

GAUNTLET

AI-Powered DevSecOps



Why Gauntlet?



Stop Security Breaches



Detect & Stop Cyber-Risk
Without Slowing Business



30+ Compliance Standards



Built by Internationally-Acclaimed
Cyber Experts

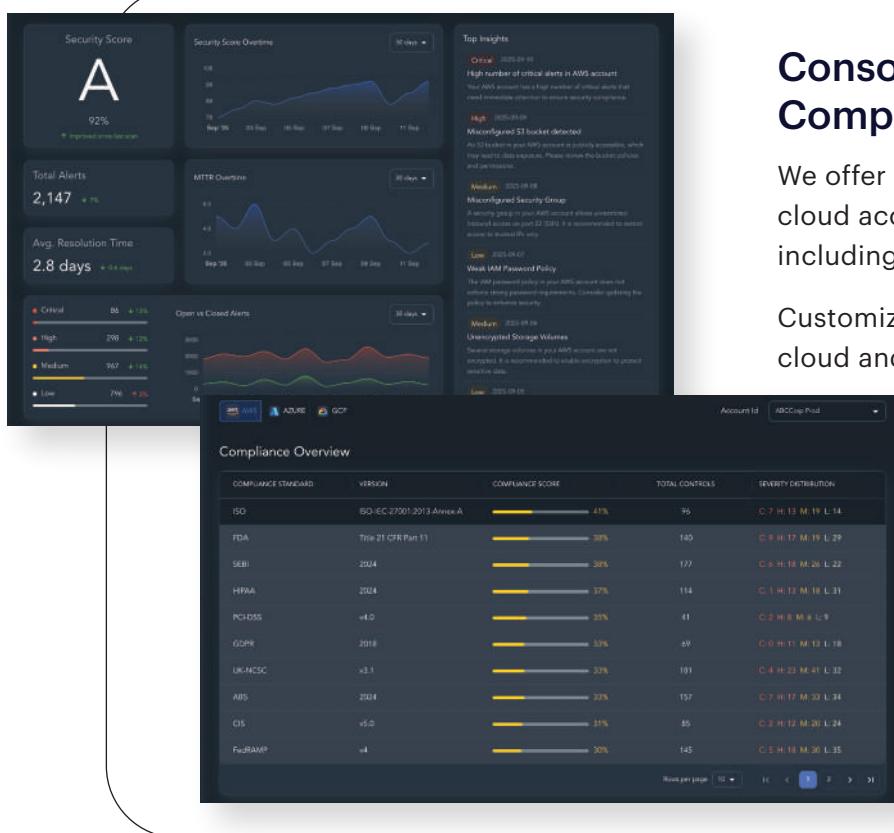


GenAI & Agentic AI
for Speed & Accuracy

Trusted by Global Companies



Cloud Security Posture Management

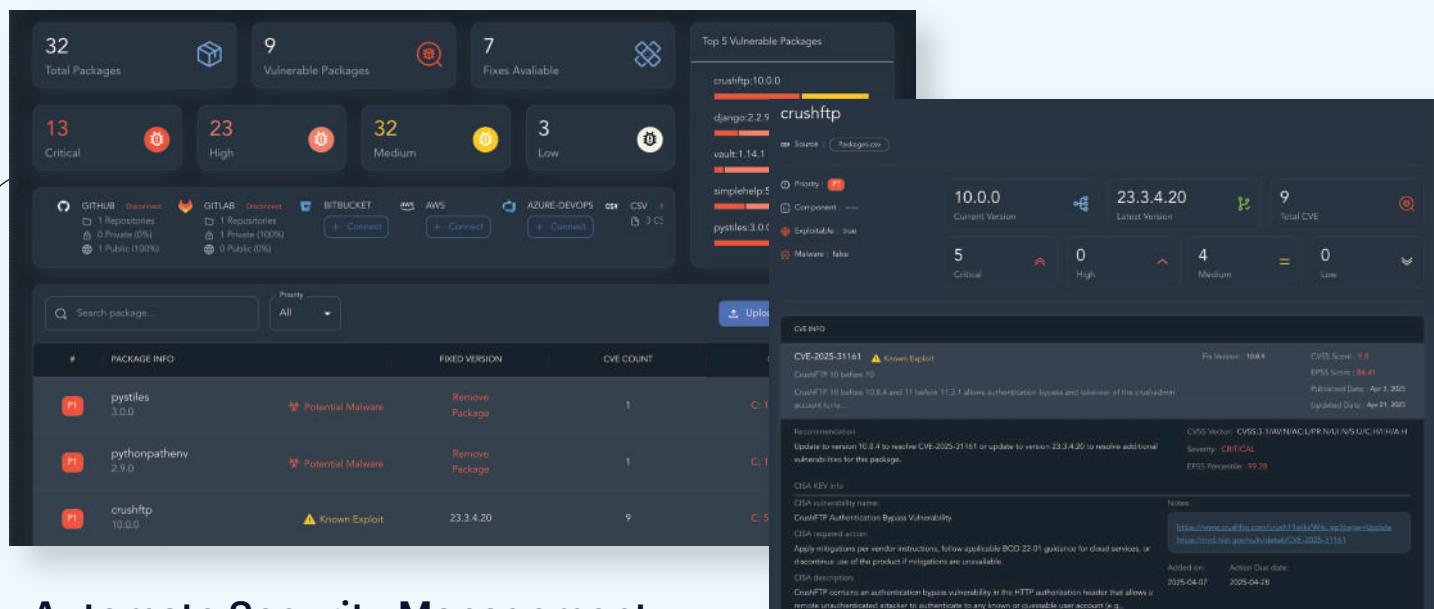


Consolidated Cloud Security & Compliance Dashboard

We offer a unified cybersecurity view of all of your cloud accounts across AWS, Azure & GCP, including Production, QA, UAT, Dev, etc.

Customize your compliance dashboards for each cloud and each account.

Software Supply Chain Security



Automate Security Management of Your Entire Software Bill of Materials

Just connect your code repo and forget about it. Gauntlet builds the SBOM everyday, scans against multiple vulnerability and exploit databases and offers a rich set of developer-friendly results – FULLY AUTOMATED.

CVSS scores are no longer enough. With Gauntlet's EPSS and KEV ratings, triage accurately and take action.

Secrets Scanning Dashboard with Confidence Score

The dashboard provides a high-level overview of secret exposure across multiple platforms:

- Repositories:** 2 GitHub (Received), 1 GitHub (Orcano), 1 Bitbucket.
- Total Secrets:** 38
- API Keys:** 15
- Passwords:** 2

Secrets Over Time: A line chart showing the number of secrets discovered over time, with a significant peak around September 23rd.

Secrets List: A table showing details for five specific secrets:

SECRET TYPE	SOURCE	AUTHOR	DISCOVERED ON	VALIDATION STATUS
generic-api-key	Secrets.txt (Public)	Demo User (demo.user@users.noreply.github.com)	9/23/2025	Verified
stripe-access-token	Secrets.txt (Public)	Demo User (demo.user@users.noreply.github.com)	9/23/2025	Verified
slack-user-token	Secrets.txt (Public)	Demo User (demo.user@users.noreply.github.com)	9/23/2025	Verified
generic-api-key	SECRETS.txt (Public)	Demo User	9/23/2025	Verified

Generic API Key Detail View:

- Repository:** Demo_repo (Public)
- Branch:** main
- Author:** Demo User (demo.user@users.noreply.github.com)
- Discovered On:** 9/23/2025
- Permissions Info:** 3 Permissions

Threat Score: 81% (High)

Action Required: Remove the secret from the codebase immediately.

AI Insights: This secret has a high confidence score of 75%, indicating a strong likelihood of being a true positive. The exploitability score of 60% suggests that while the secret is potentially exploitable, it may require specific conditions or additional vulnerabilities to be effectively leveraged by an attacker. Overall, this secret should be prioritized for remediation due to its high confidence level.

Instant Alerts for Exposed Secrets. Validated Ones, We Mean

Eliminate the window of exposure when it comes to exposed credentials & secrets. Our “Snap-Scan” feature alerts you of such exposure BEFORE they hit production. Plus we rigorously validate the legitimacy of each secret and use Agentic AI to indicate the actual risk based on permissions granted. In other words, we are fast and we are precise.

AI Security Posture Management

The dashboard provides a comprehensive view of AI service security posture:

- Security Score:** 64% (Medium Risk)
- Total Controls:** 50 (including 30 PASS, 17 FAIL, 1 CRITICAL, 2 TBA)
- Exceptions:** 2
- Resource Inventories:**
 - Top Vulnerable Resources: sagemaker-notebook-12345, sagemaker-notebook-12345
 - Inventory (AI Services): Sagemaker Notebooks (20), Bedrock Guardrails (20), Neptune DB (20), Comprehend (20)

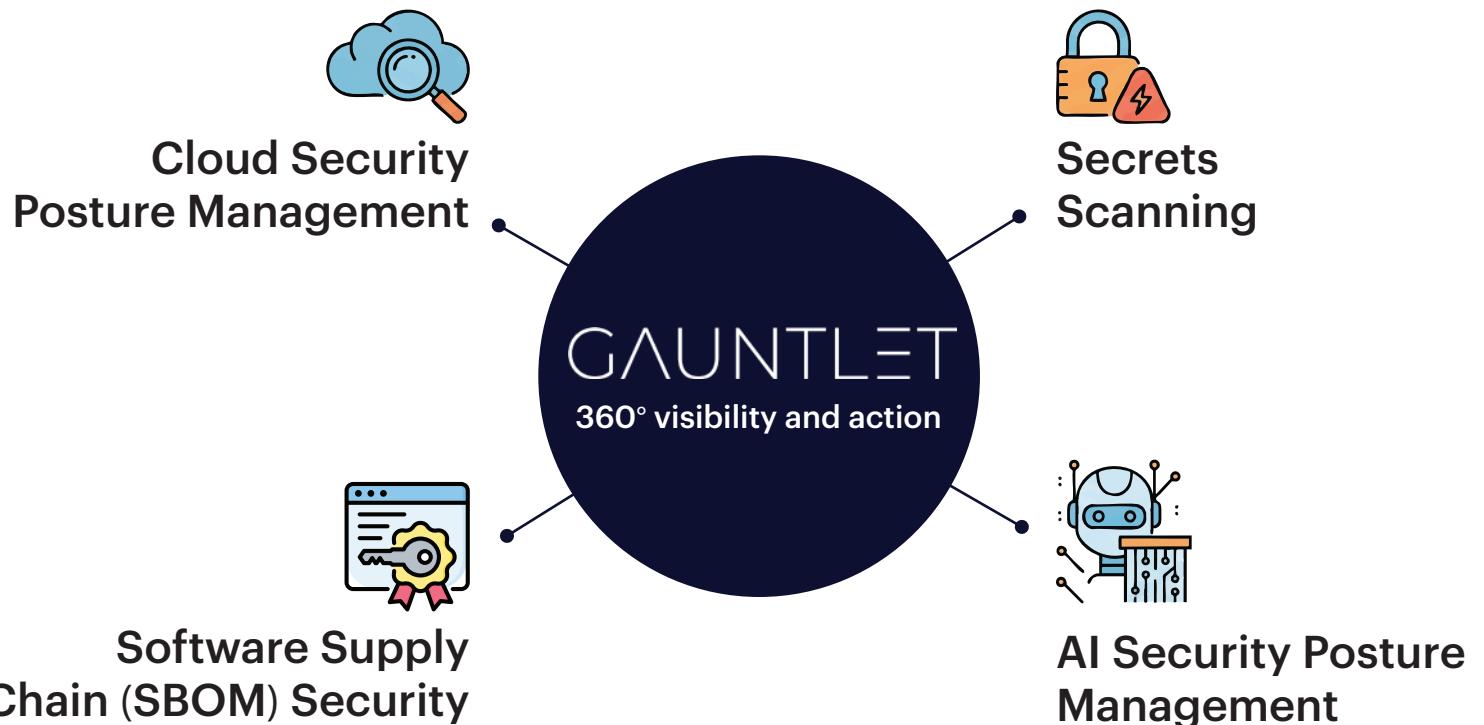
Remediation: A step-by-step guide for setting prompt attack strength for Amazon Bedrock guardrails:

- Sign in to the AWS IAM Console and open the IAM console at <http://console.aws.amazon.com/iam/>.
- On the right side of the navigation bar, choose your account name, and then choose Security credentials.
- Expand the Multi-factor authentication (MFA) section.
- Select Assign MFA device.
- In the wizard, type a Device name, choose Hardware TOTP Token, and then choose Next Step.
- In the Serial number box, type the six-digit number displayed by the MFA device. You might need to press the button on the front of the device to display the number.

Dark Side of AI Services on Cloud. We Throw Light on Them

Using Sagemaker, Bedrock, Azure AI Services, Vertex AI, or any of the modern-day cloud-hosted AI services? There are over 50 ways insecure misconfigurations for these services can wreak havoc on your infrastructure.

Gauntlet's cutting edge AI Security Posture Management validates dozens of security guardrails against your AI services on public cloud. Shift-left your AI Security Posture Management.



The Gauntlet Advantage

- ✓ Unifying cloud, code, supply chain and AI security management into one powerful platform
- ✓ Intuitive, self-managed dashboard reduces cybersecurity spend
- ✓ Gauntlet Support: Award-winning cybersecurity team at your fingertips for consultations
- ✓ Agentic & GenAI capabilities reduce MTTR by 60% compared to cloud native & market available tools
- ✓ Rigorously vetted to reduce false positives. Use your time wisely – on clear and present dangers
- ✓ Support for popular standards including ISO 27001, GDPR, SOC2, FDA, and over 30 others compliance guidances



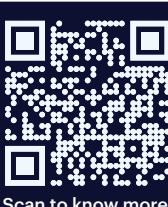
Real Stories, Real Results

Gauntlet has not only given us the holistic view we needed but also provides a prioritized list of issues and clear instructions on how to fix them. It gives us the confidence to develop fast knowing that if anything changes we will be notified.

Jeremy Bennett
Chief Technology Officer @ Boosted Reality

I think the entire feature set itself has significant impact on our security posture, but specifically, the continuous reporting is extremely valuable for us to track new issues, especially during development process when our AWS environment is very dynamic

Brian Wang
Principal Cloud Architect @ Movano Health



Scan to know more



www.gauntlet.security



contact@gauantlet.security