

More Value, Less work: Automating Security with Bit9 Platform

Tim Smith

Product Manager, Bit9 Platform

Today's Goals

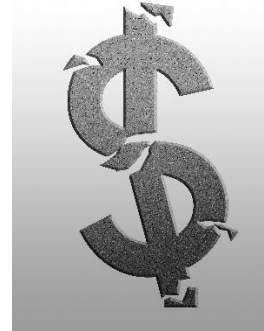
1. Discuss the value of automation within Bit9
2. Look at automation use cases
3. Learn how it's done



The Value of Automation



Simplifies workflows



Reduces FTE Costs



Speeds Time-to-Value

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

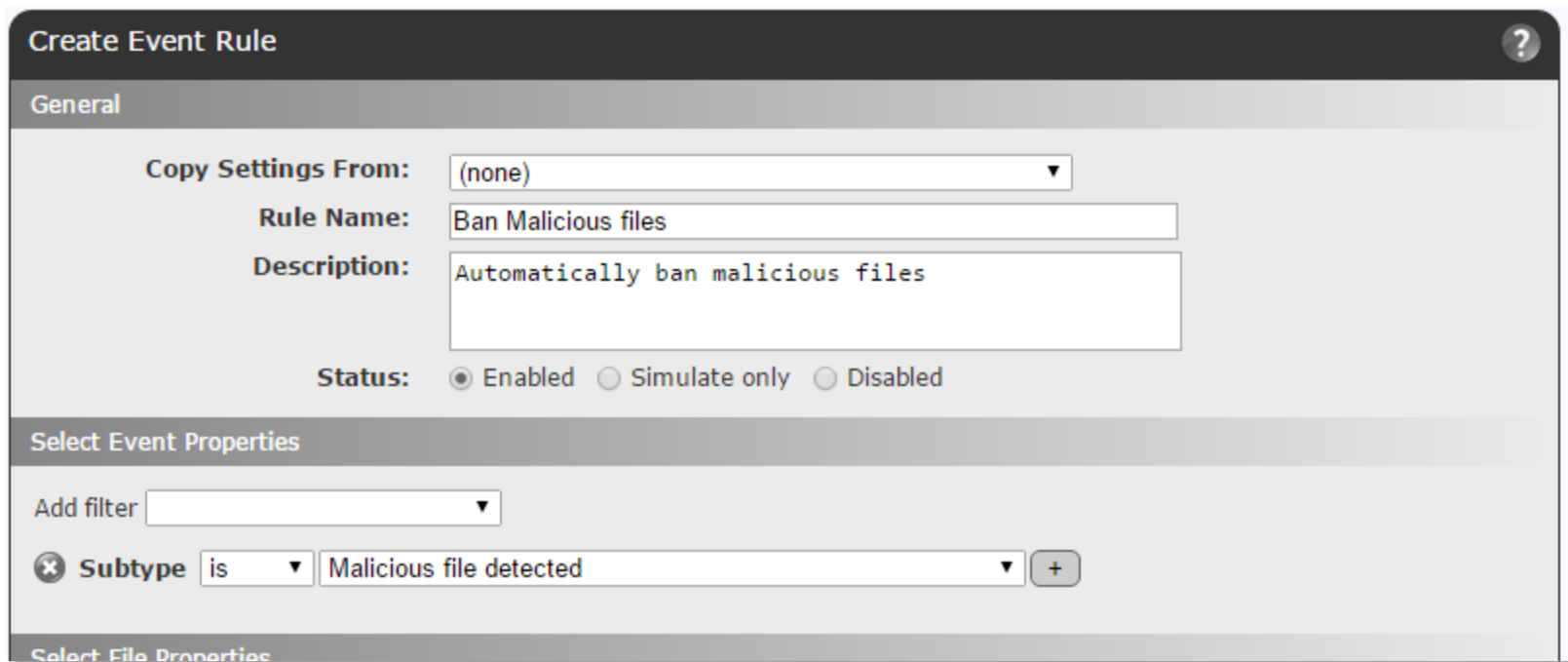
- Ban newly arriving files deemed Malicious by SRS
- Terminate running instances of these file
- Enable further investigation

Benefits

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

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”



The screenshot shows a 'Create Event Rule' dialog box with the following fields and options:

- Copy Settings From:** (none) [dropdown]
- Rule Name:** Ban Malicious files [text input]
- Description:** Automatically ban malicious files [text input]
- Status:** Enabled Simulate only Disabled
- Select Event Properties:**
 - Add filter [dropdown]
 - Subtype is [dropdown] Malicious file detected [dropdown] [add button]
- Select File Properties:** [header]

How to Automatically Ban Malware

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



The screenshot shows a dialog box titled "Select Action" with a "History" tab at the bottom. The dialog contains the following options:

- Action:** Change global file state
- Change Global State:** Approve Ban Ban (Report Only) Remove Approval or Ban
- Resolve Related Approval Request:**
- Create For:** All policies Selected policies

- ◆ 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

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.

Advanced Settings for App Servers - Allow devices ?

Name	Status	Notifiers		
Block unanalyzed scripts and executables	Active ▼	Block unanalyzed scripts and executables ▼	Add	Edit
Block unapproved scripts	Active ▼	Block unapproved scripts ▼	Add	Edit
Block unapproved executables	Active ▼	Block unapproved executables ▼	Add	Edit
Block banned file names	Active ▼	<default>: Block banned file names ▼	Add	Edit
Block banned file hashes	Active ▼	<default>: Block banned file hashes ▼	Add	Edit
Block executables run from a network drive	Off ▼	Block executables run from a network drive ▼	Add	Edit
Block files with banned publishers or certificates	Active ▼	<default>: Block files with banned publishers o ▼	Add	Edit
Enforce memory rules	Active ▼	<default>: Enforce memory rules ▼	Add	Edit
Enforce registry rules	Active ▼	<default>: Enforce registry rules ▼	Add	Edit
Enforce custom (file and path) rules	Active ▼	Enforce custom (file and path) rules ▼	Add	Edit
Enforce tamper protection	Active ▼	<default>: Enforce tamper protection ▼	Add	Edit
Terminate processes with banned images	Report Only ▼	<default>: Terminate processes with banned ir ▼	Add	Edit

Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High

Automating File Analysis

Challenge: Determining risk and status of files

Bit9: Multiple options:

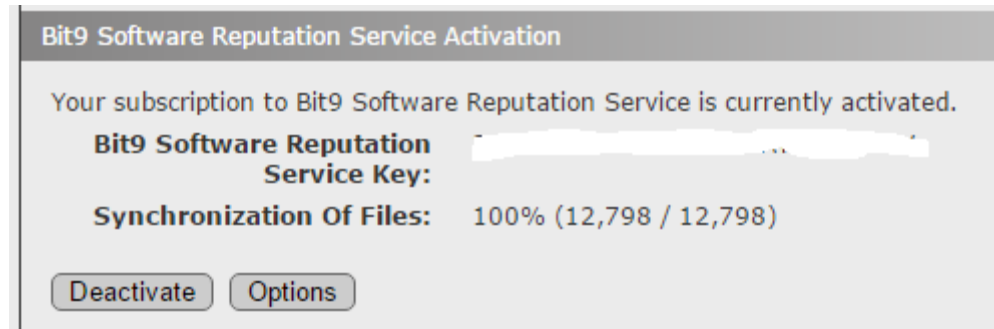
- 1) File hashes unknown to SRS can be passed to VirusTotal – opt in***
- 2) Bit9 can upload and submit files to any 3rd-party for binary analysis***

◆ 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

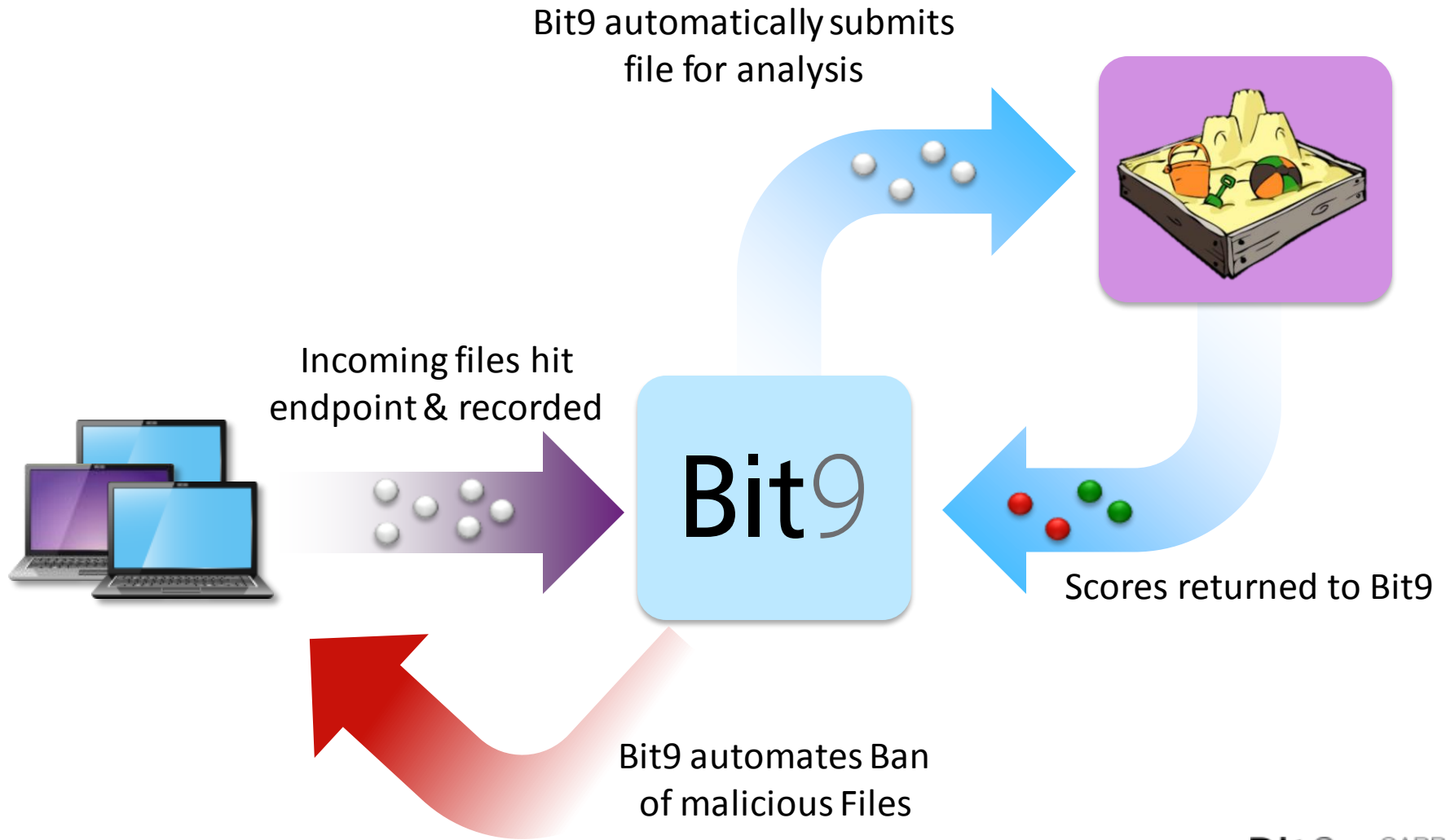
- ◆ From the System Configuration page, select the Licensing tab, and hit the SRS Options button.



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

- Enable VirusTotal lookup
New hashes (but not the files themselves) are sent to VirusTotal for reputation lookup.

Automating Bans off File Analysis



How to Submit Files to 3rd Parties

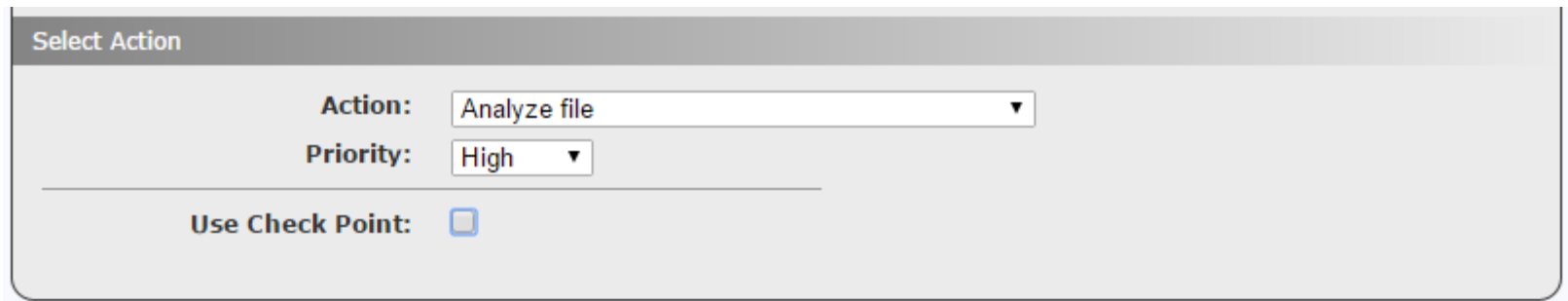
- ◆ Create a new Event rule called “Submit New File to ...” and the name of your 3rd party detonation service.
- ◆ Event Properties: Subtype = “New File on Network”
- ◆ File Properties: Trust <= 5
- ◆ Could also add the process that generated the file like Chrome

The screenshot displays the 'Create Event Rule' configuration window, organized into four main sections:

- General:** Includes a 'Copy Settings From' dropdown set to '(none)', a 'Rule Name' field containing 'Submit New File to Checkpoint', and a 'Description' field containing 'Submit newly detected files downloaded by Chrome'. The 'Status' is set to 'Disabled'.
- Select Event Properties:** Features an 'Add filter' dropdown and a filter rule: 'Subtype is New file on network'.
- Select File Properties:** Features an 'Add filter' dropdown and a filter rule: 'Trust smaller than or equal to 5'.
- Select Process Properties:** Features an 'Add filter' dropdown and a filter rule: 'Product Name is Google Chrome'.

How to Submit Files to 3rd Parties

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



The screenshot shows a configuration window titled "Select Action". It contains the following fields:

- Action:** A dropdown menu with "Analyze file" selected.
- Priority:** A dropdown menu with "High" selected.
- Use Check Point:** An unchecked checkbox.

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

How to Automate Approval Requests

- ◆ Event Properties: Subtype = “Approval request created”
- ◆ File Properties: Trust = “0 – Clean” and Trust \geq 7

Create Event Rule

General

Copy Settings From: (none)

Rule Name: Resolve approval requests for clean files

Description: Automatically locally approve and resolve approval requests related to clean files

Status: Enabled Simulate only Disabled

Select Event Properties

Add filter

Subtype is Approval request created

Select File Properties

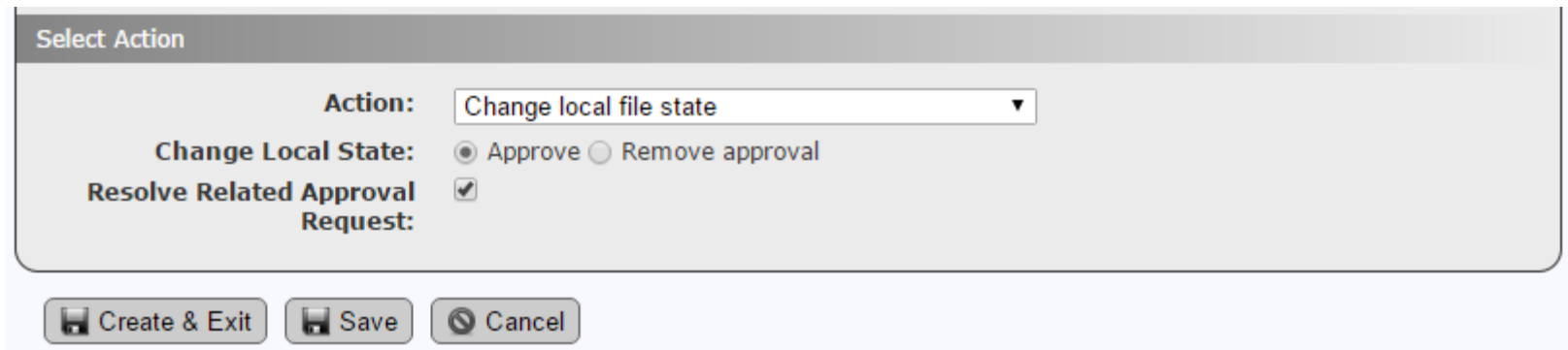
Add filter

Threat is 0 - Clean

Trust larger than or equal to 7

How to Automate Approval Requests

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



The screenshot shows a dialog box titled "Select Action" with the following configuration:

- Action:** Change local file state (selected in a dropdown menu)
- Change Local State:** Approve (selected radio button), Remove approval (unselected radio button)
- Resolve Related Approval Request:** Checked (checked checkbox)

At the bottom of the dialog, there are three buttons: "Create & Exit", "Save", and "Cancel".

How to Automate Approval Requests - Bans

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

The screenshot shows a configuration window with four main sections:

- Select Event Properties:** Contains an "Add filter" dropdown and a filter rule: **Subtype** is Approval request created.
- Select File Properties:** Contains an "Add filter" dropdown and a filter rule: **Threat** is 2 - Malicious.
- Select Process Properties:** Contains an "Add filter" dropdown.
- Select Action:** Contains the following settings:
 - Action:** Change global file state
 - Change Global State:** Radio buttons for Approve, Ban (selected), Ban (Report Only), and Remove Approval or Ban.
 - Resolve Related Approval Request:** Checked checkbox.
 - Create For:** Radio buttons for All policies (selected) and Selected policies.

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

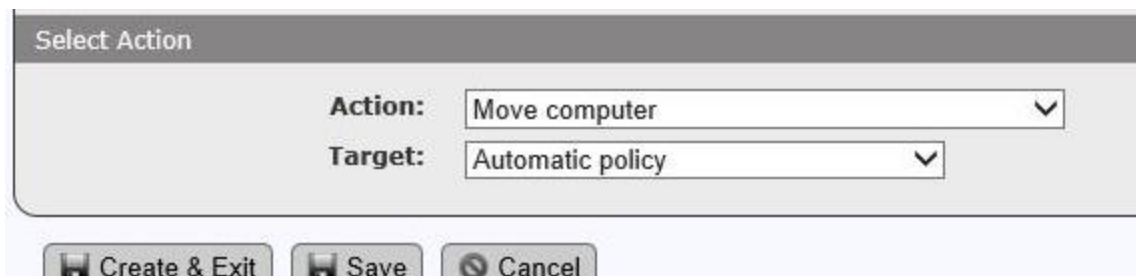
◆ Immediately protect the system

◆ Allows investigation and remediation of the event

◆ Once resolved, move back to Low Enforcement

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.