tenable

WHY MANAGING CLOUD ENTITLEMENTS IS NEARLY IMPOSSIBLE... AND HOW TO DO IT

How to manage cloud entitlements and least privilege with success

Table of Contents

EXECUTIVE SUMMARY

Driven by a need to respond with greater speed to new market opportunities and competitive pressures, the accelerated pace of digital transformation with cloud has placed unprecedented pressure on already overburdened security teams. Rapid public cloud adoption, particularly infrastructure as a service (IaaS) and multi-cloud, have resulted in a modern attack surface that is rapidly expanding, highly distributed, and exponentially more complex.

With traditional perimeters gone, identities have become the largest cloud infrastructure attack surface. Recent breaches show that attackers are exploiting mismanaged IAM privileges to penetrate an organization's cloud infrastructure and reach sensitive data. To strengthen your cloud infrastructure against such risks, you need full visibility into the identities with access to your cloud resources as well as an understanding of any associated risk and the means to mitigate quickly.

Do you have the capabilities for securing, managing and investigating your cloud entitlements effectively? If not, you're not alone

Tenable Cloud Security is a comprehensive cloud security solution for managing security and compliance in the most complex Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) environments. As a software as a service (SaaS) solution, Tenable Cloud Security spans full asset discovery, flexible risk auto-remediation, real-time anomaly detection, compliance auditing and policy enforcement. The unique identity-driven architecture gives deep visibility into effective access and the toxic scenarios that put data at risk, and unifies cloud infrastructure entitlement management (CIEM) and cloud security posture management (CSPM) in one solution. Using Tenable lets you improve your cloud security posture and implement zero trust and least privilege across your multi-cloud environment while achieving cost-saving collaboration and consolidation across security, devops and IAM.

With CIEM capabilities from Tenable you can:

- Visualize all entitlements, resources and access relationships, and related risks, across multi-cloud environments
- Govern risk and manage access by privileged identities and third parties
- Eliminate excessive entitlements for human and machine identities
- Review and certify entitlements (across admins, developers and DevOps, as well as human and SaaS third parties)
- Detect and monitor public exposure and shared resources
- Generate least-privilege policies and automate remediation
- Detect anomalies and support forensics and investigation
- Simplify developer access control with self-service just-in-time (JIT)

Further, cloud security posture management capabilities help you:

- Manage your cloud asset inventory
- Enforce policies and detection of misconfigurations
- Monitor and report on compliance with industry standards and best practices (e.g. SOC2, HIPAA, CIS)

As a security professional, it is a responsibility, and privilege, to be vested in protecting what is likely your organization's biggest growth platform. This paper explores how to get a grip on the weakest link in cloud infrastructure security — identities — and govern them at scale with minimal effort.

THE CHALLENGE - A SAD STATE OF AFFAIRS

Recent major breaches show that identities play a role in virtually every attack scenario in cloud infrastructure. Let's look at why:

- **Excessive entitlements.** In the interest of speed, organizations tend to over privilege identities when spinning up cloud environments
- **Shift left is moving infrastructure security to teams with other priorities.** DevOps teams have lots on their plate; security is not usually their top priority, nor area of expertise.
- **Driving blind.** Tracking entitlements and their use is hard. Cloud provider tools lack the visibility or context to give a full picture of access to resources and remediate access risk at scale and across clouds.
- **Legacy PAM and IGA are limited by their on-prem DNA.** In cloud infrastructure they lack granular service or resource level visibility, and cannot identify or remediate entitlement risks and excessive permissions.

Securing cloud infrastructure calls for a deep, unified view into all identities and cloud resources to understand the full stack of access entitlements and privileges, and associated risk. You must be able to secure all privileged identities and minimize their risk of being compromised. You need the means for removing excessive and risky privileges, managing access control and permissions, investigating activities and behavior, and applying least privilege across the board, throughout the cloud identity lifecycle.

There's urgency. The longer you wait to understand and undo identity risk, the greater the complexity in doing so as the number of privileged identities, exposure risks, excessive permissions and sensitive resources in your environment continue to grow.

THE SOLUTION: SECURE CLOUD INFRASTRUCTURE IDENTITY FIRST

Solutions such as CIEM, CNAPP and Cloud Infrastructure Governance (CIG) address the high importance of managing entitlements and access policy throughout the identity lifecycle. They are expected to keep pace with evolving protection requirements for cloud-native applications, spanning virtual machines, containers and serverless workloads.

Tenable Cloud Security is the first solution to offer full-stack lifecycle management of the entitlements granted by configuration of identities, compute resources, data stores and the network.

Tenable helps security, devops and IAM practitioners:

- Gain a full, contextual view into human and machine identities to identify privileged identities and evaluate all permission configurations to understand risky or excessive privileges, and how associated compute, data and network resources map across their organization's multi-cloud environment
- Leverage advanced analyses and machine-learning algorithms to address critical cloud security issues and identify identity and configuration risks and threats
- Mitigate and prevent risks at scale using automatically generated least privilege policies that integrate seamlessly with ticketing, continuous integration / continuous development (CI/CD) pipelines and infrastructure as code (IaC)

How does it deploy? An agentless, API-based SaaS solution, Tenable requires nothing to deploy and just minutes to set up. It supports the leading cloud service providers and offers deep interoperability with cloud-based identity providers. Tenable starts aggregating data in minutes after deployment, bringing actionable information into view almost instantly.

Who can use it? No prerequisites are required. Tenable meets the needs of cloud customers of all sizes, from large enterprises to smaller, cloud-native organizations. In cloud environments, all organizations have the same IAM challenges.

How do I use it? Tenable gives organizations control over their cloud infrastructure that they were unable to achieve before. Tenable empowers security, DevOps and IAM teams — even with little cloud security expertise — to see deeply into the full cloud assets inventory and permissions relationships, govern privileged entities, detect misconfigurations and practice least privilege in modern multi-cloud environments.

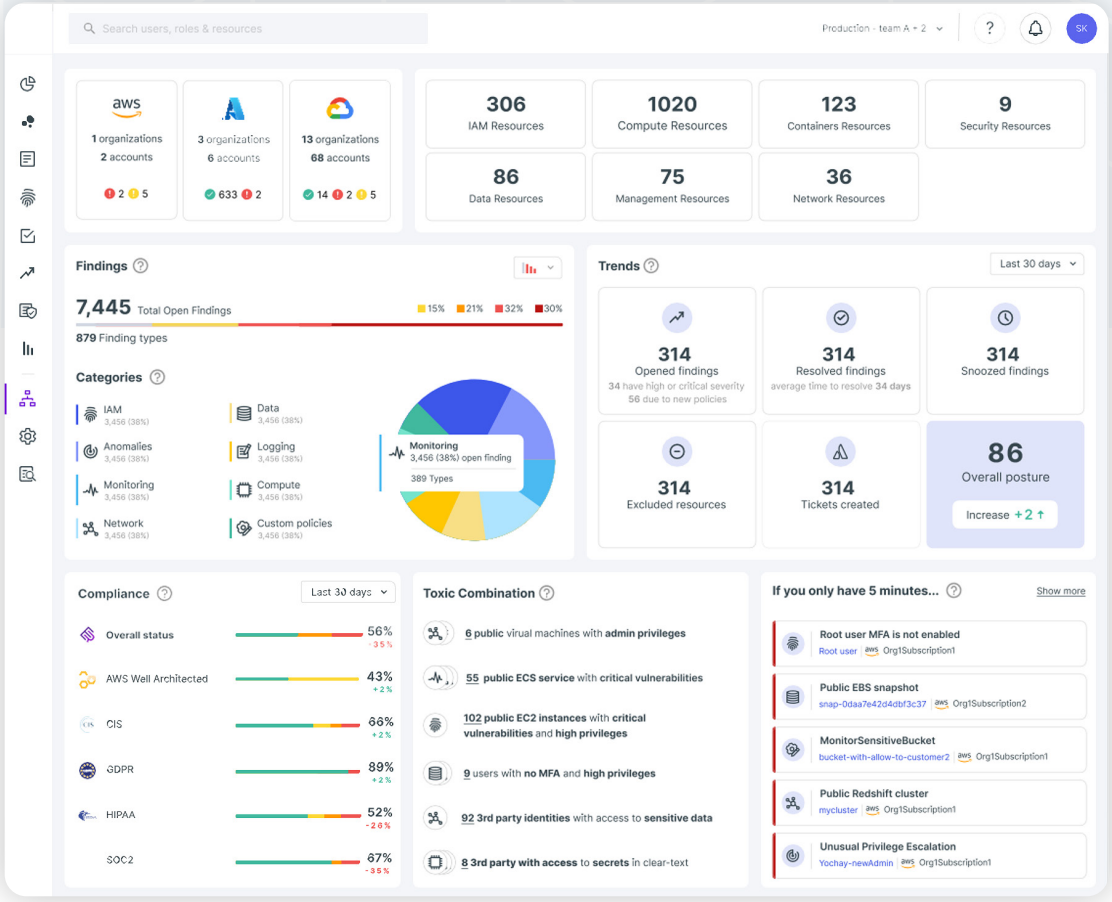
KEY USE CASES: HOW YOU CAN APPLY TENABLE CLOUD SECURITY

Visualize all cloud assets and relationships

The Tenable management dashboard provides a visual overview, with click-through deep dive, into all identities in your environment and any risk caused by excessive permissions, misconfigurations, internet exposure, compliance issues and anomalies.

The one-stop view helps answer:

- What are my top IAM risks?
- How many entitlements are excessive and what is the potential impact?
- Where are we falling short on compliance?
- Which identities are privileged and can be compromised?
- How much is my environment exposed to the outside?



Tenable Cloud Security management dashboard: Get a one-stop view into your multi-cloud environment including prioritized risks, compliance status and behavioral anomalies.

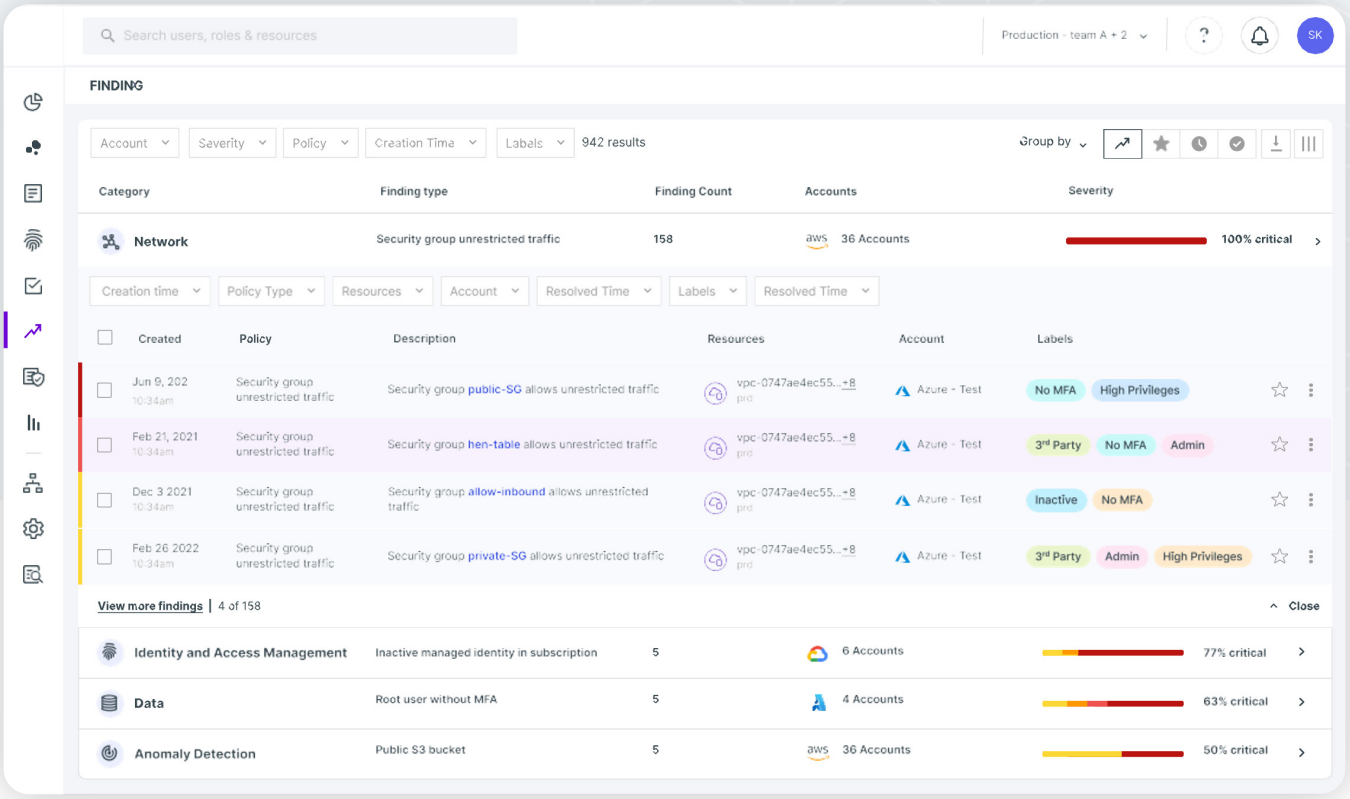
Prioritize and remediate risk

Tenable provides a prioritized view into the entitlement risks in your cloud environment. It shows risky identities and permissions, including inactive and over-privileged users, service identities and groups.

Start your day by reviewing one by one the access and configuration risks that Tenable has detected, homing in by level of severity. Mitigate risk by following easy and clear remediation steps for removing excessive permissions and applying policy changes that, for example, minimize exposure to sensitive resources, remove dangerous privileges and eliminate inactive users. Tenable works with your tech stack, including Datadog, Slack, Splunk, email, ServiceNow, Jira, Okta and Azure Active Directory, to seamlessly communicate on risk and deliver new least privilege policies directly into your IT and DevOps workflows.

Actionable views help you drill down to answer:

- Is the severity of the risk warranted?
- Has the entitlement ever been used?
- Can the user self-escalate to an admin role, creating unwarranted risk?

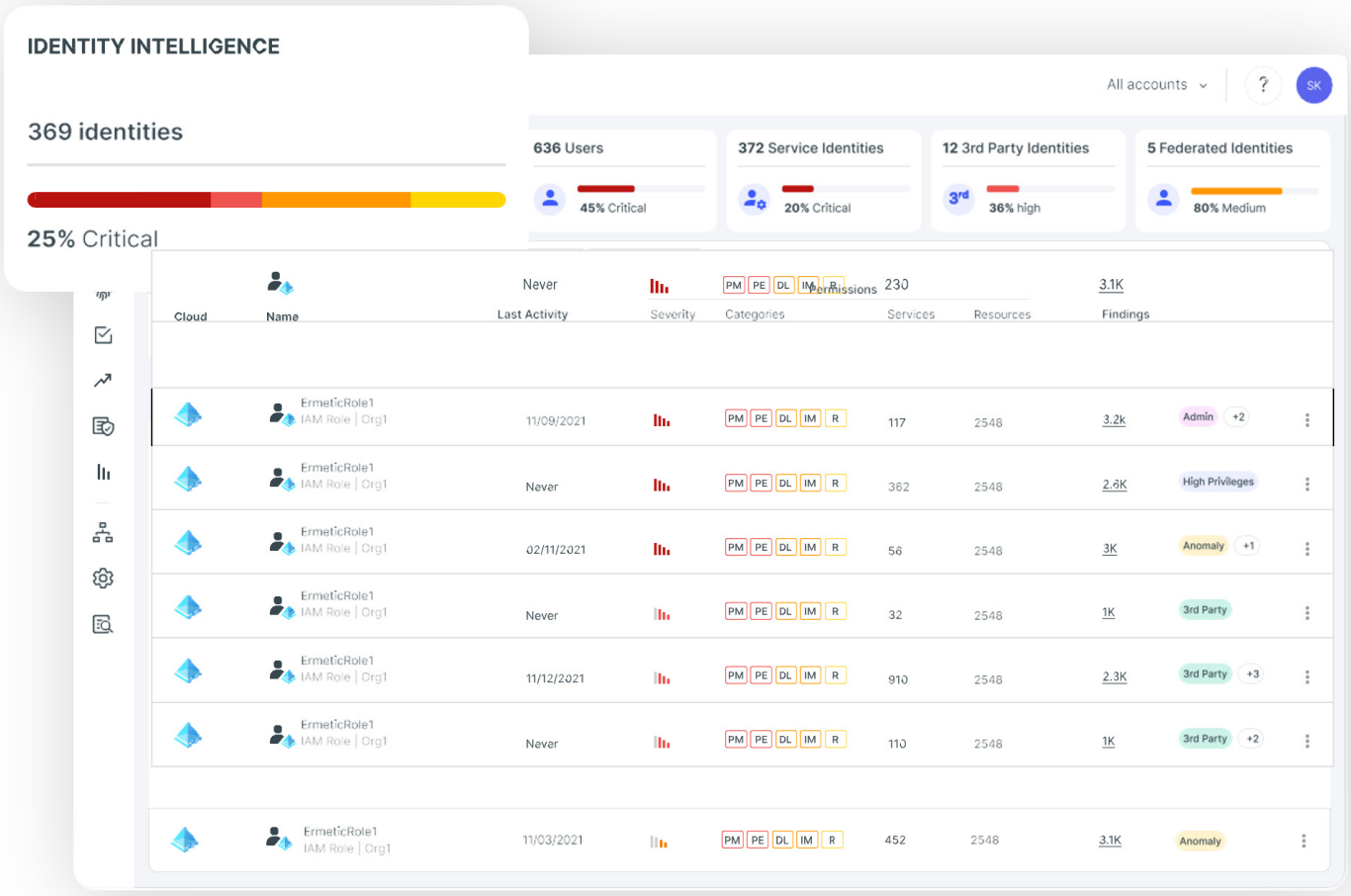


Findings view: start your day assessing and remediating the greatest permissions risks, reducing your organization's attack surface

Govern privileged identities

Tenable reveals all privileged identities in your cloud infrastructure by type, including user, service, third-party applications and federated identities from identity providers. It enables you to understand what a privileged identity is entitled to do, including its ability to manage permissions, leak data, modify infrastructure, escalate privilege and/or carry out reconnaissance — helping you assess if the identity is overprivileged.

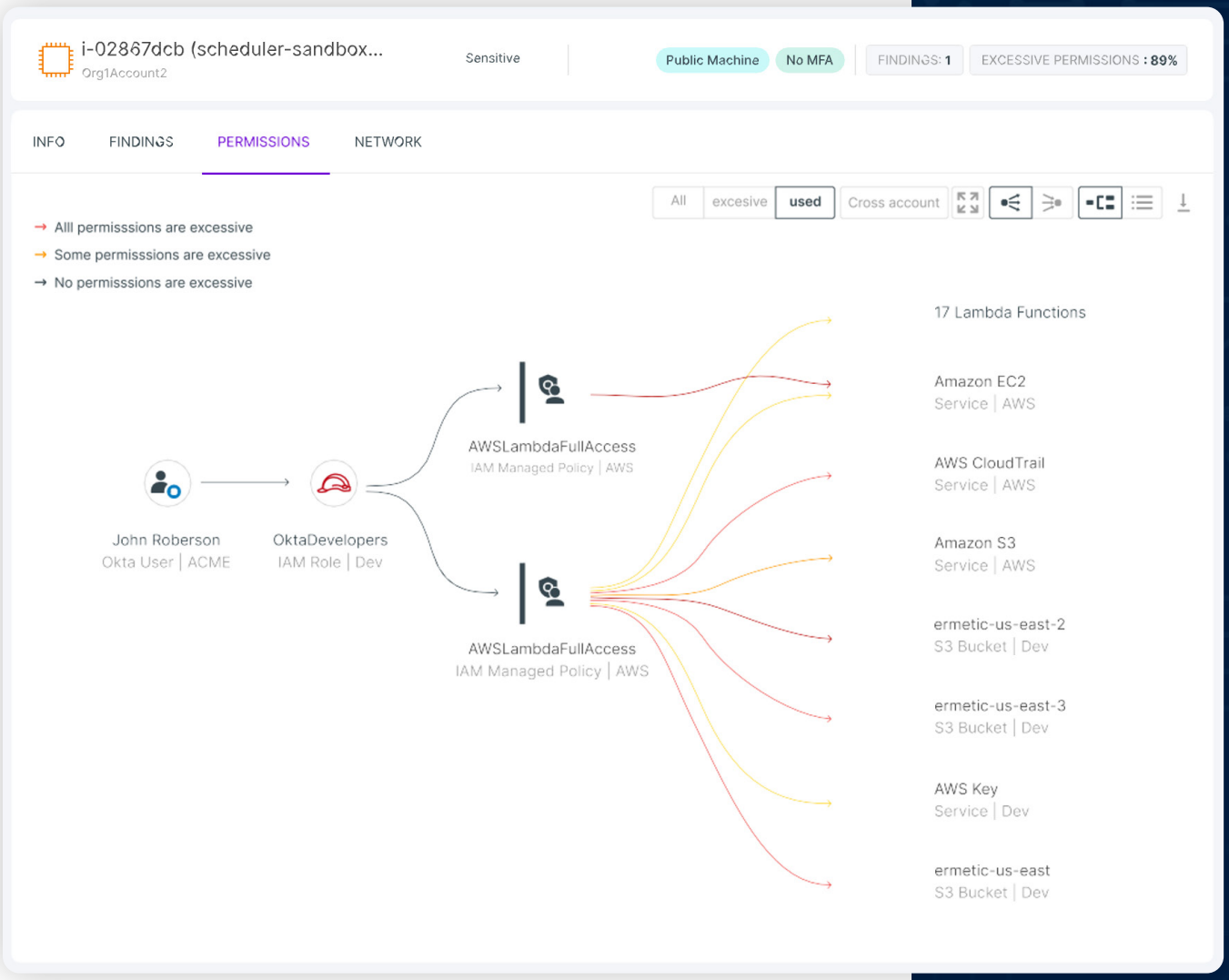
Tenable also gives details about an identity's risk factors, such as use of access keys and multi-factor authentication, and exposure of data to the internet or third parties. This enables you to govern privileged identities with efficiency and ease by monitoring them, eliminating their excessive entitlements and acting on an ongoing basis to minimize their risk of being compromised by an external — or internal — threat actor.



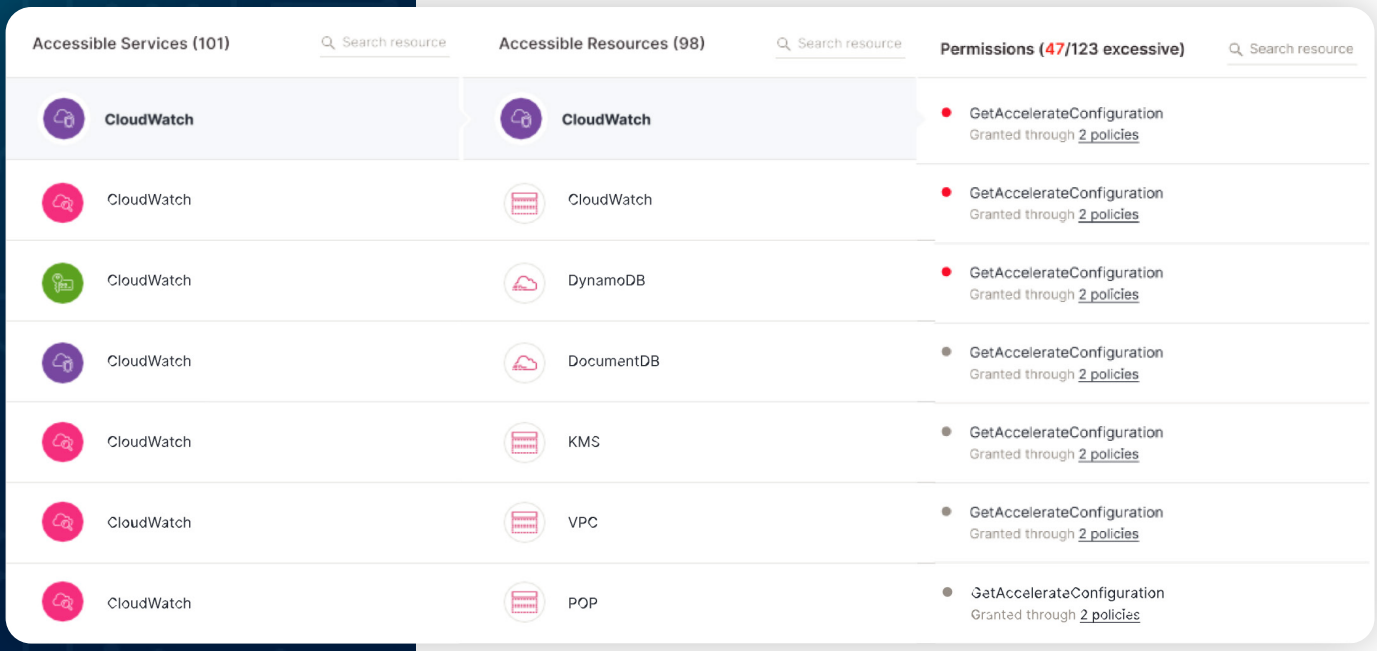
Identity intelligence view: Govern all privileged identities in your cloud infrastructure aided by deep and contextual insight into entitlements and risk

Review and certify entitlements

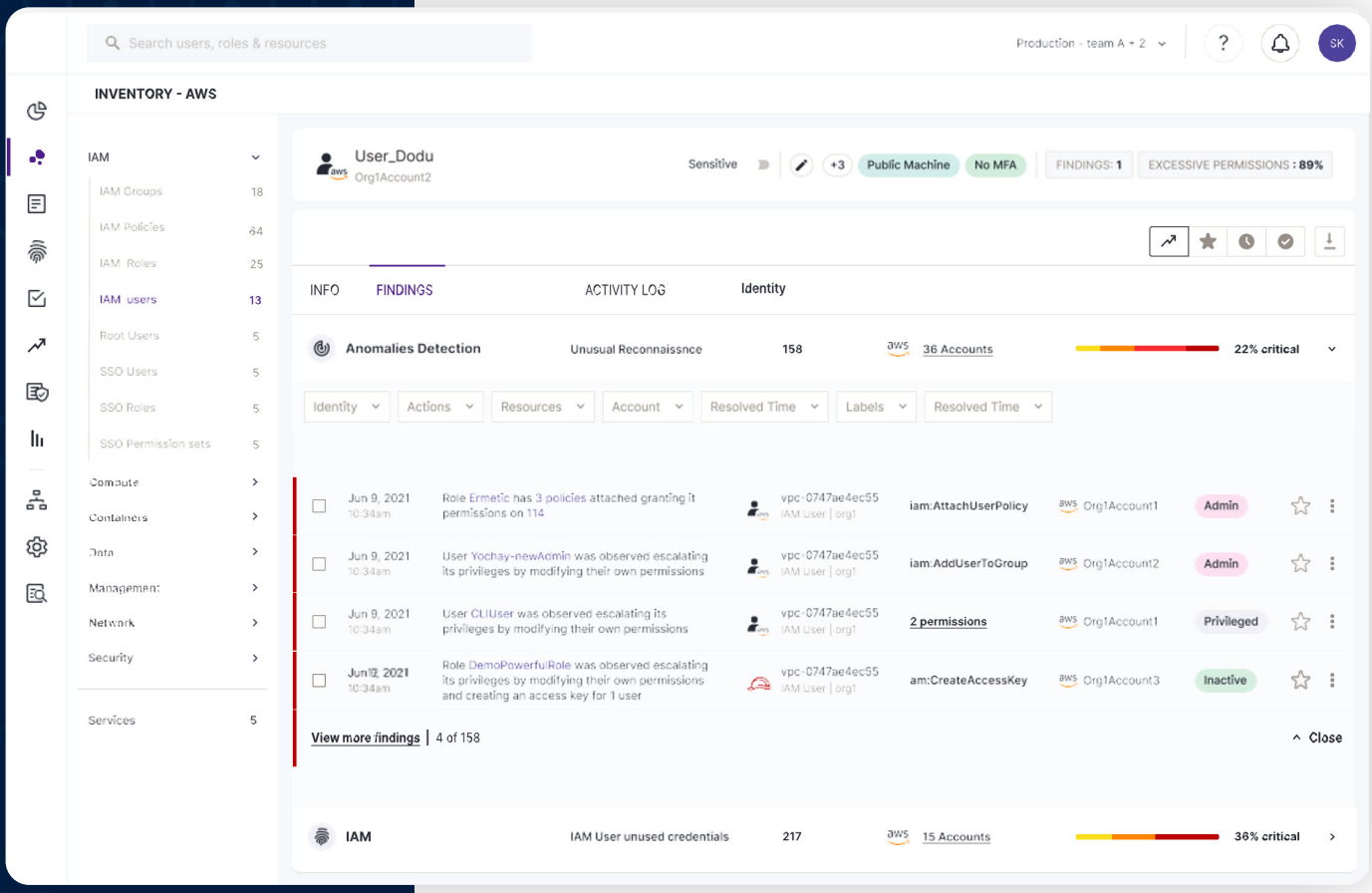
Tenable Cloud Security lets you deep dive into entitlements of specific entities, such as IAM role, user or group to determine if the assigned access is justified and to mitigate as needed. Tenable shows the entitlements for every identity at the most granular level of a specific resource or permission — far beyond the capabilities available in cloud-native tools like AWS Access Advisor or Azure Role-Based Access Control (RBAC). Tenable presents not just the general information for a specific entity but also a visual graph showing all the entity's permissions, color-coded for easy understanding of the extent to which permissions are excessive. You can assess the information and, importantly, review Tenable's findings of unnecessary or dangerous access, and execute recommended remediation steps at a click.



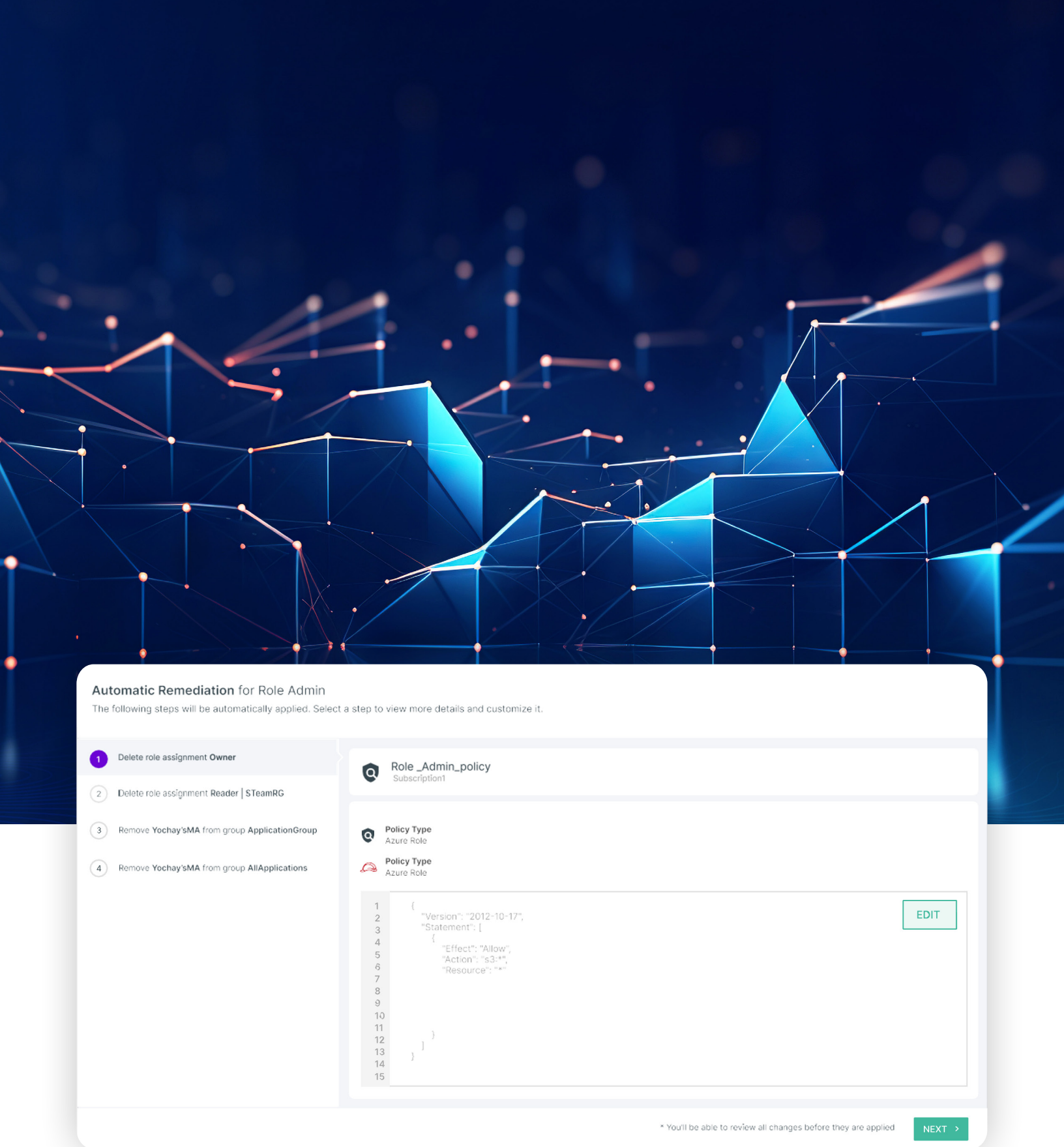
View entitlements by role and user, guided by color coding that shows excessive permissions by severity, filter for more detail, remediate at a click



See detailed entitlement information in list format; click on an item to drill down



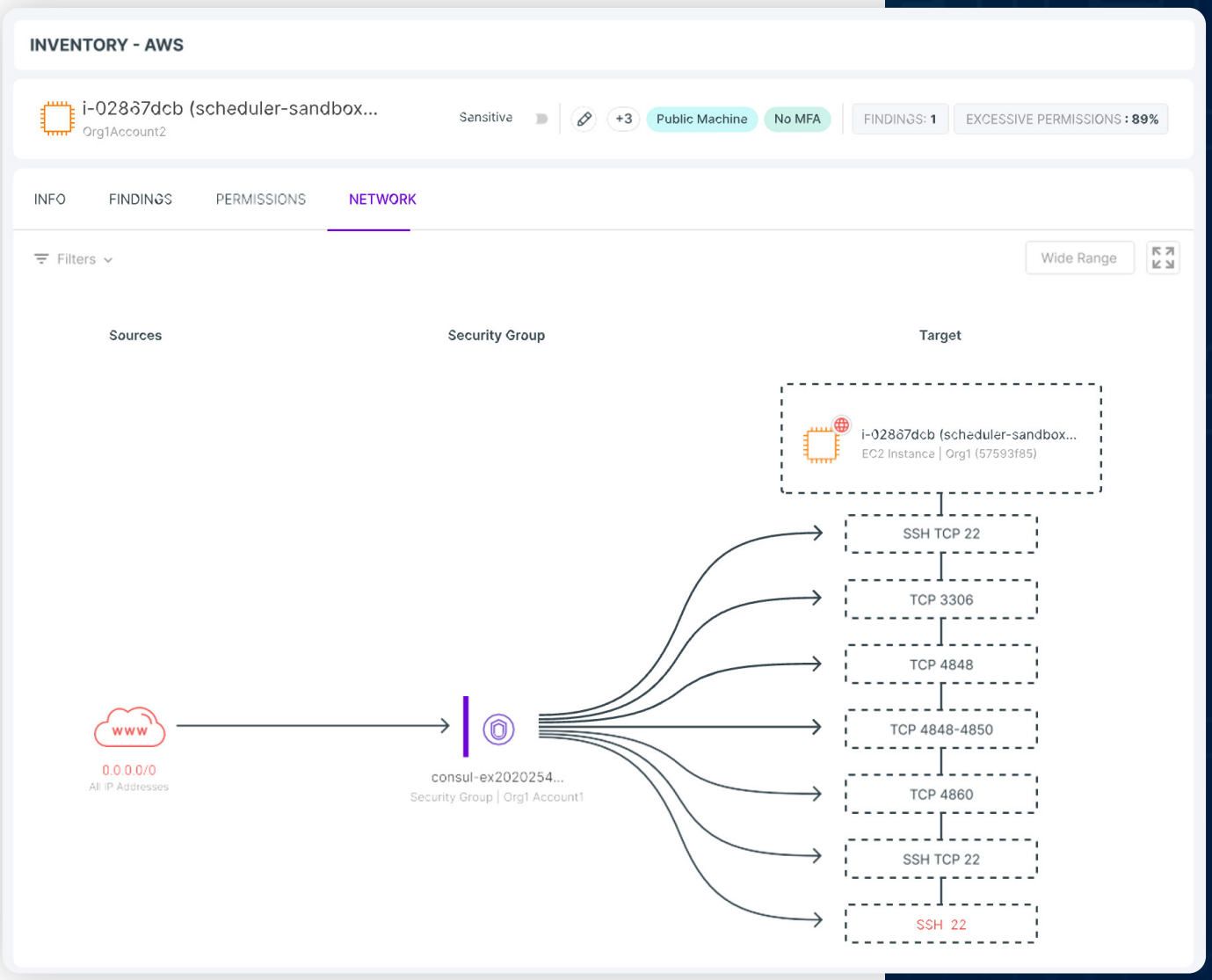
Review any role to understand why Tenable Cloud Security has defined an entitlement as risky or excessive



Follow easy steps for remediation

Detect and mitigate access to sensitive resources

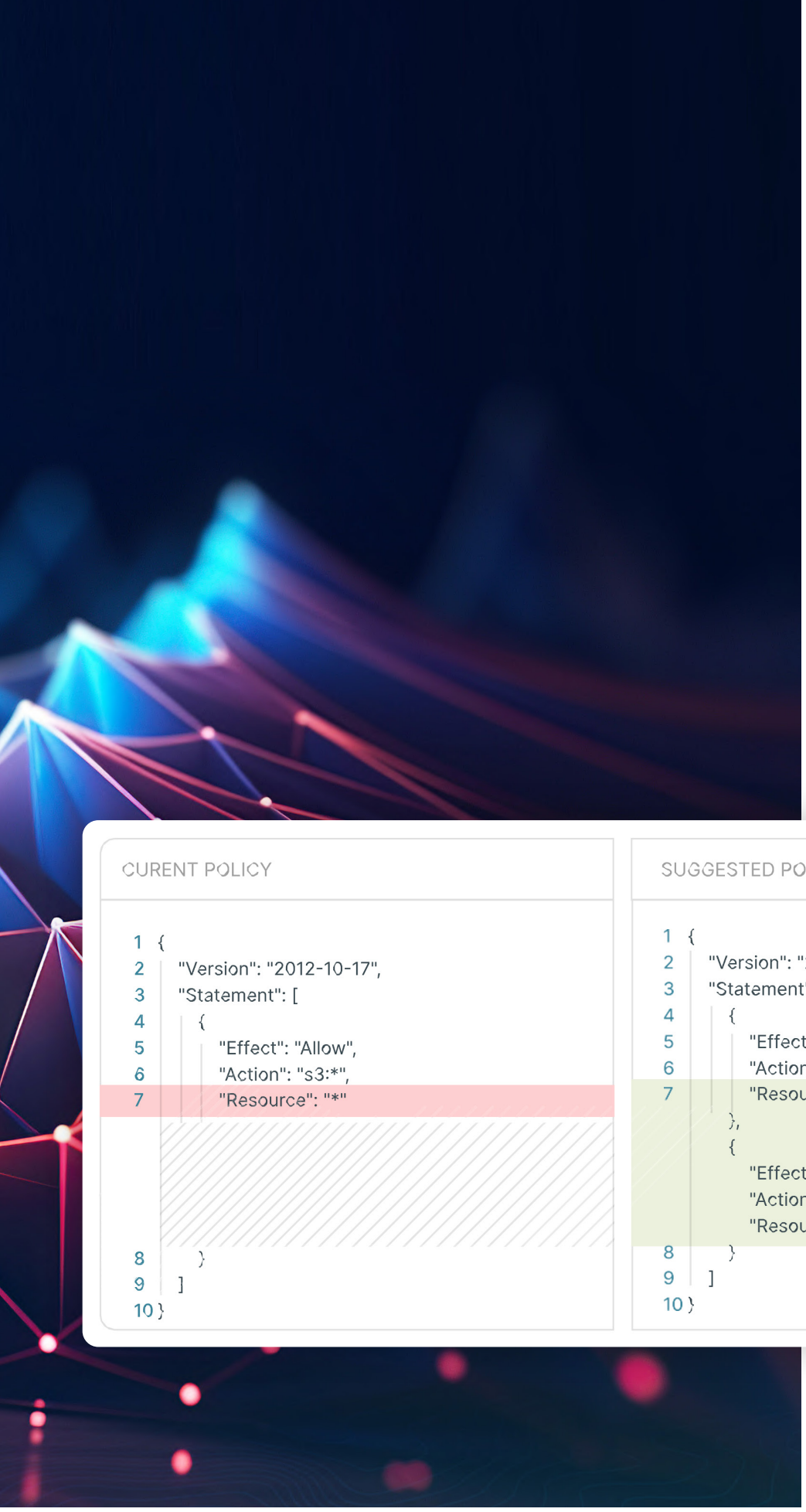
Tenable enables you to flag a resource — data, compute, security or management — as sensitive, and filter views to see which users and roles can access it, and if their permissions are excessive. It cuts through complexity to reveal network access and publicly exposed resources. It takes a multi-vectored approach to give a true assessment of risk. For example, Tenable detects if entitlements expose a database, yet the risk is low due to adequate network configuration protection. You can assess the information and remediate at a click, updating the policy to minimize the potential risk.



Detect and monitor risk in the context of a resource exposed to the internet and the security validity of its entitlements

Apply least privilege policies and automate remediation

Tenable analyzes data from cloud activity logs such as AWS CloudTrail to generate resource-level, least privilege policy based on actual usage. Tenable auto-remediates risky privileges and faulty configurations directly with wizards. You can also use Tenable to enforce least privilege policies across multi-cloud environments. Tenable enables you to ticket auto-generated, optimized policies and configuration fixes within your CI/CD pipelines (Jira, ServiceNow) and generate IaC snippets in Terraform and CloudFormation, accelerating your shift-left efforts.

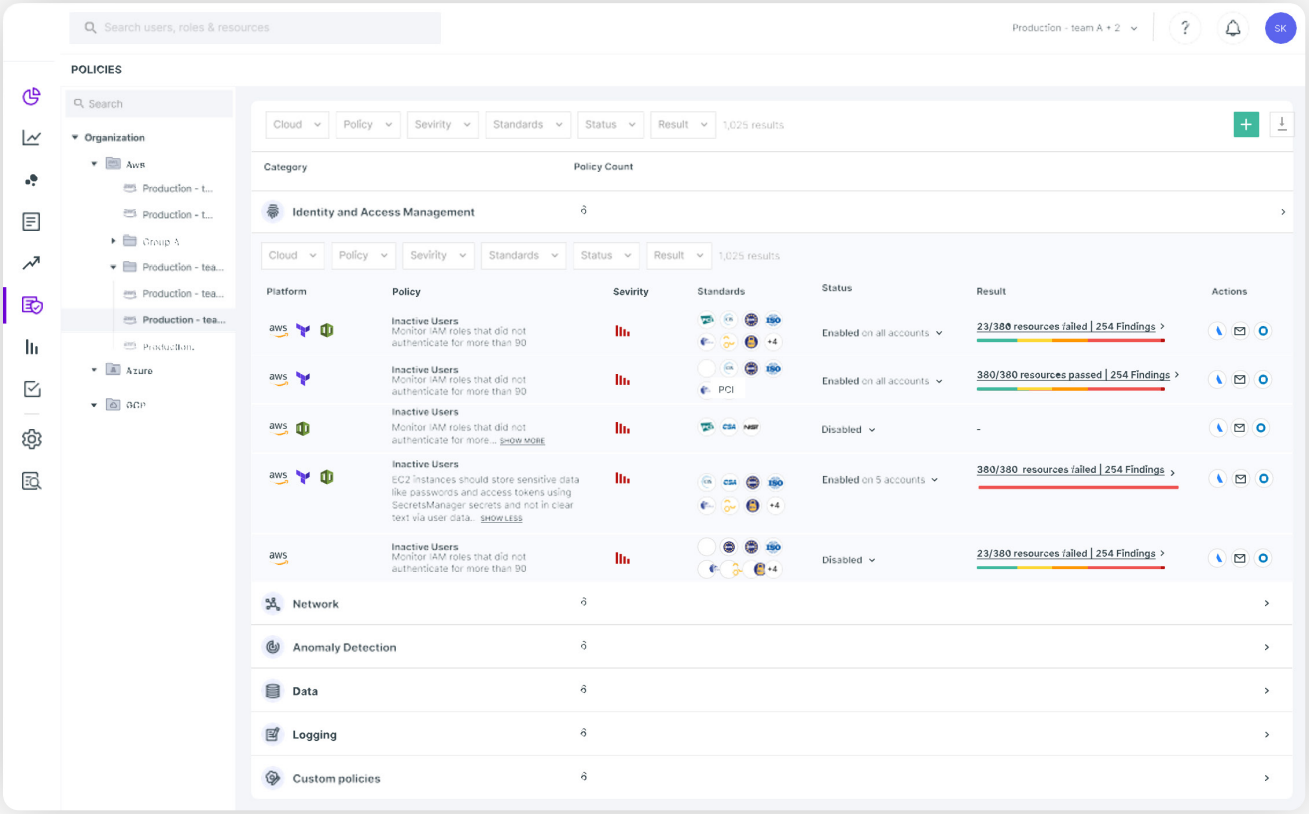


Remediate risky and excessive permissions with the automatically generated least-privilege access policy

Monitor and investigate anomalies and threats

Tenable improves your cloud security posture by tracking suspicious activity against behavioral baselines and making investigation easy. The solution detects anomalies in real-time and accurately determines potential threats, minimizing false positives. It brings together — and presents in context — activity data from multiple sources, including the access logs of your cloud providers, making anomalies easy to analyze and investigate.

Specifically, it detects unusual data access, privilege escalation and other identity-related threats, as well as changes in login settings, unusual reconnaissance and unauthorized use or theft of access keys. The solution identifies configuration anomalies related to network exposure, data security and audit settings. It analyzes every cloud provider log to reveal the identity behind an activity and affected accounts, resources and services. Enhance your access governance efforts through smart queries on these enriched, contextual activity logs. The solution also monitors user activity during elevated sessions — sessions for which permissions have been elevated for a predefined period of time — and generates reports detailing all just-in-time access requests and authorizations.

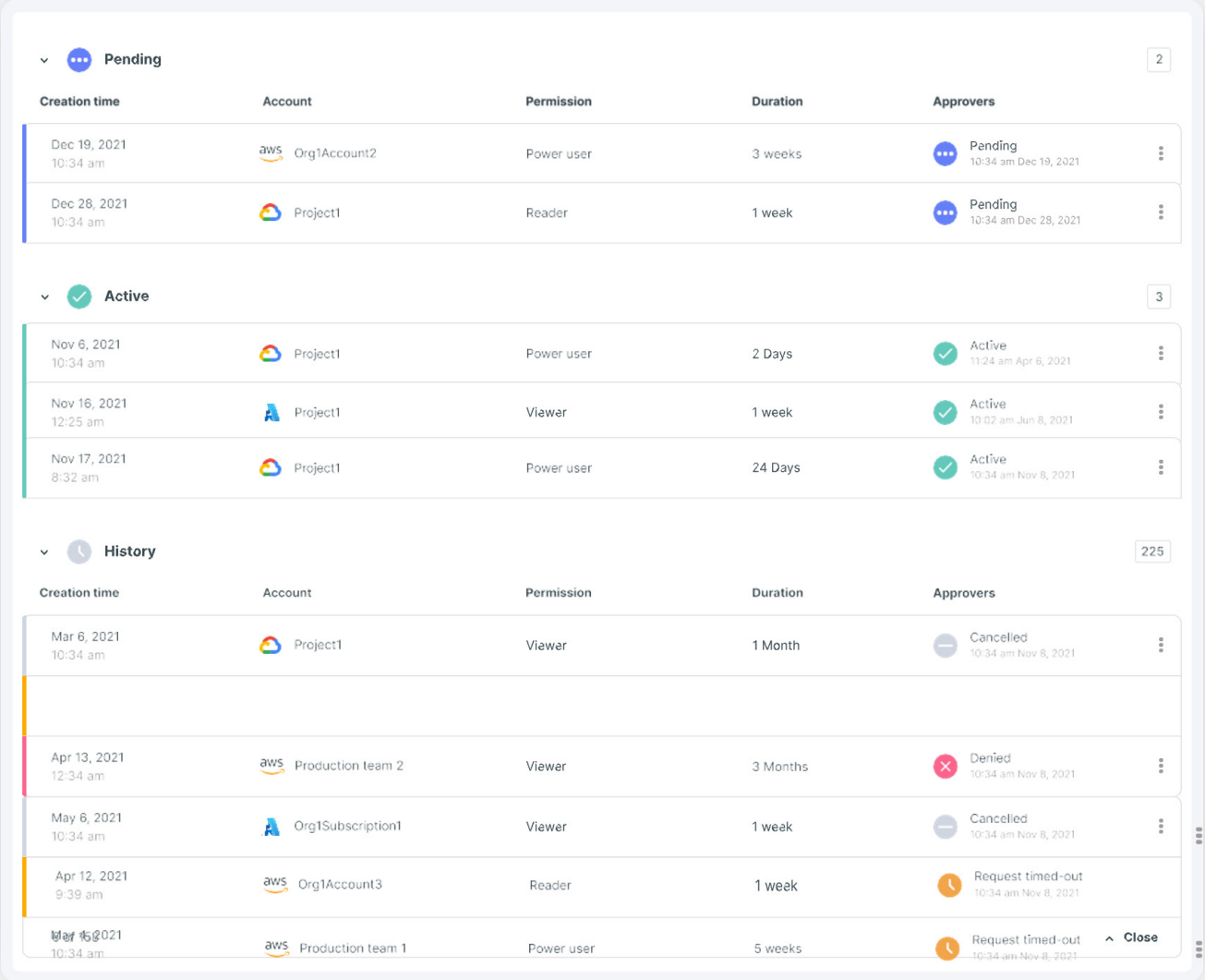


Detect anomalies and investigate unusual behavior, including reconnaissance, across date, networks and premissions

Simplify developer access control with self-service just-in-time (JIT)

Highly-privileged access to sensitive cloud environments is one of the biggest security challenges facing organizations today — and one that can quickly become a security and compliance nightmare. Your engineering teams are sometimes granted "always on" access when, in reality, they only need brief, intermittent access to get the job done. Tenable helps achieve and maintain zero standing privileges by providing authorized access for a predefined period of time, after which it automatically terminates access and revokes the temporary permissions.

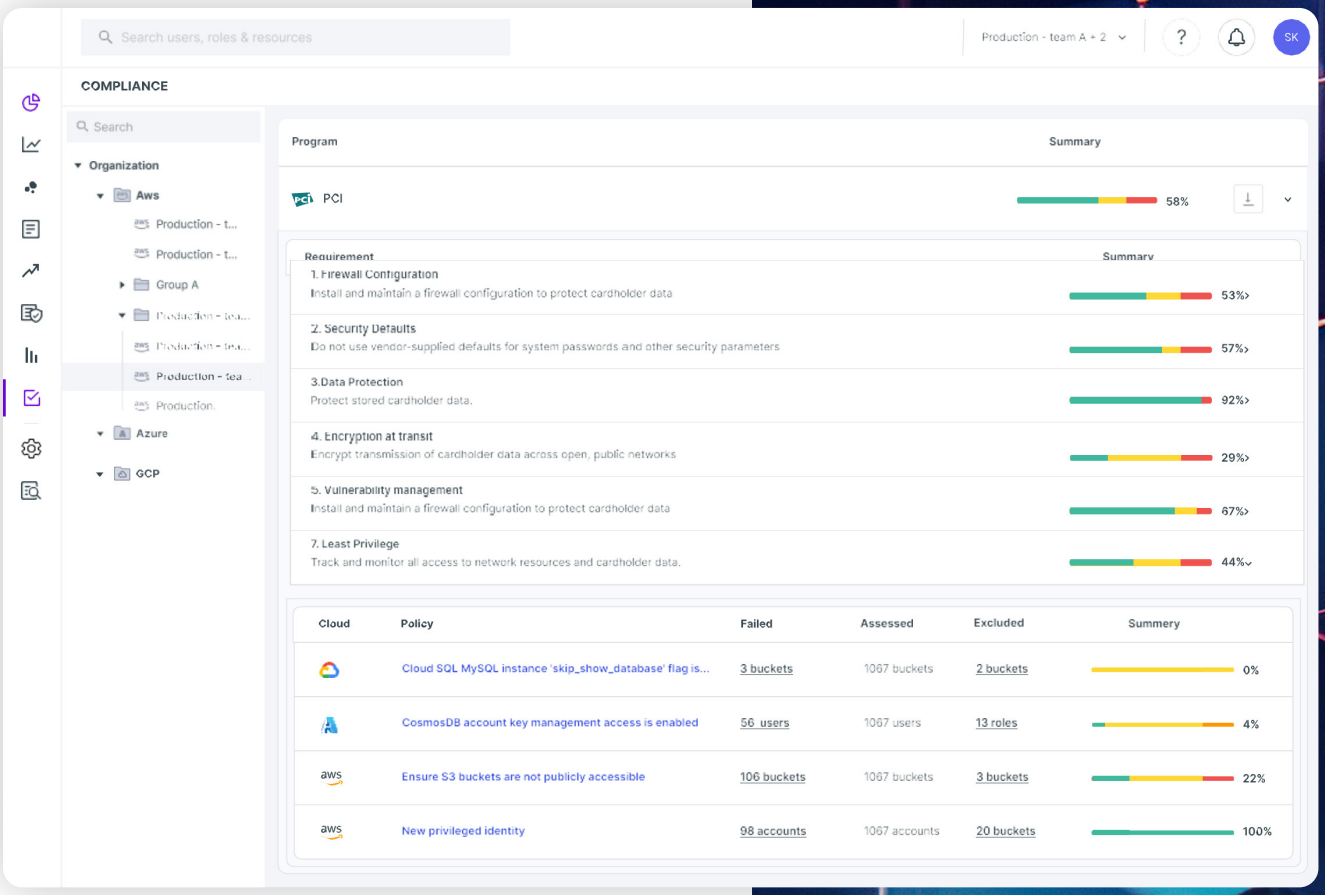
Using just-in-time self-service capabilities, developers can quickly submit a request — which automatically notifies the designated approvers — and gain temporary access. By granting access for the shortest amount of time needed for a user to complete a task, security teams can proactively enforce least privilege and dramatically reduce the risk of unrevoked long-standing privileges.



Drive and simplify least privilege based developer access with just-in-time control

Tenable for Cloud Security Posture Management

Tenable offers CIEM and robust CSPM in a fully integrated solution. It lets you manage your cloud asset inventory and compliance from a single pane of glass — and drill down into and auto-remediate misconfigurations.
The solution tracks how your organization scores against common industry standards and best practices including: GDPR, NIST, PCI DSS, HIPAA, ISO, SOC 2, AWS Well-Architected and CIS Benchmarks.



Detect misconfigurations, track compliance and report on your cloud security posture improvements

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com.

CONCLUSION

The complexity of public cloud infrastructure makes understanding the risk to your organization extremely difficult. Tenable provides an award-winning cloud security solution that offers leading CIEM and CSPM as part of a full Cloud Native Protection Platform (CNAPP). Organizations use Tenable to reduce their cloud attack surface and blast radius while reducing time and costs — and amplifying cloud security expertise for security and engineering teams.

Tenable is the only solution in its category to offer full-stack insight into entitlements across identities, compute resources, data stores and the network. This comprehensive view enables you to investigate deeply what is going on in your cloud infrastructure at any given time. Tenable helps you secure your cloud infrastructure effectively and automate least privilege based on actual use.

The Tenable One Exposure Management platform breaks down data silos across on-premises and multi-cloud environments, providing a 360 degree view of assets and exposure, including misconfigurations, vulnerabilities and excess privileges, which are the leading causes of virtually all breaches. With Tenable One, organizations can consolidate expensive point solutions, while gaining an actionable view of exposure for mission-critical business applications, data and processes. Armed with a quantified cyber exposure score, security leaders can prioritize investments and limited staff to maximize risk reduction and continuity of critical revenue streams.

For more information on Tenable Cloud Security and the Tenable One Exposure Management Platform, or to try them yourself, visit www.tenable.com/products/