Bloomip

Enervee Case Study Client:

Enervee delivers the world's most advanced suite of applications and services to energy providers, engaging residential customers in intuitive energy-smart purchasing decisions for their home. Users are provided an Enervee Score® to rate the energy efficiency of comparable products. Enervee has expanded their appliance and electronics categories to include lighting, smart home devices, along with a recent release of Enervee Cars, all to help consumers make energy-efficient purchases that fit their lifestyle. Enervee saves their users money, while transforming the consumer market for efficiency and clean energy.

https://enervee.com/about/

Context:

Enervee provides utility partners with a marketplace where end users can search for appliances and electronics, with the Enervee Score®, user ratings, price, and retailer availability, helping users make informed purchase decisions.

Enervee enables users to choose products ahead of their purchase and setup price tracking with notifications for products in each category, allowing the consumer to save money. Enervee also connects consumers with available rebates, including utility rebates. The rebate application process is simplified and reduces application time to minutes via the Enervee platform.

Enervee is the global leader in using data to deliver simpler and better choices at scale. The Enervee Score® ranks products on their energy performance. Updated daily, the Enervee platform drives unmatched buying behavior change and influences millions of purchases a year.

https://enervee.com/

Challenges:

In order to link users to available rebates, Enervee receives and stores purchase information, including personally identifiable information. This information needs to be received, stored, and processed in a secure manner in accordance with all necessary data safety requirements.

The utility partners that leverage the Enervee platform have compliance requirements and conduct regular in-depth audits to ensure these requirements are continually met. Policies and procedures must be in place, and the technology implementation must comply with requirements across NIST 800-53 and GDPR.

As the Enervee platform grows, and new users, products, and partners are added, the application and underlying technology must scale with that growth. As the infrastructure

and application scale, it must also maintain all necessary security and compliance requirements, while providing performance, for a high-quality end user experience.

Solution:

Bloomip built a compliant infrastructure inside of Amazon Web Services, according to best practices, solving 6 areas of challenge: authentication, auditing and logging, encryption, automation, perimeter network protection, and malware protection.

Bloomip leveraged Fortinet's Fortigate platform for Perimeter Network Protection enablement, inside of the AWS platform. This extends the simple inbound and outbound firewalling that is typically provided by AWS Security Groups to also enable SSL VPN, IDS/IPS, Policy Logging, and the full feature set provided by FortiOS. Enervee and Bloomip have extended the protection offered by Fortigate on AWS to additionally protect other AWS offerings such as RDS, Amazon Redshift, and ElasticSearch, allowing these resources to be accessed over SSL VPN, and to be access controlled with IPv4 and IPv6 policies.

Leveraging an Identity Management solution, Bloomip implemented Multi-Factor, Centralized, SSO for the entire infrastructure, and enabled use of the directory service to extend to other areas of Enervee's organization, for cases such as VPN, administrative access, and other secondary applications.

SIEM and AWS Cloudwatch work together to ingest logs from the AWS resources, as well as from the application and other infrastructure sources. Through access control policies, Enervee and Bloomip have enabled the development team and other organization departments to view and process logs relevant to their area of interest, securely, while retaining these logs for future compliance and audit purposes, thereby satisfying controls of several compliance standards.

The application stack operates on instances configured according to the Center for Internet Security's Benchmark for Enterprise Linux, ensuring a hardened baseline, upon which the application is deployed. Bloomip and Enervee have worked together to perform most operations in the infrastructure via an automation platform, and have collaborated to mesh SiteOps,

DevOps, as well as other areas of the Software Development Lifecycle together, achieving seamless integration, and consistent, reproducible, security-hardened results. This ensures that all past, current, and future elements of the technology stack comply to the same standards and enables rapid development and implementation.

Result:

Enervee continually passes all client audits with no remediation, and satisfies new client requirements with ease. Their development team is able to rapidly prototype, test, and deploy their application, while their users enjoy a secure, scalable application that continues to grow in functionality and reach. This has directly resulted in cost savings,

lower energy usage, and an awareness of energy efficiency across a growing selection of product categories.

Ready to Bloom?