
secberus
What’s your most pressing security need?

Any business that’s migrating to the cloud has security needs, whether they’re related to development and operations, security and compliance, management, or costs. Explore how the Secberus cloud governance platform responds to each use case.

## Development & Operations

Achieve continuous innovation and development at the speed of business.

01. Organize and govern your cloud infrastructure.
02. Define and globally manage policy that reflects the specific needs of your business.
03. Scale your governance policies.
04. Minimize alert fatigue and get the most from advanced workflow capabilities.

## Security & Compliance

Focus on the violations that are actually affecting your business performance instead of wasting time on false-positive alerts.

Map, manage, implement and audit compliance exactly how you need to.

05. Map your regulatory compliance requirements to your policies.
06. Get real-time compliance reporting.
07. Understand your risk posture at any time, from any perspective.
08. Optimize how you manage alerts and your remediation workflow.

## Management

Get real-time context from the right people and then deliver that context to the right individual to reduce MTTR.

Gain visibility into cloud posture management cost gaps.

09. Manage your cloud posture with fewer third-party tools.
10. Detect misconfigurations in as close to real time as possible.
11. Easily build cloud governance into your budget and reduce TCO.
12. Get faster, more responsive, more adaptable cloud resource coverage.

# Organize and govern your cloud infrastructure.

## You want to:

- Organize applications, cloud accounts, resources and teams based on specific business criteria (regulatory compliance, business units, integrations, etc.) within your governance solution (including cloud security posture management, or CSPM functionality).
- Ensure that the specified organizational criteria comes from pre-existing tags in the cloud environments that you have already created.

## You've tried:

- Hiring at least one additional engineering team to manually and continuously search for cloud resource tags, then assign tagged resources to specific OUs in your CSPM.
- Having engineers create custom scripts to add cloud environments and resources to appropriate account groups in the CSPM.

## With Secberus you can:

- Govern your public cloud infrastructure with policies based on tags, business units, applications, clouds or a bespoke organizational configuration.
- Ensure that the security or operational controls and compliance frameworks you need are in place.

# Define and globally manage policy that reflects the specific needs of your business.

## You want to:

- Define a global cloud security strategy that may contain dozens to hundreds of custom policies.
- Apply this strategy to specific OUs, applications, and environments in order to monitor and manage drift from intended baseline security configurations.

## You've tried:

- Working with highly limited policy customization, such as adjusting each policy's risk appetite score or granularity only to a specific OU or cloud environment—limitations that contribute to a high false-positive alert rate and longer median time to remediate (MTTR) because you must do triage.
- Third-party tools and custom scripts to manage alerts.
- Choosing between speed of delivery and security.

## With Secberus you can:

- Customize policies directly on our platform and apply policies across data sources connected to the platform.
- Configure policies to support exceptions, read tags, and more.
- Adjust policies to risk and completely align policies with the business.
- Almost completely eliminate false positives.

# Scale your governance policies.

## You want to:

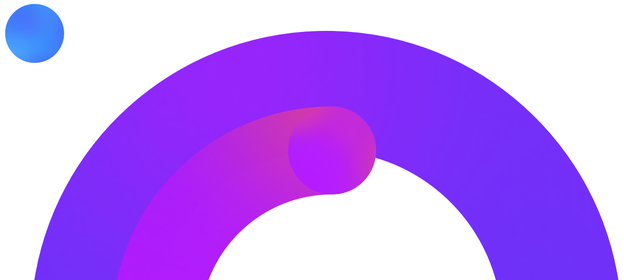
- Auto-scale global governance policies (security, compliance, operations) as your cloud footprint and tools evolve from a single platform.

## You've tried:

- Building internal applications to determine your global governance posture and having teams manually apply and update generic policies which must then be investigated to manage false positives and meet compliance audit requirements.

## With Secberus you can:

- Be assured your cloud environments are covered, no matter how quickly you scale.



# Minimize alert fatigue and get the most from advanced workflow capabilities.

## You want to:

- Some industry benchmarks estimate that the average enterprise spends 1 business day on triage for every 32 alerts—and enterprises can easily surpass 500 alerts per day.

## You've tried:

- Hiring more people to do triage.
- Investing in products that offer post-alert triage, but create a scenario where the policy doesn't match the response, so baseline policies are not a true indicator of intent.
- Ignoring the growing number of alerts while trying to find the needles in the haystack that create the highest risk.

## With Secberus you can:

- Ensure that your policies are CARTA-enabled (Continuous Adaptive Risk and Trust Assessment), defined by the business, and free of false positives.
- Get an accurate baseline and an end to alert fatigue, and get the right violations to the right people.

# Map your regulatory compliance requirements to your policies.

## You want to:

- Map regulatory compliance requirements to custom policies and specific scopes of applications, OUs, divisions, clouds, and cloud accounts.

## You've tried:

- Manually mapping your compliance requirements to build reports.

## With Secberus you can:

- Enjoy built-in, customizable mapping capabilities that are mapped to compliance requirements and aligned with the organizational logic and business requirements of each application, cloud provider, tag or data source.
- Get real-time compliance reporting.

# Get real-time compliance reporting.

## You want to:

- Be able to share in-scope regulatory compliance reports with the compliance team when they request them.

## You've tried:

- Exporting CSPM data in CSV format, then using Excel to filter in-scope resources and map them to regulatory compliance requirements, then sending them to the team requesting the report. High rates of false-positives render the reports inaccurate unless the team investigates each alert in the report—which renders the report out-of-date.

## With Secberus you can:

- Get your required compliance audits in real time—any time. Secberus monitors compliance to help the business consistently and continuously maintain its compliance-required controls.
- Use your tagging strategy to get customized reports.
- Map any compliance framework to controls, enabling the business to customize its strategy without complicating the compliance process.

# Understand your risk posture at any time, from any perspective.

## You want to:

- Understand your risk posture from multiple perspectives—data source, application, tags, and more.

## You've tried:

- Having engineers export logs of misconfiguration discovery and remediation confirmation from CSPM products to Excel, then filtering the in-scope resources to create charts and reports.

## With Secberus you can:

- Fully align your governance strategy and policies so that your baseline and any deviation from the baseline are 100% accurate and available in real time for any segment of the cloud or any multi-cloud segment.

# Optimize how you manage alerts and your remediation workflow.

## You want to:

- Remediate misconfigurations and return your security posture to the appropriate baseline as quickly as possible to reduce risk exposure.

## You've tried:

- Creating scripts to investigate alerts with supplementary context to identify true violations, or combining custom-built scripts and third-party tools to triage, prioritize and direct alerts to the correct teams for remediation.

## With Secberus you can:

- Fully customize policies, keeping your specific needs in mind, from business intent to resource ownership. This approach allows you to eliminate virtually all false positives false positives and allows resource owners to move faster, receive only true violations, and accelerate remediation.

# Manage your cloud posture with fewer third-party tools.

## You want to:

- Be able to apply a cloud security posture management (CSPM) approach with minimal costs.

## You've tried:

- Using multiple tools that ultimately create more inefficiency and less productivity because they require additional workarounds.

## With Secberus you can:

- Stop relying on third-party tools because our cloud governance platform lets you manage your cloud posture independently of them.

# Detect misconfigurations in as close to real time as possible.

## You want to:

- Detect misconfigurations in as close to real-time as possible.

## You've tried:

- Increasing scanning intervals to address growing API call costs.

## With Secberus you can:

- Benefit from a lightweight solution that's architected to detect changes in your infrastructure immediately. It then runs policies to check the changes and the affected resources and policies, making API calls cost-effective while maintaining extensive coverage.

# Easily build cloud governance into your budget and reduce TCO.

## You want to:

- Be able to budget for your governance solution for a 12-24 month period and significantly reduce your total cost of ownership (TCO).

## You've tried:

- Scrimping on the applications, resources and other business-critical expenses that would enable growth and innovation to make up for overage charges on 'per billable workload' services that eat away at your annual budget.

## With Secberus you can:

- Benefit from a straightforward pricing model, simplified projections that make budgeting easier, and no overage charges.
- Significantly reduce your cloud security TCO by reducing your need for and investment in point solutions, minimizing time lost to false-positive alerts, and boosting productivity by allowing your teams to focus where they can best drive growth.

# Get faster, more responsive, more adaptable cloud resource coverage.

## You want to:

- Manage your existing cloud services and adopt new cloud resources and tools that will help drive business value.
- Get more from these tools and ensure that your policies are supported as quickly as possible.

## You've tried:

- Using manual investigation to audit, validate, and create tickets to remediate violations that were out of the scope of your CSPM, and supplementing that work with native tools.

## With Secberus you can:

- Support most new cloud services in a matter of days, and extend policies to those services immediately.

secberus

# Ready to start simplifying cloud security?
# **Drop us a line.**

Want to read more about how cloud governance simplifies cloud security?

Show me more