

THE BEDROCK OF CYBER SECURITY



Solutions Architect / Axonius

AGENDA

- 01 What is SOCI and Why?
- 02 Security Process Improvement
- 03 Maintaining Compliance
- 04 Security Process Automation
- 05 Questions?



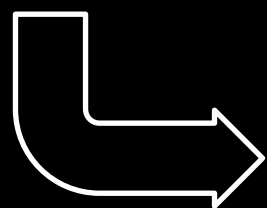
3 Object

The object of this Act is to provide a framework for managing risks relating to critical infrastructure, including by:

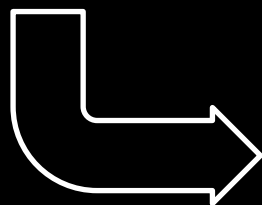
- (a) improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks; and
- (b) facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks; and
- (c) requiring responsible entities for critical infrastructure assets to identify and manage risks relating to those assets; and
- (d) imposing enhanced cyber security obligations on relevant entities for systems of national significance in order to improve their preparedness for, and ability to respond to, cyber security incidents; and
- (e) providing a regime for the Commonwealth to respond to serious cyber security incidents.



Security Process Compliance



Change of current process



**Business Process
Improvement**



Security Process Compliance

**SOCI is only ONE driver
for ~~Business~~ Security
Process Improvement**



1. Assess your current state
2. Define your future State
3. Define performance metrics
4. Identify and prioritise improvement
5. Create a process improvement plan



- Manual Audit
- Interview stakeholders
- Review individual processes
- **Data Mining Capability**



Integration with all existing tools

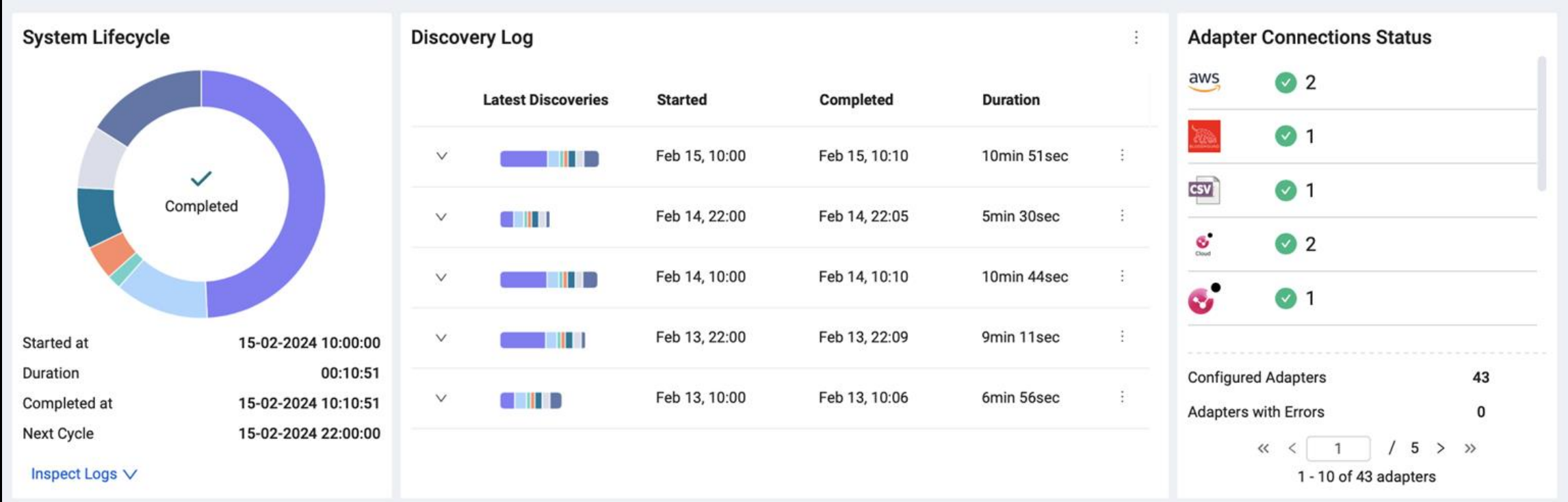


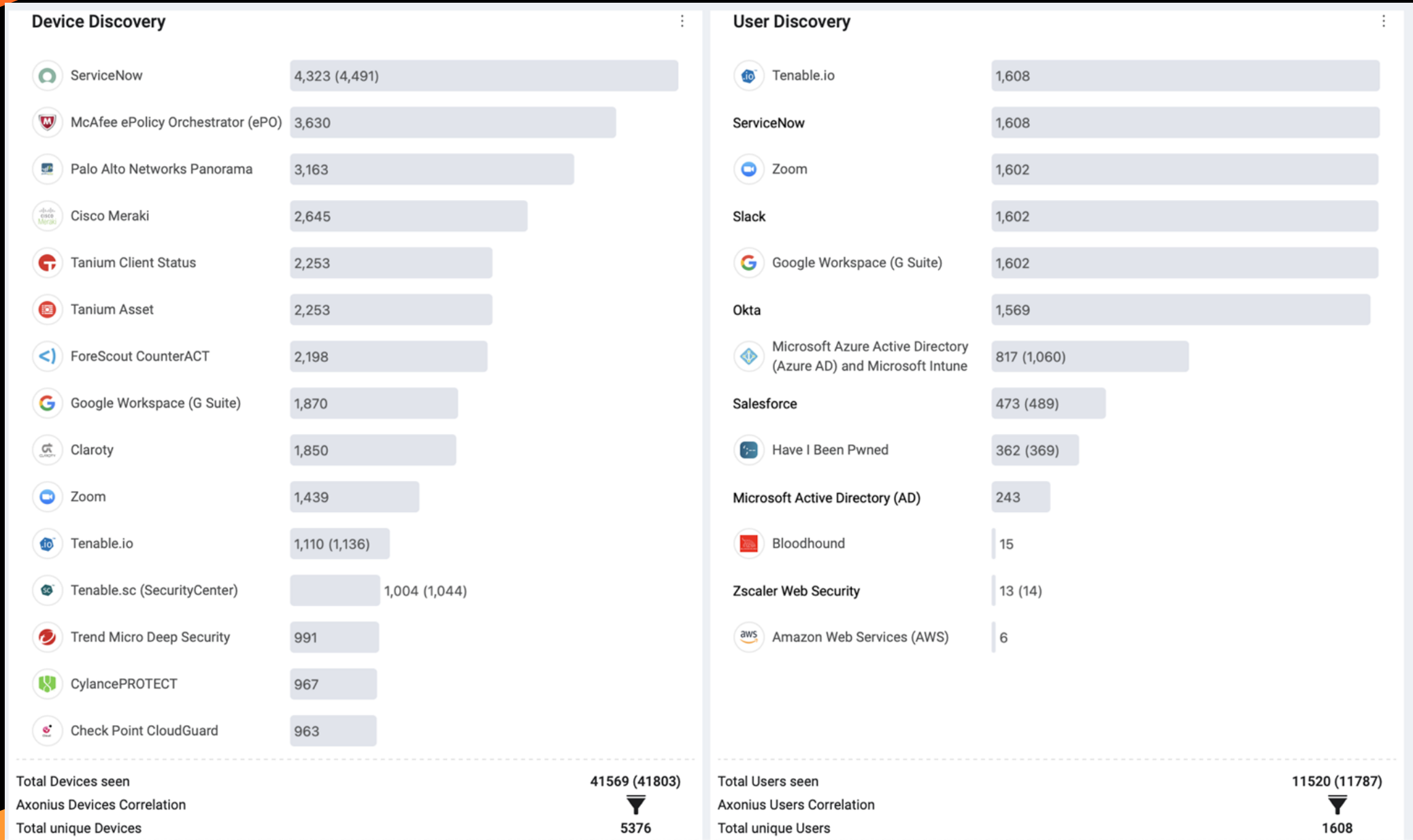
Extract and aggregate Asset Data continuously



Allows analysis of the Holistic Current and Historical State of Assets
Asset Intelligence







04



Guidance of future state is prescribed by SOCI

With **Asset Intelligence the Delta between current state and the future compliant state can be objectively measured**



Asset Intelligence assists by *Indicating what is currently possible* and allowing *further analysis* of Assets data to validate proposed metrics.



Asset Intelligence facilitates moving to a state of continuous compliance.



































Asset Intelligence provides the context required to confidently automate processes.



Create Incident or Ticket

 ServiceNow - Create Incident	 Cherwell - Create Incident	 Opsgenie - Create Alert	 Adobe Workfront - Create Issue	 ServiceNow - Create Incident per Asset
 Demisto - Create Incident per Asset	 ChangeGear - Create Incident	 Jira Service Management - Create Issue per Asset	 Microsoft Azure DevOps - Create Task	 Freshservice - Create Ticket per Asset
 Freshservice - Create Ticket	 Update ServiceNow Tickets	 Jira Service Management - Update Tickets	 Update Zendesk Tickets	 Jira Service Management - Create Issue
 SolarWinds - Create Incident	 BMC Helix Remedy - Create Ticket	 Cherwell - Create Incident per Asset	 SysAid - Create Incident	 TOPdesk - Create Ticket
 Zendesk - Create Ticket	 Zendesk - Create Tickets Per Entity	 Create Case - Salesforce	 ManageEngine ServiceDesk Plus - Create Request	 ManageEngine ServiceDesk Plus - Create Request per A...
 Zoho Desk - Create Ticket	 BOSSDesk - Create Ticket	 TeamDynamix - Create Ticket	 CA Service Management - Create Ticket	 Create Incident - PagerDuty

* Enforcement Set name


Create ticket for missing ePO on Windows

+ Add description

* Run action on assets matching following query:

Devices Windows devices missing McAfee ePolicy Orchestrator (ePO) software

Main Action

 ServiceNow - Create Incident [?](#) [Test Connection](#)

* Action name

Ticket to Install McAfee ePO on Windows

☐ Configure Dynamic Values [?](#)

☒ Use stored credentials from the ServiceNow adapter

Select Adapter Connection [?](#)

65b69c50a3acc4e41a9dda1b

*Incident short description

McAfee ePO is required

*Incident description

These Windows devices do not have the required McAfee ePO agent installed. Route to the desktop team for remediation

*Message severity

error

*Instance Name

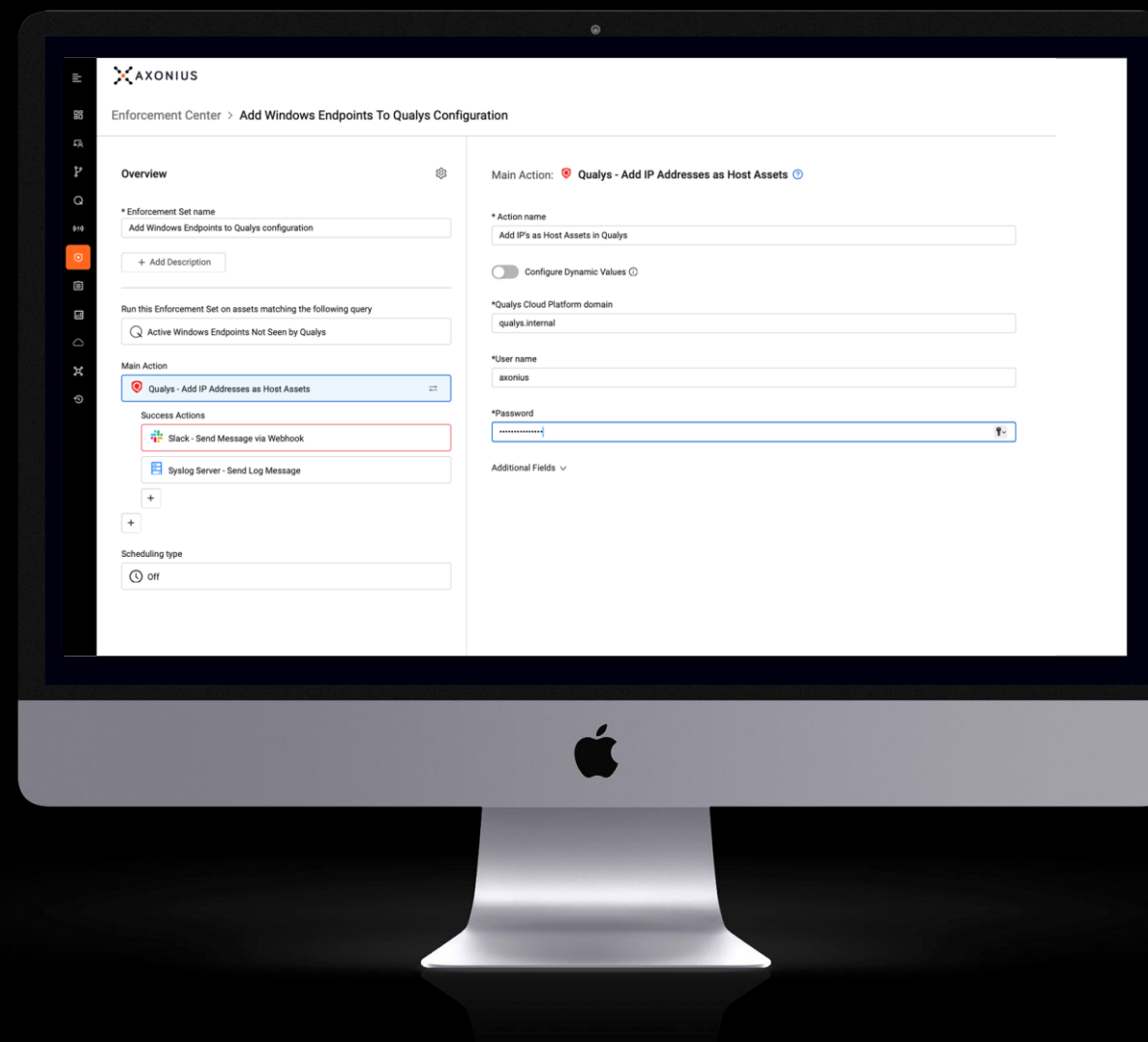
Primary

[Advanced options](#) [Save](#) [Test Run](#) [Save and Run](#)



By connecting to all the security and management solutions, Axonius helps customers:

- More accurately assess risk
- Track compliance maturity daily
- Respond rapidly to changing requirements and situations
- Facilitate Collaboration between teams for containment and remediation
- Optimise Processes and incorporate automation



QUESTIONS?

THANK YOU!



Solutions Architect / Axonius
paul.thomas@axonius.com

