Blend Case Study

Description

Blend needed to protect its banking partners' customer PII, including Social Security numbers, income records, and more across email, web browsers, and removable media for their Windows-based endpoints and managed through API access.

Challenge

Prevent the exfiltration of sensitive data, including Social Security numbers, income records, and other sensitive data

Solution

Implementing Endpoint Protector Unify, including Device Control and Content Aware Protection

Results

Improved insight into user actions, greater visibility into data movements, seamless API implementation

Challenge

Blend is a leader in the fintech industry, with many of the largest financial providers using Blend's cloud-based banking platform to streamline workflows such as mortgage applications. As such, the company needed to protect its banking partners' customer personal identifiable information (PII) stored on their Amazon Workspaces (AWS) architecture, including Social Security numbers, income records, and more across email, web browsers, and removable media for their Windows-based endpoints.

Unfortunately, Blend's existing Data Loss Prevention (DLP) solution lacked the ability to protect data loss at the endpoint, and didn't have API access - critical to its infrastructure as code approach - leading them to look for a replacement.

The Solution

To address these concerns, Blend turned to Endpoint Protector Unify by CoSoSys - the industry's only API-first, endpoint DLP solution. They embarked on a comprehensive implementation strategy, which involved setting up policies to improve insight into user actions, oversee data movements, and identify particular keywords and confidential information.

Leveraging the platform's Content Aware Protection functionality to inspect and contextually scan data for sensitive PII, Blend is able to monitor for confidential information and oversee data movement, thus significantly enhancing their data protection measures.

With the API-driven architecture of Unify, Blend can now automate infrastructure as code, facilitating seamless integration of DLP policy changes through a streamlined process of creating pull requests on GitHub. This sophisticated automation ensures that approved code

modifications are efficiently pushed to Endpoint Protector Unify, establishing a robust audit trail for enhanced accountability. Additionally, the introduction of an API into the Unify platform allows them to verify the presence of security agents across all anticipated devices, bolstering confidence and assurance for their customers.

By embracing automation, enhancing visibility, and exerting control over security configurations and policies, this solution empowers Blend's security operations team to maintain a resilient security posture, particularly in the intricate and dynamic landscape of AWS. The platform not only fosters transparency but also reinforces accountability in the management of security-related changes, contributing to a more secure and well-governed IT environment.

Why Endpoint Protector?

- Data and file transfer monitoring and remediation
- Flexibility and detailed control over content movement
- Fast and easy implementation process
- Detailed monitoring and reporting
- API-driven to support automation initiatives

Quote

"Our favorite thing about Endpoint Protector is the granularity of the Content Aware Protection. Being able to drill down exactly into not only the types of data that we're looking for but in the file types and all other things."

Jeffrey Plotts
Security Operations Engineer at Blend Labs

Endpoint Protector Unify is a highly scalable, multi-OS cybersecurity platform that prevents sensitive data from being lost beyond an organization's control. Its open API architecture closes the visibility gap between network/cloud security and the endpoint, putting the endpoint at the center of an organization's data security strategy.