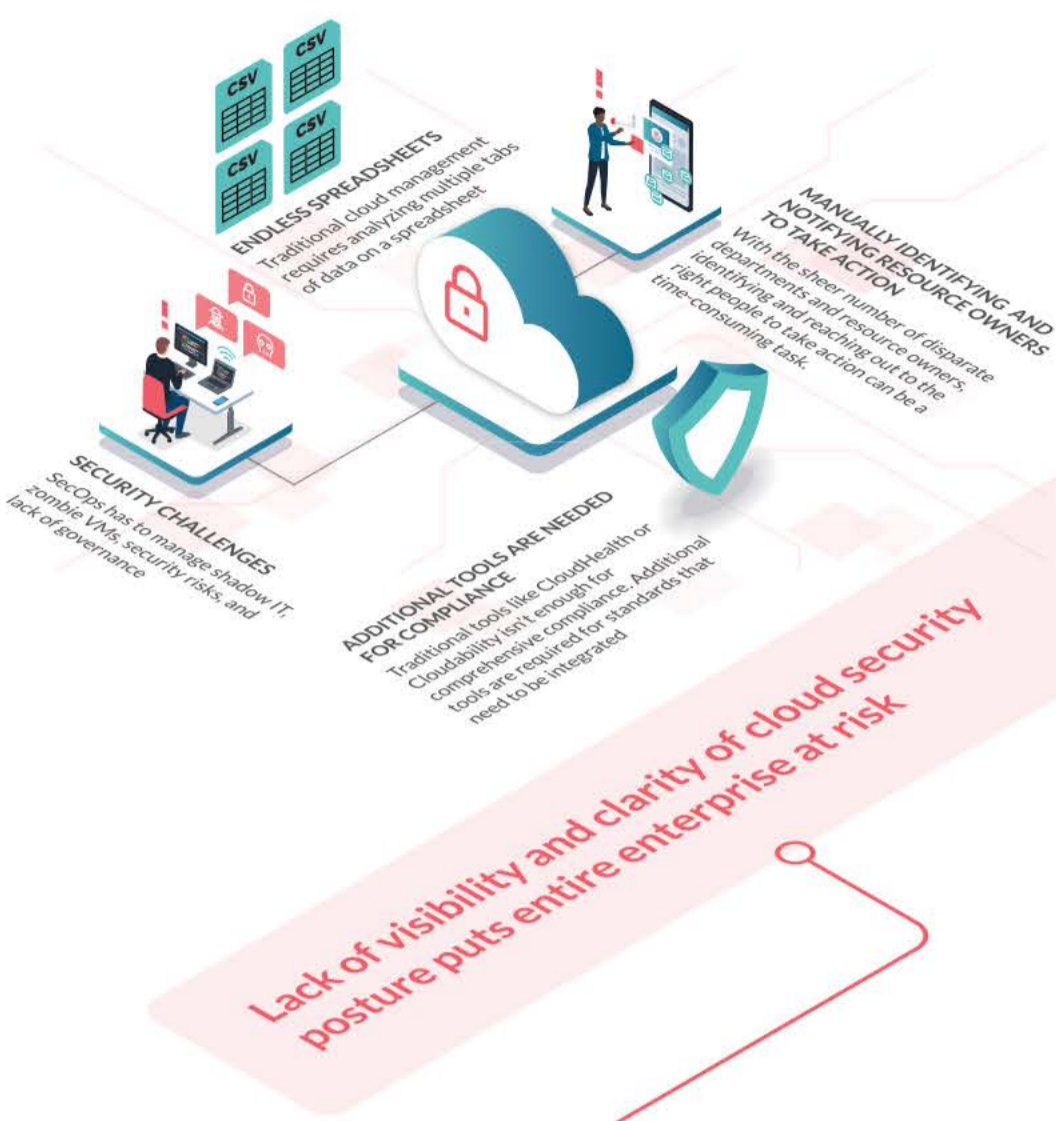# Cloud Security Management
Old Way vs the Intelligent Way

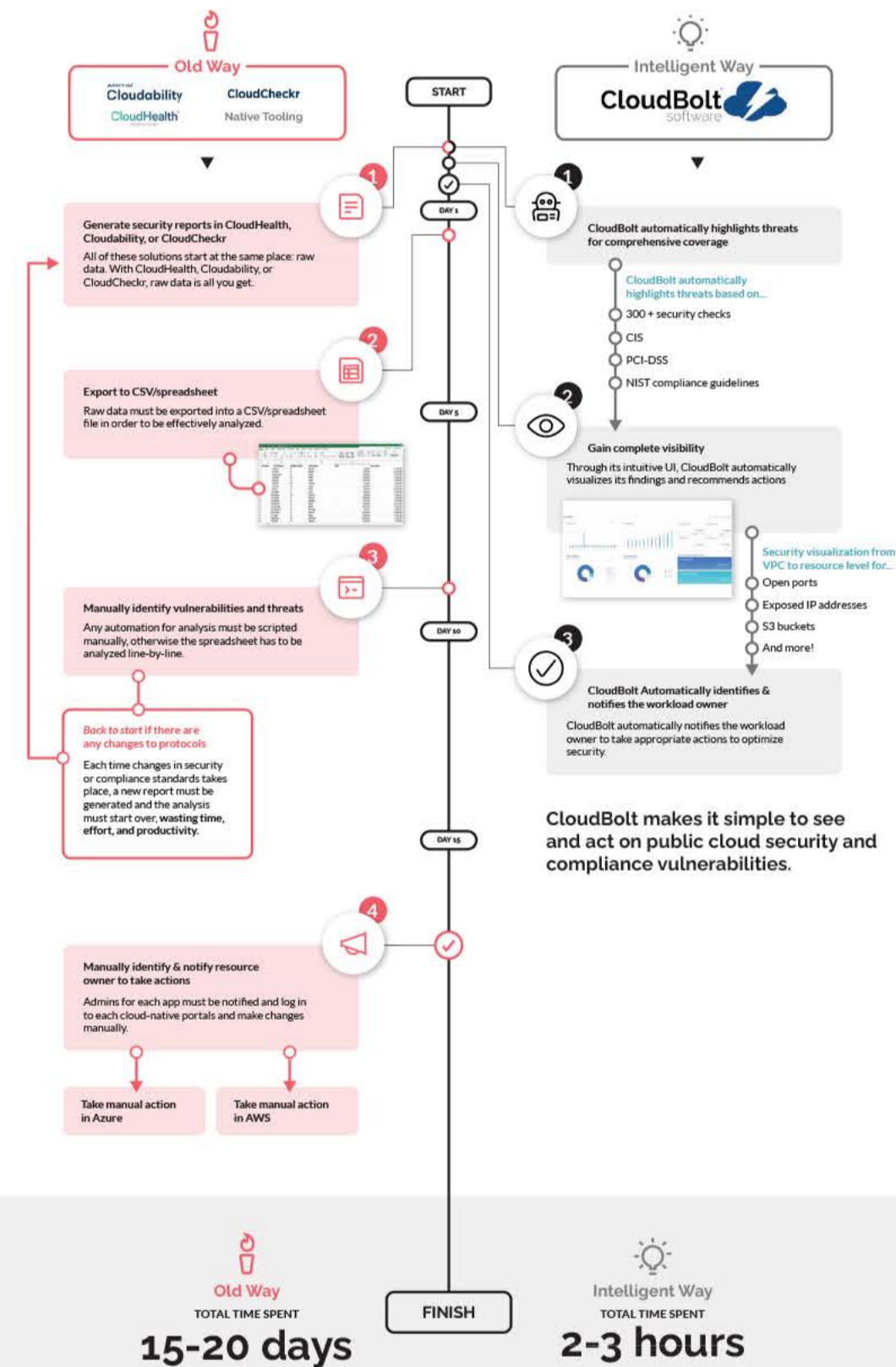THE PROBLEM WITH TRADITIONAL WAYS OF
Managing Cloud Security

ENDLESS SPREADSHEETS
Traditional cloud management requires analyzing multiple tabs of data on a spreadsheet.

MANUALLY IDENTIFYING AND NOTIFYING RESOURCE OWNERS TO TAKE ACTION
With the sheer number of disparate departments and resource owners, identifying and reaching out to the right people to take action can be a time-consuming task.

SECURITY CHALLENGES
SecOps has to manage shadow IT, complex VM security risks, and lack of governance.

ADDITIONAL TOOLS ARE NEEDED FOR COMPLIANCE
Traditional tools like CloudHealth or Cloudability aren't enough! For comprehensive coverage, additional tools are required for standards that need to be integrated.

Lack of visibility and clarity of cloud security posture puts entire enterprise at risk

---

MANAGING CLOUD SECURITY
Old Way vs The Intelligent Way

Old Way

Cloudability   CloudCheckr
CloudHealth   Native Tooling

Intelligent Way

CloudBolt software

START

Old Way

1 Generate security reports in CloudHealth, Cloudability, or CloudCheckr
All of these solutions start at the same place: raw data. With CloudHealth, Cloudability, or CloudCheckr, raw data is all you get.

2 Export to CSV/spreadsheet
Raw data must be exported into a CSV/spreadsheet file in order to be effectively analyzed.

3 Manually identify vulnerabilities and threats
Any automation for analysis must be scripted manually, otherwise the spreadsheet has to be analyzed line-by-line.

Back to start if there are any changes to protocols
Each time changes in security or compliance standards takes place, a new report must be generated and the analysis must start over, wasting time, effort, and productivity.

4 Manually identify & notify resource owner to take action
Admins for each app must be notified and log in to each cloud-native portals and make changes manually.

Take manual action in Azure   Take manual action in AWS

Intelligent Way

1 CloudBolt automatically highlights threats for comprehensive coverage
CloudBolt automatically highlights threats based on...
- 300+ security checks
- CIS
- PCI-DSS
- NIST compliance guidelines

2 Gain complete visibility
Through its intuitive UI, CloudBolt automatically visualizes its findings and recommends actions

Security visualization from VPC to resource level for...
- Open ports
- Exposed IP addresses
- S3 buckets
- And more!

3 CloudBolt Automatically identifies & notifies the workload owner
CloudBolt automatically notifies the workload owner to take appropriate actions to optimize security.

CloudBolt makes it simple to see and act on public cloud security and compliance vulnerabilities.

FINISH

Old Way
TOTAL TIME SPENT
15-20 days

Intelligent Way
TOTAL TIME SPENT
2-3 hours

- Provides only raw data
- Requires **weeks of manual** analysis and action
- Automation requires manual building of scripts
- Impossible to scale

- More real-time information (15 minutes refresh rate vs days)
- Find vulnerabilities and resource owners in minutes
- Intuitive visualization of findings
- More automation for an **immediate response**

Continuously and automatically secure and govern your public cloud usage with CloudBolt

---

Save 20% on your cloud spending immediately with CloudBolt
See how CloudBolt can save you 20% on wasted public cloud spend with a free comprehensive assessment today!

LEARN MORE

CloudBolt software

CloudBolt's hybrid cloud platform for enterprises helps IT admins provide simple to very complex IT resources to end users from a single portal.