Ecolane

Ecolane Digital Safety and Security Features

We have a dedicated, around-the-clock security team at Ecolane. They're responsible for not only protecting your data and mitigating threats — but for diving into emerging research and determining the best course of action for current and future security updates. Our current team has a target response rate of 1 hour for critical issues and up to 24-hours for medium-tier issues. This means that we expect to deliver a solution to critical disaster recovery tickets within an hour. While we have industry-standard criteria that dictate the criticality of service issues, we also employ several automated security measures to reduce the day-to-day security frictions that almost every business on the planet is currently facing.

Over the past few months, we've been in the process of migrating critical customer data to our new Amazon Web Services (AWS) servers. Amazon Web Services is the world's largest cloud platform. With over a million servers scattered across the globe in 28 available zones, AWS is utilized by some of the largest brands, governments, and military entities across the world.

As cloud becomes the new normal in security, our team has invested in cloud-based and Software-as-a-Service (SaaS) solutions to help provide additional safeguards against data breaches.

Today, we're going to cover both the existing solution that helped us neutralize the digital attacks thrown our way in 2019 as well as our new AWS solution that will help us continue to keep our customers safe, secure, and happy in the Ecolane ecosystem.

AWS Security Features

Did you know that 4.1 billion on line records were exposed to attack in the first half of 2019 alone? Hackers try to attack businesses every 39 seconds on average — leading to a massive $2 trillion cost to businesses across the globe.

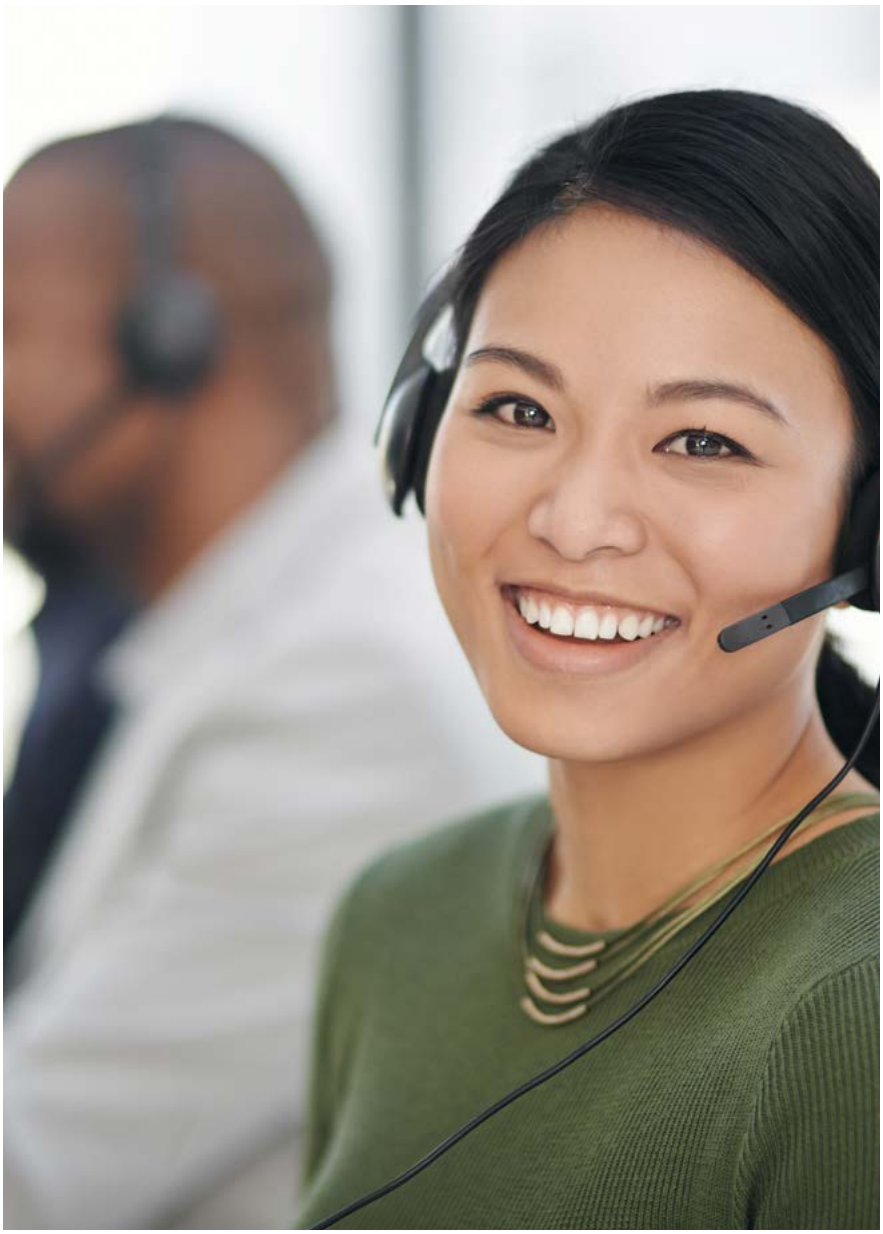
At Ecolane, we're committed to providing best-in-class security to our full range of transit providers and drivers. Our incredible suite of security features has helped us endure this era of cyber instability, and we're committed to continuously upgrading and updating our systems to keep them at the front of the cybersecurity landscape.

Each day, drivers and transit providers across the country entrust us with their safety-sensitive and HIPPA compliant information which is mission-critical for agencies of all sizes. From vehicle monitoring and dynamic navigation to real-time schedule dispatching, vehicle locations, passenger data, and invoicing, our full-service demand response transportation and on-demand solutions utilize your data to provide real-time insights and unparalleled automation and optimization.

As the threat landscape continues to grow, and as consumers become more alert to how they share their privileged information to companies, we want to touch on our robust security features that allow us to keep your precious data safe and secure.

Ecolane's AWS Solution

This year, we've migrated resources to Amazon Web Services (AWS). Not only does Amazon's incredibly powerful cloud environment help bolster our security posture, but it will reduce infrastructure headaches for our security staff and help us continue to provide best-in-class speeds and performance for our clients. We won't cover some of the key operational benefits of AWS. Still, it's important to note that Amazon's flexibility, elasticity, and overall scalability will provide the framework we need to continue to expand, grow, and improve our automation and routing capabilities.



We Care About Your Data Security

You trust us to provide real-time scheduling and optimization for your routes and dispatches. We work tirelessly to ensure that trust is well earned. We're happy to announce our recent migration to AWS servers to further bolster our security posture. We've joined the +1 million other companies that rely on AWS to scale their servers and enhance their security presence. But it doesn't stop there. In the future, we'll continue to disrupt our security practices and innovate to help keep your data safe. Dispatching has never been safer, easier, and faster. Let's hit the roads and make a difference, together.

Are you ready to eliminate manual processes in your on-demand transportation scheduling, dispatching, and reporting?

Understanding AWS Security

AWS operates in a “shared security” ecosystem. Ecolane is responsible for ensuring that data is transmitted appropriately to AWS servers, and we’re certainly still the party responsible for keeping all of our clients’ critical data safe, secure, and healthy. But AWS is also responsible for infrastructure security. With global banks, massive government entities like the DoD, and major organizations like LinkedIn, Facebook, and BBC, AWS is responsible for maintaining the best cloud security posture in the world.

Not only does AWS have a wide range of cloud security tools backed by world-class security experts, but they also offer over 230 security and compliance capabilities and conform to 90 security standards and policies (including GDPR, HIPAA, FedRamp, and ISO standards). At Ecolane, we use DevSecOps and AWS Well Architectured Framework to create security workflows across four primary pillars:

Prevention

With AWS, we can granularly control access policies to hyper-control how data is consumed on our servers. At Ecolane, we implement least-privileged policies — meaning that our security team and staff are only able to access the data that’s immediately necessary for their day-to-day workflows. We back this highly-secure practice with best-of-breed security automation monitoring software that immediately detects security events across our AWS environment.

In addition, the AWS infrastructure already provides surface-level security with multiple layers of data encryption, incredible on-premise data site physical security, and enterprise-class firewalls, climate control, power backup, and fire suppression. AWS also provides automated backup across regions, giving us unparalleled up-time support. If a server crashes, we’re back online almost instantly in another region while the issue is remediated.
At Ecolane, we believe that preventative security is the best security, and we work tirelessly to ensure that all of our data is maintained and secure at all times.

Detection

In addition to ensuring that we exceed industry-standard security prevention, we also utilize a variety of third-party security automation tools to help us detect any issues immediately. We are able to ingest security incident data into fully automated security systems immediately, and leverage that data to tackle any potential pain points before they become issues.

Ecolane has centralized logging and reporting features, vulnerability analysis capabilities, and a policy framework that helps us maintain best-practice policy control and user identification across our server environments.

Rapid Response

Of course, having a response team in the case of emergencies is an absolute necessity in today’s threat landscape. Not only have we migrated our world-class security response mechanisms to our new AWS servers, but we now leverage a plethora of automated incident response tools to help us discover and visualize threats immediately. Once a threat has been contained, our team can immediately begin root-cause analysis to find out where the problem came from, how it happened, and how it can be prevented in the future.

New threats happen every day. The security world is in a constant state of flux, and threat actors employ new attack strategies constantly. We want to be in front of the problem. While our existing security posture has kept our client data safe-and-secure in the past, we want to ensure that we take every possible step to keep it that way. Your data security is our business. You keep driving; we’ll keep the routes flowing and your driver data under a warm, safe blanket.

Remidiation

In the past, we’ve relied heavily on our amazing security team to remediate issues. Now, we also rely on event automation to remediate issues in real-time. If an issue bypasses all of our firewalls, policy frameworks, security automation solutions, and physical security, we can immediately begin employing real-time remediation efforts in conjunction with our on-premise security team’s efforts. This provides an additional layer of remediation should we ever need it.

List of Companies Who Have Migrated to AWS

You may be asking yourself, which companies have switched to AWS?
Here is a list of ten top companies who use the AWS:

We're in pretty good company, don't you think?

Make the switch to Ecolane today.

Ecolane

Please visit
www.ecolane.com
for more information
on our company and
products.