FORTINET

LawnStarter Gains Visibility with Automated Security from Lacework FortiCNAPP and AWS

LawnStarter founded its business with the goal of making lives and homes better by taking lawn care off its customers' growing to-do lists. The online, on-demand platform, built on Amazon Web Services (AWS), connects customers with insured and vetted outdoor service providers to schedule lawn mowing, tree care, landscaping, pest control, and many other outdoor services.

LawnStarter collects customer, provider, and payment data to determine accurate pricing, ensure quality service, and offer seamless transactions online. When a potential customer visits LawnStarter.com and enters an address, LawnStarter uses that data to determine the best pricing in the neighborhood. This data also helps LawnStarter organize its providers' routes by location, allowing them to do more jobs per day. After a provider completes a job, customers can rate the provider, and providers are financially incentivized based on the ratings.

A Growing Business Can Mean Growing Security Risks

As with many startup organizations, LawnStarter's initial focus was on acquiring and retaining customers and building for the future with security as an afterthought. That was the case when Alberto Silveira joined LawnStarter as the head of engineering. After conducting a manual technology audit, Silveira found that LawnStarter lacked visibility into its cloud infrastructure. There were no mechanisms in place to identify noncompliant resources, vulnerabilities, or anomalies.

LawnStarter also had a lean security team with limited knowledge of how cloud infrastructure was created and maintained efficiently.

With visibility into its AWS environment made possible by Lacework FortiCNAPP, LawnStarter gains the ability to proactively address emerging threats, maintain compliance, and increase its security posture. LawnStarter's lean team also gains actionable intelligence to manage security more effectively.

The Need to Embed Proactive Security within LawnStarter's Platforms and Culture

Silveira and his team sought support from Lacework FortiCNAPP to gain a view of LawnStarter's resources in the cloud to keep up with its share of the AWS shared responsibility model. Under the model, AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud, providing the highest levels of security possible and aligning with numerous compliance programs. As an AWS customer, LawnStarter is responsible for securing its resources in the cloud, keeping its content secure and compliant.

LawnStarter

Details

Customer: Lacework LawnStarter

Industry: Business Services

Location: Austin, TX

Business Impact

- Gained visibility into its cloud infrastructure
- Gave its security team actionable intelligence
- Reduced alert volume
- Identified compliance vulnerabilities that require remediation
- Encrypted 100% of its production database

Solutions

- FortiCNAPP

LawnStarter needed to quickly identify insecure and exploitable misconfigurations and regulatory compliance violations due to drift and misuse. Also, Silveira wanted the ability to embed security across LawnStarter's software development pipeline to allow those with less security knowledge to build and deploy secure code.

Shifting Security to the Left with Lacework FortiCNAPP

Silveira's overarching vision for LawnStarter was to build a "one team, one heart" culture where security became everyone's responsibility, not just the security team's. This aligns with the DevOps practice of shifting security left, or earlier in the application development cycle.

The Lacework FortiCNAPP data platform provides LawnStarter with progressive layers of protection by embedding security at multiple stages of its software delivery life cycle from build to production. For development teams, embedded and automated security means they can confidently accelerate development cycles.

LawnStarter uses container images to build its infrastructure, so the Lacework FortiCNAPP team helped LawnStarter integrate its Docker Hub container registry into the platform to gain visibility. Lacework also shared best practices for viewing and using the container vulnerability data within the platform, such as sorting and grouping the data. The ability to identify unexpected risks and threats much earlier in the development cycle gives LawnStarter a greater understanding of where issues happen so the team can build more resilient infrastructure.

Proving and Maintaining Continuous Compliance

The platform allows Silveira and his team to protect its data, and that of its key stakeholders, by continuously scanning LawnStarter's cloud environments for misconfigurations.

Lacework FortiCNAPP automatically discovers and catalogs users, services, security groups, and secrets that are active within LawnStarter's AWS environment and compares them against industry frameworks and compliance requirements. LawnStarter can quickly pull customized reports created by Lacework FortiCNAPP to see which resources are compliant.

As a result, LawnStarter has seen a 75% decrease in compliance violations over the past year, saving the company significant time and money. LawnStarter now has a robust compliance practice that is essential to earning and maintaining trust with customers, providers, investors, and advisors.

F:RTINET

www.fortinet.com