tenable | Customer Story

Latch uses Tenable Cloud Security to automate least privilege for new services in AWS

Overview

Latch is focused on monitoring, maintaining and improving the security posture of their cloud environment. This includes identifying and coordinating the remediation of vulnerabilities, reviewing and consulting on cloud architectures, and developing tooling and automations for common security tasks in concert with security analysts and site reliability engineers (SREs).

Challenge

It was extremely important for Latch teams to gain full visibility into all of its AWS identities and any risks related to access permissions to the many AW services the organization was using. Among the risks Latch sought to understand was potential Internet exposure of any of its AWS resources.

Latch also aimed to integrate mitigation of such risks into its organizational workflows. Further, laser-focused on enforcing least-privilege principle across their cloud environment, servers, databases and SaaS platforms, Latch sought to leverage technology to bring least privilege efficiencies and accuracy to its site reliability team.

Solution

Tenable Cloud Security is an APN Advanced Technology Partner, ISV Accelerate and ISV Validated SaaS security solution that provides an easy understanding of potential cloud security risks that can lead to the breach of a client's environment. Tenable differentiates through granular visualizations and analysis of combined exploits like cloud misconfigurations and the over entitled access rights that machine or human identities have over IaaS or PaaS cloud infrastructures. In addition, Tenable enables remediation of these risks via IAM rights policy enforcement, allowing clients to focus and leverage an identify defined security strategy like the principle of least privilege or zero trust.

LATCH®

Latch makes spaces better places to live, work, and visit. Latch delivers a full-building operating system designed to help owners, residents and third parties like guests, couriers and service providers seamlessly experience the modern building. It has done this by digitizing building access and control platforms that combine software, devices and services with advanced technologies for smart building usage, control and connectivity to improve and heighten the occupant's experience, safety and convenience.

[Tenable Cloud Security] has saved Latch hours of time and the headcount equivalent of three to four additional analysts.

Latch is using Tenable Cloud Security to:

- Implement least-privilege access in its cloud environments
- Achieve granular visualization and analysis into risks associated with excessive permissions on AWS services
- Identify potential risk associated with AWS role access and public exposure of its AWS resources, and coordinate remediation
- Streamline security response workflow automation through Tenable's integration with technology partner solutions like Atlassian Jira and HashiCorp Terraform
- Enable its SREs to use auto-generated least privilege policies in AWS CloudFormation and Terraform templates to build secure AWS roles and policies into new services
- Automate periodic audits on all AWS IAM permissions, avoiding the expense of a third party Privileged Access Management platform

Using Tenable Cloud Security has enabled Latch's security analysts and SREs to continuously provide cloud security architecture reviews and easily automate the analysis of AWS IAM policies and permissions. Compared to the organization's legacy approach, this has saved Latch hours of time and the headcount equivalent of three to four additional analysts.

Latch's next steps with Tenable Cloud Security

- Latch plans to expand use of Tenable Cloud Security recommended policies in its CI/CD pipeline to further implement least privilege practice and remediate excessive entitlements.
- Latch seeks to leverage Tenable Cloud Security reporting to produce compliance evidence for audit requests pertaining to cloud infrastructure.
- Latch would like to consolidate their existing security tools and leverage Tenable's anomaly detection feature to proactively spot and mitigate AWS cloud security risks early on.

About Tenable Cloud Security

Tenable Cloud Security is the actionable cloud security platform (CNAPP), rapidly exposing and closing priority security gaps caused by misconfigurations, risky entitlements and vulnerabilities. These weaknesses are the epicenter of cloud risk. Tenable is a world leader at isolating and eradicating these exposures at scale across infrastructure, workloads, identities, data and AI services.

About Tenable

Tenable is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe. Learn more at tenable.com.

Contact Us

Please email us at sales@tenable.com or visit tenable.com/contact.