anchore

Case Study

Cisco Umbrella for Government is a cloud-native security solution tailored to meet the unique security and compliance needs of government agencies. It integrates multiple security functions into a single, easy-to-manage solution, ensuring comprehensive protection across various environments, including remote work settings.

Cisco at a Glance

San Jose, CA

www.cisco.com

Industry: Network infrastructure

Revenue: $57 billion USD | F100

Challenges

- Meet all 6 FedRAMP vulnerability scanning requirements
- Maintain and automate STIG & FIPS compliance for Amazon EC2 virtual machines
- Integrate end-to-end container security across CI/CD pipeline, Amazon EKS & Amazon ECS
- Meet SBOM requirement for White House Executive Order (EO 14028)

Solutions

Anchore Enterprise secures the software supply chain with:

- Distributed container security scanner
- Automated policy engine (security & compliance evaluation and enforcement)
- Turnkey SBOM generation and management
- On-prem cloud deployment model

Results

- Achieved FedRAMP, FIPS and STIG compliance in weeks versus months
- Reduced implementation time
- Improved developer experience by integrating directly into existing workflow
- Future-proofed compliance against anticipated requirements

Introduction

Cisco Umbrella is an AI powered cloud security platform that delivers a holistic security suite for enterprises. This includes security service edge (SSE), cloud application security, endpoint protection and incident response services to defend organizations from internal and external threats. Cisco Umbrella manages a complex environment with a number of different compliance requirements. They utilize AWS GovCloud to provide their services to federal agencies and need to meet FedRAMP, FIPS, STIG and EO 14028 compliance for their entire GovCloud deployment.

Build and deployment environment:

- *AWS Code Pipeline*
- *AWS Elastic Container Registry (ECR)*
- *Amazon Elastic Kubernetes Service (EKS)*
- *Amazon Elastic Container Service (ECS)*

Challenge

FedRAMP compliance is table stakes for the Cisco Umbrella organization in order to serve their customer base. Over the past decade FedRAMP has become more complex and comprehensive—its high impact level has over 400 controls alone.

The challenge was ensuring Cisco Umbrella's complex cloud infrastructure met all of the relevant compliance objectives and maintained compliance over time. Of particular concern was securing the software supply chain for container vulnerabilities that could potentially leak into their applications via 3rd-party dependencies.

In order to achieve FedRAMP compliance, Cisco had to meet the following 6 vulnerability scanning requirements for containers:

1. Hardened and compliant container images
2. Automated build pipeline with policy enforcement
3. Vulnerability scanning in the build pipeline and container registry
4. Security sensors to prevent malware in the pipeline, registry, and in production
5. Container registry monitoring with notifications on non-compliant images
6. Asset management with a full inventory of containers in production

Additional high-security requirements

Furthermore to meeting FedRAMP compliance, Cisco Umbrella's container vulnerability scanning solution is also required to be deployed into a High-Security environment. This came with the additional requirements that:

- STIG compliance for compute infrastructure
- FIPS compliance for compute infrastructure
- EO 14028 compliance for software supply chain

Solution

Cisco Umbrella selected Anchore, the leading software supply chain security platform specializing in container security, vulnerability management and the automation of compliance standards to solve their challenge. Anchore Enterprise integrated seamlessly with Cisco's existing infrastructure and empowered them to meet all six FedRAMP requirements for vulnerability scanning and the additional STIG, FIPS and EO 14028 compliance within the project deadline that was only weeks out.

Proactive vulnerability detection

After Cisco Umbrella integrated Anchore Enterprise into its developer's workflows, engineers were able to proactively uncover vulnerabilities at the time of development. This saved hours of developer time by alerting them to problematic dependencies before they began writing application code that would need to be remediated at deployment time.

Save time with built-in policy packs

Cisco Umbrella takes advantage of Anchore Enterprise's built-in FedRAMP compliance policy pack to evaluate each scanned container for FedRAMP compliance. With the pre-build policies the Cisco Umbrella team can focus on resolving the non-compliance rather than translating NIST documentation into software checks. Anchore's policy engine manages the process of evaluating a container against these policies and returning a PASS or FAIL signal back to the CI/CD process that then either gates the deployment or allows it to continue through the pipeline.

Automated security data management

As with many modern DevSecOps platforms, Cisco Umbrella also generates hundreds or even thousands of containers daily. Complying with EO 14028 requires an SBOM for each container. This quickly becomes a data management nightmare. As a turnkey solution, Anchore Enterprise includes a complete SBOM management solution to store and analyze this security data. This saves the security team time from having to manually collect and manage the data.

Simplified compliance via inheritance

Different from most cloud-based security solutions, Anchore Enterprise is deployed on-prem within a customer's own cloud environment. The key advantage is that customers have full control over the system and can inherit the underlying compliance standards that the cloud provider has achieved. This is how Cisco Umbrella was able to take advantage of the FedRAMP compliance aspects of Anchore Enterprise without jeopardizing the FIPS compliance that their cloud infrastructure provider had achieved. This isn't possible with traditional SaaS-based cloud security providers and is a unique advantage that is valued by Anchore's enterprise and public sector customers worldwide.

Outcome

Cisco Umbrella was able to significantly reduce implementation time of FedRAMP compliance requirements. The time to compliance was reduced to weeks versus the more typical months. The team was able to overcome 4 compliance hurdles in parallel; FedRAMP, STIG, FIPS and EO 14028. The security team improved developer experience for container security vulnerability by integrating directly into existing development workflows. This both reduced the friction of security testing and enabled developers to discover vulnerabilities in development rather than production. Finally, Cisco Umbrella has ensured compliance with anticipated requirements. This increased confidence that there won't be unexpected compliance work in the future.

If you're looking for a technical deep dive into the architecture that powered this outcome, Anchore in partnership with Amazon Web Services (AWS) co-authored an article that walks you through all of the details. You can find it on the AWS Partner Network (APN) Blog at this location:

https://aws.amazon.com/blogs/apn/achieving-fedramp-compliance-with-anchore-on-aws-for-cisco-security-cloud/

About Anchore

Anchore enables organizations to speed digital transformation and reduce risks by streamlining the development of secure and compliant cloud-native applications. Anchore's solutions integrate with existing DevOps toolchains to automate security and compliance checks throughout the software development lifecycle. Organizations can reduce costs and accelerate time to market by remediating security and compliance issues early and continuously. Headquartered in California with offices also in Boston and the UK, Anchore's customers include large enterprises and government agencies that require secure and compliant cloudnative applications.

anchore

sales@anchore.com

anchore.com