

REDUCE

OPERATIONAL RISK

**AND ACCELERATE
M&A INTEGRATION
USING AXONIUS.**



AXONIUS



Devices

M - Missing McAfee [Edited] Save As Reset

(specific_data.data.os.type == "Windows") and (adapters_

Devices (98)

Adapter Connections										Asset Name
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			DES TO
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			DES TO
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			DES TO
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			DES TO
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			PC-BIT
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			WIN CH
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			WIN R
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			PC-L T
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			WIN CO
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			PC-P N
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			WIN O
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			WIN A
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			WIN A
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			WIN O
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			WIN CE
<input type="checkbox"/>	<input checked="" type="checkbox"/>		ath0	cisco	Meraki	<)	edynum			WIN OY

RESULTS PER PAGE: 20 50 100

Acquisition and merger centric organizations have the material benefit of audited financial statements to gauge the fiscal health of a potential acquisition. But true clarity into cyber health and overall IT hygiene of another company is only possible post-acquisition. Immediately post- acquisition, many organizations rightly enter the “do not break anything phase”.

**HOW CAN THE NEWLY COMBINED IT AND SECURITY TEAMS
CREATE THE KIND OF VALUE THAT JUSTIFIES THE PRICE OF
ACQUISITION?**

Without credible, comprehensive information on the acquired computing state, it’s hard to identify potential problems and even harder to evaluate solutions that address them. Axonius brings clarity to the state of all IT assets – both for the acquiring company and integrated company – to inform IT and security decisions and make the integration successful.



AXONIUS

**Inventory and fully
define all IT assets
acquired including
cloud assets and
unmanaged devices**

1.

With computing environments more dynamic than ever, relying on documentation alone to understand an acquired environment can be a journey of unwanted discoveries. It's rare that a company has a comprehensive, credible asset inventory. Assets overlooked in the due diligence phase but later integrated are blind spots for IT and security teams. Axonius removes those blind spots by giving you clear visibility into all assets.

**Identify the
strength of your
security posture
and IT hygiene**

2.

Any company with a history of acquisitions understands a certain amount of "dressing up" happens in the due diligence phase. For example, security teams at acquiring companies often find out that a smaller number of devices are properly protected and configured than what was specified in audits prior to integration. Post-acquisition, you can use Axonius for asset and user visibility inspection and monitoring to identify and validate:

System environments that can be combined as part of IT system integrations

Properly managed, **secure environments** that should be expanded

Environments or applications should be deprecated

Using Axonius for inspection and monitoring also surfaces areas of risk exposure that require attention, like devices missing security agents, unauthorized or EOL software, users with excessive privileges, or devices missed by a vulnerability scanning regiment.



AXONIUS

Define **automated**
actions to close
gaps, document
change, and report
progress



It becomes difficult to track progress and maintain the momentum needed to achieve integration goals without automation. Axonius reporting is updated continuously as new assets are integrated, helping show progress during large scale integration projects.

The Axonius Cybersecurity Asset Management platform gives organizations a comprehensive asset inventory. By seamlessly integrating with over 250 security and IT management solutions, Axonius deploys in days (not weeks) to improve threat and vulnerability management, security operations, incident response, and overall security posture.

How Customers Use Axonius To **Reduce M&A Cyber Risk**

Quickly and easily understand the assets being acquired. Axonius is agentless and doesn't require network scans or agents on endpoints. Instead, customers connect to the solutions they already use, delivering a complete asset inventory in just days.

Find areas of immediate risk. Axonius can be used to continually search for assets that pose an imminent risk, such as devices missing endpoint security agents, devices found with high and critical vulnerabilities, public-facing assets not being scanned for vulnerabilities, users with expired passwords, and more.

THE AXONIUS QUERY WIZARD

The screenshot displays the Axonius Query Wizard interface. At the top, there's a header with the Axonius logo, a 'Discover Now' button, and a settings icon. Below the header, the 'Devices' section shows a search bar with a query: `(specific_data.data.os.type == "Windows") and ((adapters_data.active_directory_adapter.id == ("{\$exists":true,\$ne:""}))) and not ((adapters_data.epo...`. There are buttons for 'Saved Queries' and 'Query Wizard'. The main area shows a list of devices with columns for 'Adapter Connections', 'Asset Name', 'Last Seen', and 'IP Address'. A modal window titled 'Show only data:' is open, allowing users to filter results by criteria like 'OS: Type' (Windows), 'ID', and 'Last Seen'. The bottom of the interface shows 'RESULTS PER PAGE' with options for 20, 50, and 100, and a pagination control.

The Axonius Query Wizard

allows for one-off and programmatic searches across all IT assets, helping to inform M&A integration decisions

Automatically enforce policies for integrated assets. When integrated assets don't meet security policies, the Axonius Security Policy Enforcement Center automatically notifies teams, enriches devices and user data, or deploys files and commands to mitigate risk.

For more information, reach out to sales@axonius.com



AXONIUS