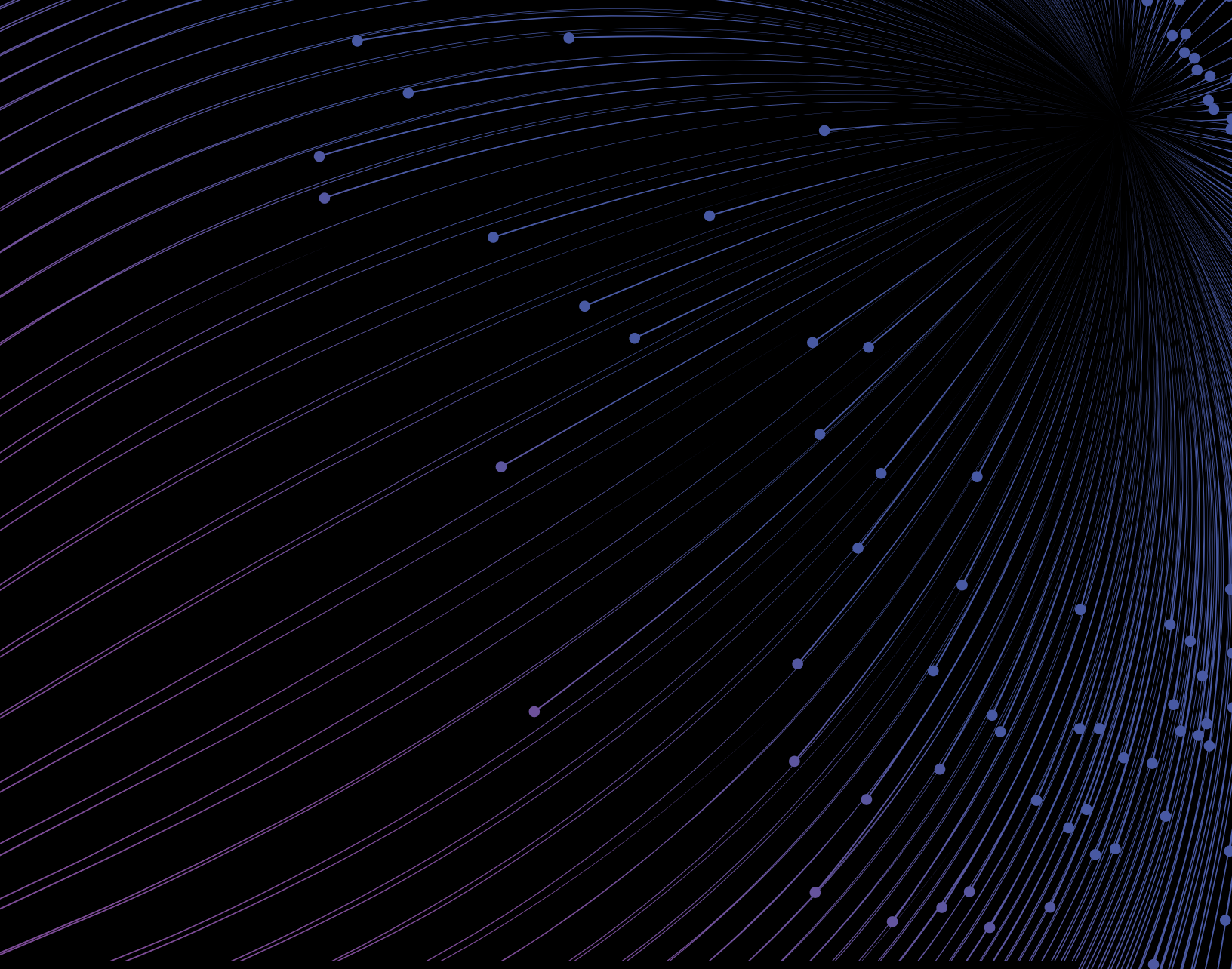

Cylance® and Bitglass Partner for Increased Protection and Compliance

Unparalleled Cloud-Based Application Access

CYLANCE

bitglass

About Cylance

Cylance uses artificial intelligence to deliver prevention-first security solutions and specialized services that change the way organizations approach endpoint security. Cylance security solutions combine AI driven predictive prevention with dynamic threat detection and response to deliver full spectrum threat prevention and threat visibility across the enterprise.

About Bitglass

Your company's move to the cloud delivers flexibility and cost savings, but that doesn't mean you should lose control of your data. Bitglass' Next-Gen Cloud Access Security Broker (CASB) solution enables your enterprise to embrace the cloud while ensuring data security and regulatory compliance. Bitglass secures your data across any cloud app and any device.

Bitglass was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.

Introduction

Cylance and Bitglass formed a technology alliance to provide enhanced security to cloud-based applications through ensuring hosts that connect to these applications are protected by Cylance technology. Additionally, Bitglass' Zero-day Threat Protection, powered by the CylanceINFINITY™ engine, stops the spread of malicious files across all cloud apps.

Value Statement

The integration between Cylance and Bitglass allows organizations to require all hosts that connect to cloud-based applications are protected by Cylance technology, ensuring only fully protected endpoints access critical cloud applications.

Customers are finding value in the Bitglass-Cylance alliance. At the heart of the alliance is the goal to deliver cost savings to customers while preserving control over endpoint management and cloud activity. CylancePROTECT® Endpoint Protection Platform (EPP) provides comprehensive control over managed endpoints. Bitglass's Next-Gen cloud access security broker (CASB) solution, coupled with Cylance's powerful artificial intelligence engine, enables enterprises to embrace the cloud and unmanaged endpoints, knowing their data is protected.

Use Cases

Cloud Access Control

- Challenge: More organizations are moving critical applications to the cloud. To secure corporate data, enterprises must ensure that the users and devices accessing these applications are fully protected and compliant
- Solution: Cylance's prevention-first methodology provides industry leading threat protection (less infections, alerts, remediations and re-imaging). This, along with Bitglass' real-time access control capabilities, limits cloud access to only those authorized users and devices. Bitglass' agentless proxy-based scanning ensures that even traffic from unmanaged devices is scanned, preventing proliferation of malware via these risky devices

Threat Coverage Sharing

- Challenge: Security teams need to ensure threats uncovered by Bitglass and other security products are proactively shared with Cylance technology and vice versa to ensure all threats are stopped across the customer's extended ecosystem
- Solution: Bitglass' Zero-day Threat Protection is kept up-to-date with the latest versions of the CylanceINFINITY™ engine. Customers can also search and blacklist file hashes across their environment

Inspect All Cloud-Based Data

- Challenge: Many organizations have little visibility into files that are uploaded, downloaded, or traversing cloud platforms, placing both cloud data and connected devices at risk
- Solution: By combining the cloud-based CylanceINFINITY engine with Bitglass' Zero-day Threat Protection, all files can be inspected by Cylance technology and quarantined by Bitglass without invasive endpoint agents

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618

CYLANCE

20180412-0422