Malware, p.i.

Tracking Cloud Infections

bitglass

The cloud provides a myriad of benefits for the enterprise. However, for organizations that haven't invested in modern security solutions, such as cloud access security brokers (CASBs), cloud applications and personal devices can serve as very convenient proliferation points for malware. Frequent news stories about infected organizations illustrate what can go wrong for those lacking appropriate security measures.

To analyze the proliferation of malware in the cloud, the Bitglass Threat Research Team scanned the cloud applications of customers that do not use its Advanced Threat Protection (which leverages AI-based malware protection from Cylance). After scanning tens of millions of files, Bitglass discovered a high rate of infection in cloud applications, indicating a low efficacy rate for apps with built-in malware protection like Microsoft OneDrive and Google Drive. To test this further, Bitglass identified a new piece of ransomware which went undetected by most native and third-party anti-malware solutions.

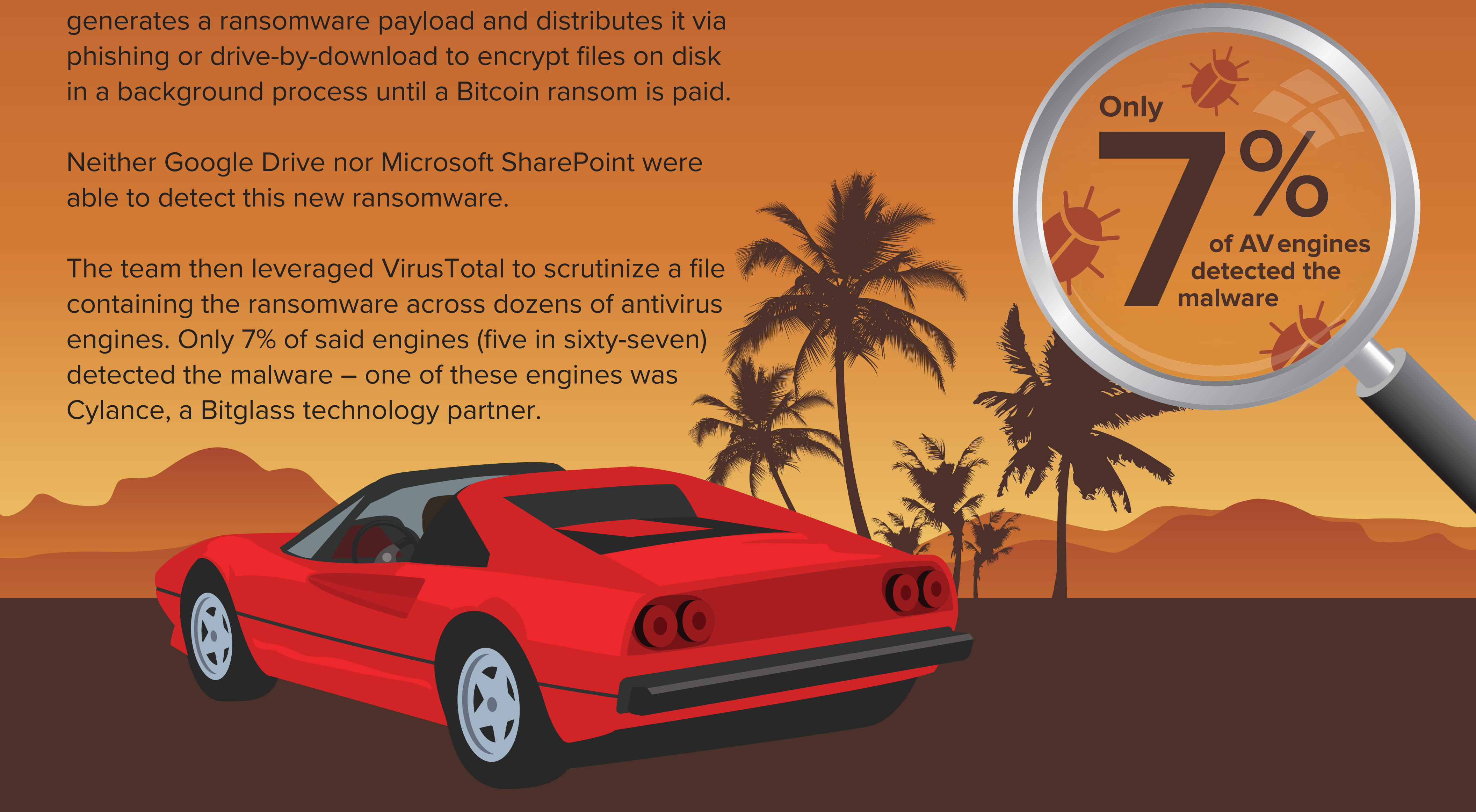
A Perpetrator

In conducting its scan of malware in the cloud, the Bitglass Threat Research Team discovered a new piece of zero-day ransomware dubbed ShurL0ckr. ShurL0ckr, validated as ransomware by Cylance, is ransomware-as-a-service, meaning the hacker generates a ransomware payload and distributes it via phishing or drive-by-download to encrypt files on disk in a background process until a Bitcoin ransom is paid.

Neither Google Drive nor Microsoft SharePoint were able to detect this new ransomware.

The team then leveraged VirusTotal to scrutinize a file containing the ransomware across dozens of antivirus engines. Only 7% of said engines (five in sixty-seven) detected the malware – one of these engines was Cylance, a Bitglass technology partner.

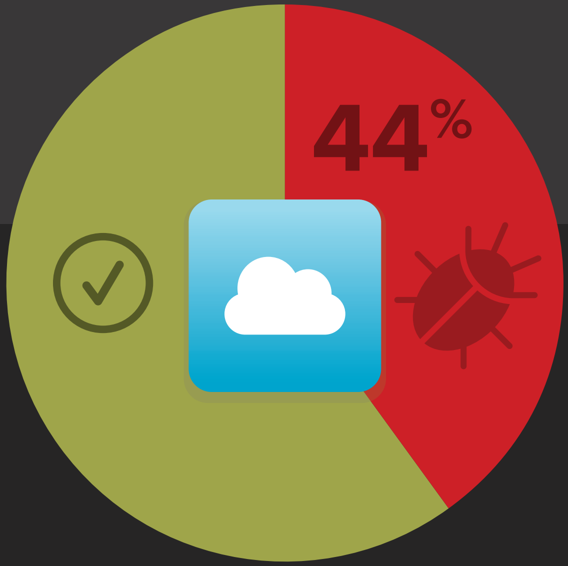
A piece of zero-day ransomware went undetected by Google Drive, Microsoft SharePoint, and the vast majority of commercial AV engines.

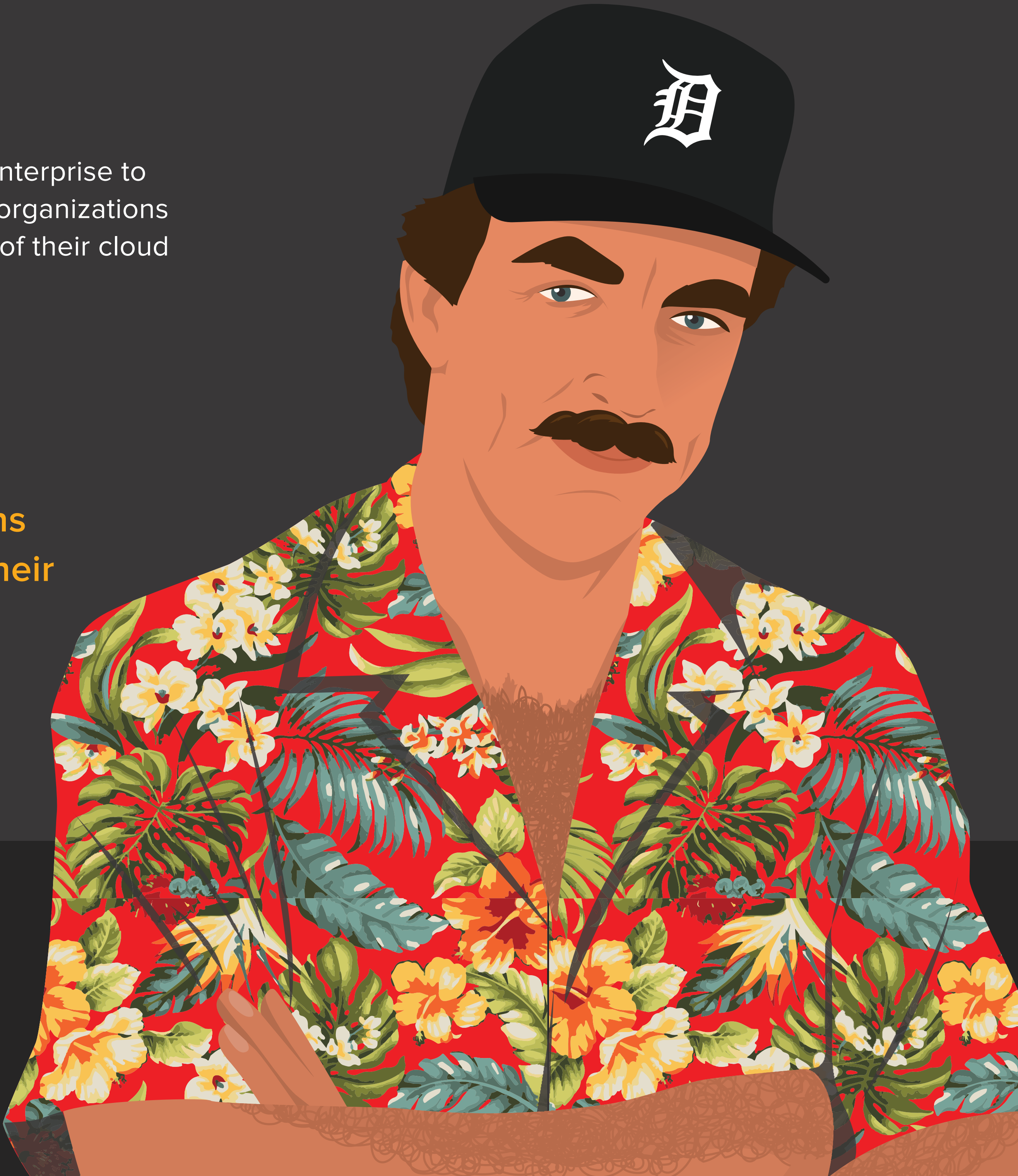


Companies in the Crosshairs

A single piece of malware can bring any enterprise to its knees. Unfortunately, 44% of analyzed organizations had some form of malware in at least one of their cloud applications.

Nearly half (44%) of organizations had malware in at least one of their cloud apps.

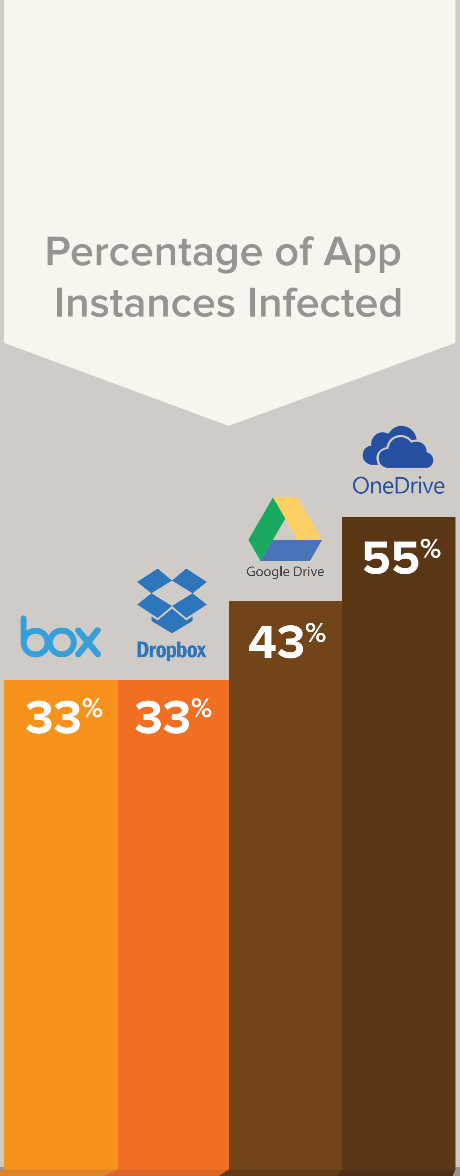




The Lawless Cloud

When cloud applications are not properly secured, malware infections can use the cloud as a distribution point for spreading to connected apps and users' devices. In Bitglass' analysis, one in three SaaS app instances contained at least one threat. Below, one can see the rate at which each cloud application was infected. 54.5% and 42.9% of OneDrive and Google Drive instances were infected, respectively.

On average, one in three corporate instances of SaaS apps contained malware.



The Malware Masquerade

Below are the infected file categories from Bitglass' research. Each poses a unique threat to the enterprise, ranging from data theft to the monitoring of user behavior. Scripts and executables can launch malicious applications with the click of a button. Office formats (like PowerPoint and Word containers) are common corporate file types that most users trust and open without hesitation. Other formats include text files, images, and more, while compressed formats include Zip files.

The average organization held nearly 450,000 files in the cloud, with 1 in 20,000 containing malware.

Infected File Types

42% Script and Executable Formats

21% Office Formats

19% Other Formats

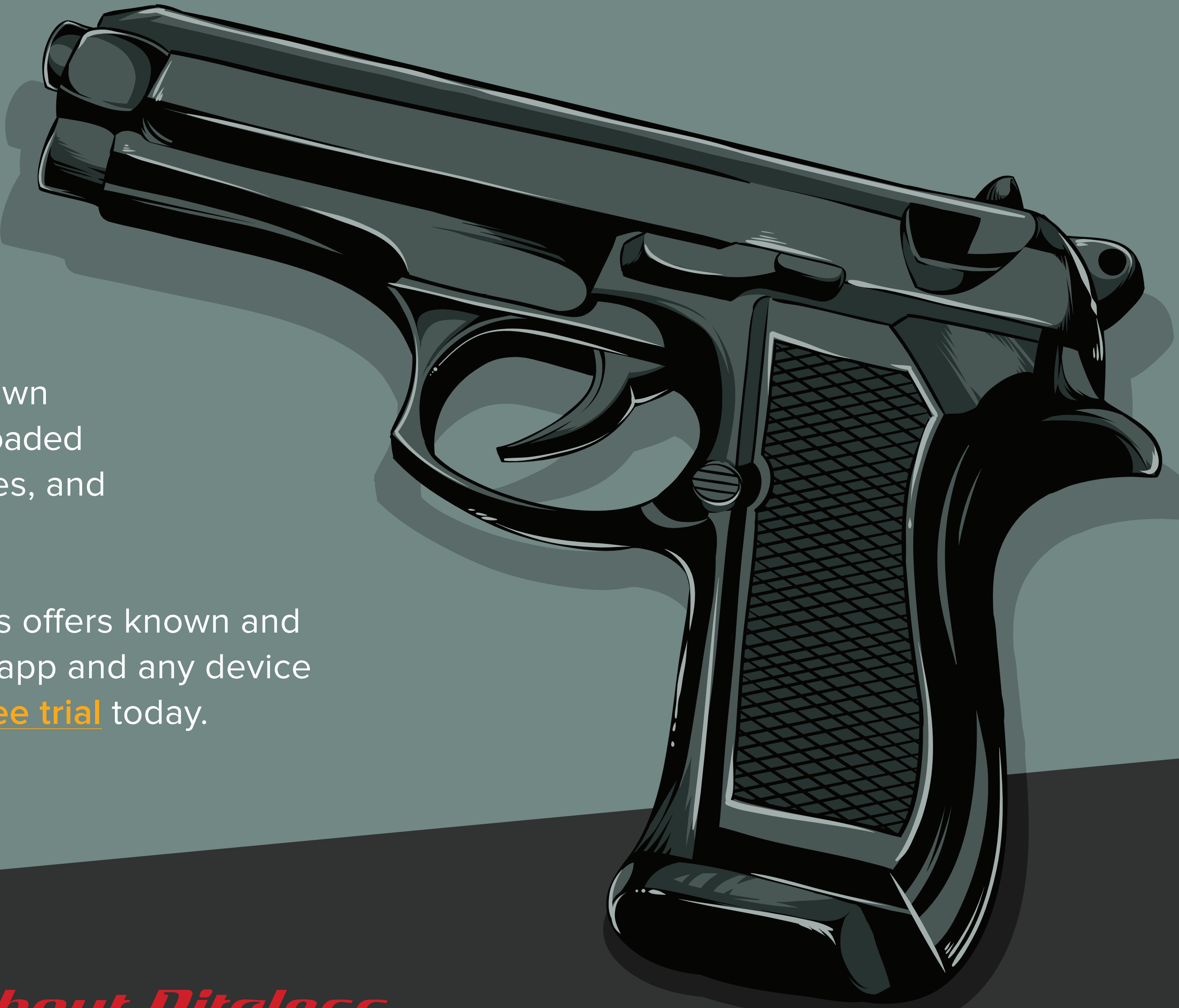
10% Windows System Files

8% Compressed Formats

Wrap-Up

While malware is not a new threat, many companies fail to defend against its modern forms; relying solely upon endpoint or native cloud security is no longer adequate. Organizations must now adopt cloud-first solutions that defend against known and unknown malware as they are uploaded to applications, downloaded to devices, and resting in the cloud.

Fortunately for the enterprise, Bitglass offers known and unknown malware protection for any app and any device with its Next-Gen CASB. Request a free trial today.



bitglass

Phone: (408) 337-0190
Email: info@bitglass.com

www.bitglass.com

About Bitglass

Bitglass, the Next-Gen CASB company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver zero-day, agentless data and threat protection for any app, any device, anywhere. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.