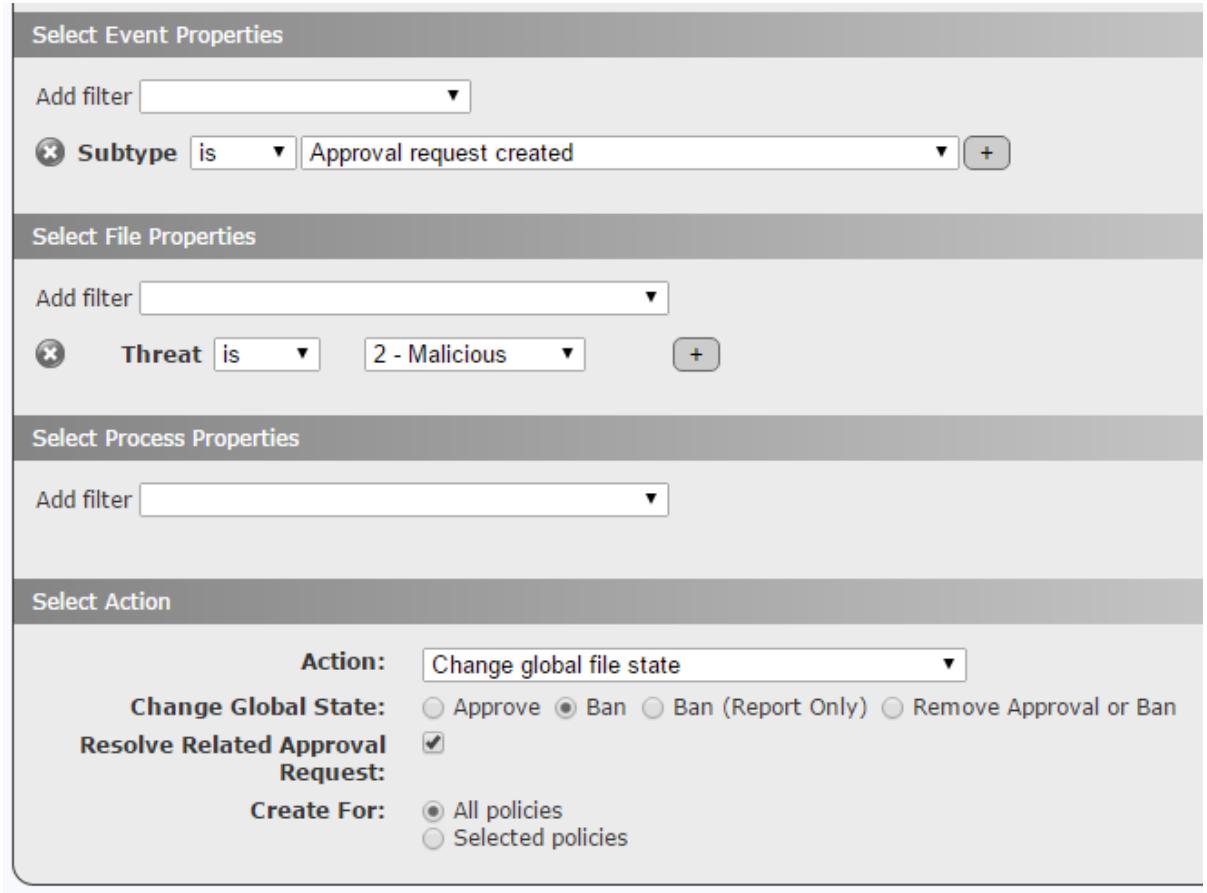
How to Automate Approval Requests

- Action: Change local file state
- Change Local State: Approve
- Resolve Related Approval Request: Checked



How to Automate Approval Requests - Bans

- Action: Change global file state
- Change Local State: Ban
- Resolve Related Approval Request: Checked



Automating System Lockdown

Challenge: Company has very open culture but wants to secure the system when suspicious activity is encountered

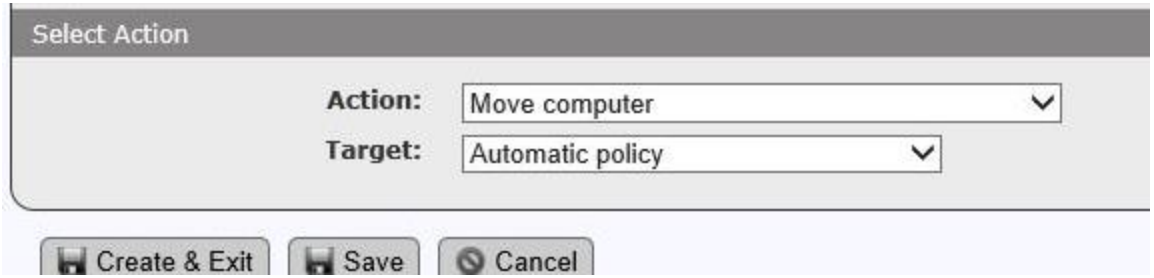
Bit9: Run in Low Enforcement, move systems to High Enforcement when suspicious activity occurs

- **Triggers**
  - Malicious file identified
    - SRS
    - Connectors
    - MS SCEP
  - API-based integration triggering some event
  - Cb Watchlists
- **Immediately protect the system**
- **Allows investigation and remediation of the event**
- **Once resolved, move back to Low Enforcement**

Bit9 + CARBON BLACK
ARM YOUR ENDPOINTS.

How to Automate System Lockdown

- Create a new Event rule using whatever Event Properties you want, like “Subtype is Malicious File Detected.”
- Make the Action: Move Computer
- Set Target to your high enforcement policy



- Move Computer via Event Rules is not enabled out of the box
- Go to shepherd_config.php to enable
  - Define property AllowMoveComputerFromEventRules
  - Set value to true

Combining Use Cases

New file arrives on endpoint

1. **Submit file for analysis - to one or more 'detonation' solutions**
2. **Ban and terminate the file based on analysis results, or a combination of results**
3. **Change endpoint policy to lockdown**
4. **Upload file for further analysis**

Key Takeaways

Bit9 offers high value in any enforcement level

Bit9 can deliver high value on day 1

Bit9 automation greatly reduces admin effort

Bit9 delivers high value on all endpoints

This is possible today on Bit9 7.2.0 and later

Questions?

Bit9 + CARBON BLACK

ARM YOUR ENDPOINTS.