AppOmni

PARTNER CASE STUDY

Castle Ventures Protects Financial Services Data for Fortune 1000 Companies

INDUSTRY
Cybersecurity Services

EMPLOYEES
20

HQ
Morristown, NJ

DEPLOYMENT
AppOmni SSPM Platform

USE CASES
Data Protection
SaaS Security Posture Management
Data Security
SaaS-to-SaaS Cyber Risk

ABOUT CASTLE VENTURES
Castle Ventures is a cybersecurity consulting and managed services provider focused on data protection services for Fortune 1000 companies. Although the firm's clients are overwhelmingly situated in the finance and healthcare verticals, it also provides data security services to companies across industry verticals. Castle Ventures offers managed cybersecurity services, builds bespoke cybersecurity solutions, as well as identifies and remediates cybersecurity vulnerabilities.

APPOMNI'S IMPACT

- Comprehensive **SaaS and data security coverage**
- Consolidated approach to **security across multiple SaaS apps**
- SaaS security **configuration management at scale**

"People are understanding that their data, including lots of valuable data, is in more places than they originally thought.

Arthur Hedge
President, Castle Ventures

appomni.com

The Challenge

Castle Ventures has been a pioneer in the data security space, working with organizations of all sizes and across industry verticals. All their engagements center on the core focus of "what is going on inside the business" from a data security vantage point.

With 20 years of cybersecurity experience, Arthur Hedge, President of Castle Ventures, is finally starting to see an awakening among the industry on the risks that ungoverned SaaS data sprawl represents. "People are realizing that their data is in more places than they realized," states Hedge. As SaaS service providers now cater to all areas of the business — including CRM, file storage, and human resources management to name just a few — more and more organizations are adopting SaaS services for these core business functions. In the majority of cases, cybersecurity for these apps and their associated data is an afterthought.

The main shortcoming boils down to most organizations protecting only what is in front of them. Hedge notes that companies generally lack the ability or bandwidth to track down all data that needs to be secured. It's a classic case of what's "out of sight is out of mind," but one with significant business and regulatory ramifications if an organization experiences a data compromise.

This challenge, according to Hedge, has been long in the making. It started with on-premise workloads moving to the cloud, was followed by data stores such as Sharepoint and Box, and now continues with applications like Salesforce, Workday, and Microsoft 365. Hedge finds that this data migration pattern often takes place without the blessing of IT or cybersecurity departments.

SaaS apps should be viewed as data repositories, which Hedge considers the best approach for prioritizing the data security risks for SaaS apps.

But organizations typically don't understand that the shared responsibility model applies to their SaaS estate, leading to lax SaaS data security governance and pockets of data spread insecurely across the organization. When contemplating the scope of this security challenge, Hedge states that "it's hard enough to protect your own environment, let alone all the SaaS-to-SaaS connections you find in a typical organization's environment."

> "The adoption of SaaS apps like Salesforce and Workday by business departments have resulted in more and more data moving to the cloud — and in more cases than not, without the blessing of IT and cybersecurity departments. This has resulted in limited security monitoring of these core enterprise applications for as long as they have been around. People are finally waking up to the cyber risks that this presents.
>
> **Arthur Hedge**
> President, Castle Ventures

The tide, however, is starting to turn. Cybersecurity and IT teams are gaining a better understanding of the risks that insecure SaaS apps pose, largely due to growing incidences (and media coverage) of SaaS breaches. But more work on security awareness, and the responsibilities for securing SaaS, is urgently needed.

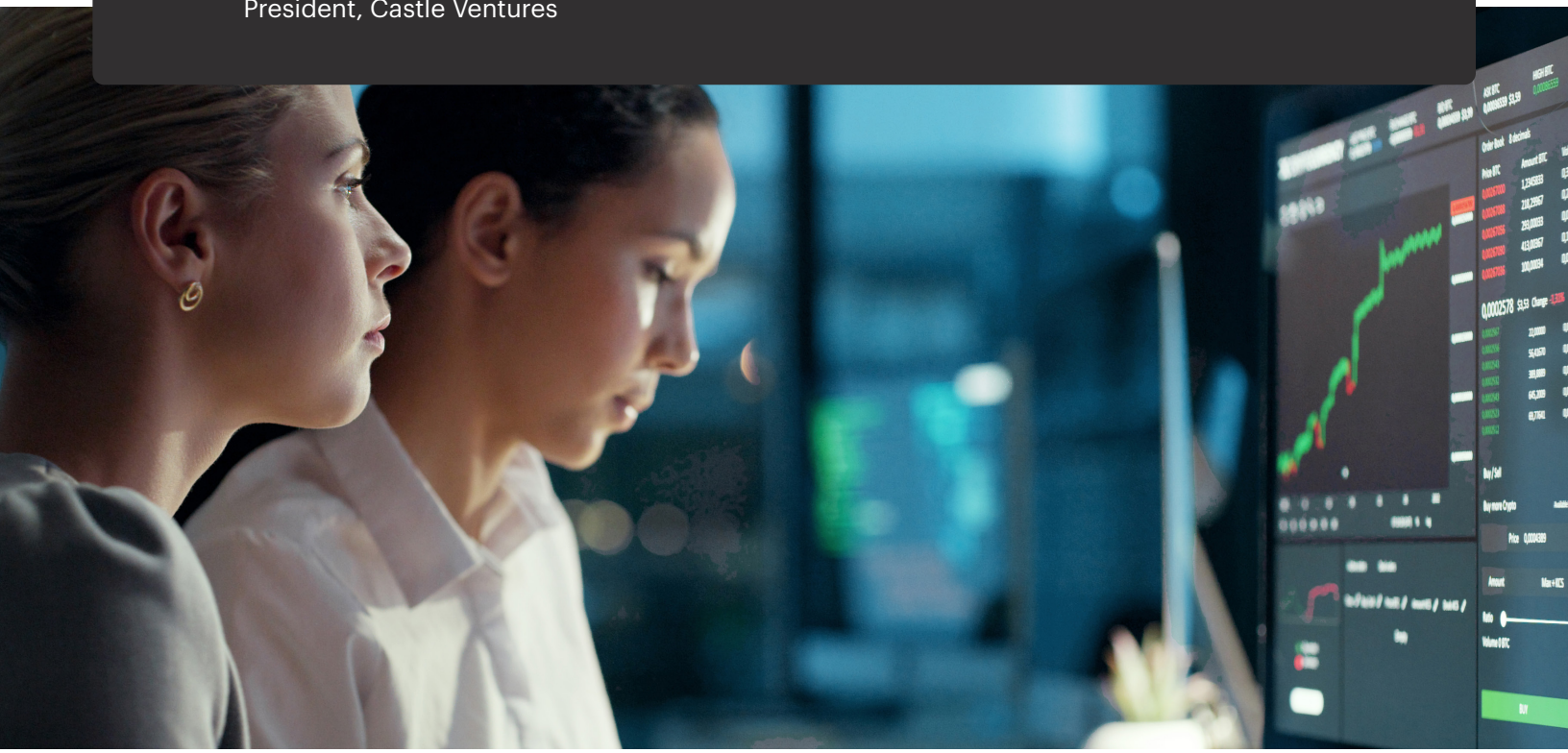
Requirements

Castle Ventures selected AppOmni as a strategic technology partner based on the core product capabilities and the company's vision. Hedge believes that "AppOmni wasn't just solving a point problem, but was taking a platform-based approach to solving SaaS security comprehensively. This was critical to us."

Must-have capabilities for Castle Ventures include:

- A single solution that secures their entire SaaS estate
- Deep SaaS Security Posture Management (SSPM) coverage for core SaaS apps where most sensitive data is kept
- High degree of customizability
- Protection for clients' custom-built application
- Highly experienced Partner and Technology teams
- The ability to develop a customizable, managed SaaS security service offering around Castle Ventures' products

> The depth of the coverage that AppOmni provides for SaaS apps was the differentiating feature on why we selected AppOmni for our data security practice.
>
> **Arthur Hedge**
> President, Castle Ventures



The Results

Castle Ventures' need for a new approach to comprehensive SaaS cybersecurity was driven by two key concerns:

1. Configurations of commonly used SaaS services providers in the enterprise are so complex that understanding the appropriate configuration settings is humanly impossible, whether at a point in time or on an ongoing basis. Configuration management can only be addressed through security automation.
2. Considering these core SaaS applications are leveraged on a daily basis for core business use cases, a continuous monitoring capability must be in place to detect and alert on potentially anomalous end-user activity.

Castle Ventures got this and more from AppOmni.

The overall experience of AppOmni — from the product's advanced SaaS Security Posture Management (SSPM) capabilities, the roadmap, to the expertise of its entire team — is what set AppOmni apart from the competition. Hedge states, "We literally get calls from SaaS security companies every week, and no one comes close to AppOmni's SaaS security capabilities."

Many Castle Ventures clients, primarily in the financial services sector, have mature cybersecurity practices, including resilient cybersecurity posture. While these clients internalize the importance of adopting proactive cybersecurity solutions for their SaaS apps, other industry sectors desperately need SaaS security education, particularly among their IT executives. Hedge acknowledges that "the scale of the data security challenge for SaaS is, frankly, still not adequately understood."

The pace of SaaS breaches is increasing awareness among organizations, and their cybersecurity and IT teams are realizing that they are ultimately responsible for data security. Education for the executives (often the SaaS app owners) is still needed to illustrate the significant operational and financial risks that insecure SaaS and ungoverned SaaS data represent.

> "AppOmni isn't a point product. It's a comprehensive SaaS cybersecurity platform for managing SaaS security at scale. We recommend it as the go-to SaaS Security Posture Management solution for all of our clients.
>
> **Arthur Hedge**
> President, Castle Ventures

When considering the overarching value AppOmni brings to SaaS data security, Hedge concludes that "the perimeter no longer exists. Operating in today's environment is equivalent to being protected by a wall of Swiss cheese. So you've got to be able to figure out where all those holes [insecure SaaS data access] are. And AppOmni helps you do that and ensures that your SaaS and associated data are protected comprehensively."

About AppOmni

AppOmni is the pioneer of SaaS Security Posture Management enabling customers to achieve secure productivity with their SaaS applications. With AppOmni, security teams and SaaS application owners quickly secure their mission-critical and sensitive data from attackers and insider threats. The AppOmni platform constantly scans SaaS APIs, configurations, and ingested audit logs to deliver complete data access visibility, secure identities and SaaS-to-SaaS connections, detect threats, prioritize insights, and simplify compliance reporting. Over 20% of the Fortune 100 and global enterprises across industries trust AppOmni to secure their SaaS applications. For more information, please visit https://appomni.com.