AVANAN

CLOUD SECURITY REPORT

Executive Summary

As your organization moves to the cloud, new risks emerge. Issues such as privacy, security and compliance are harder to identify and remediate without a cloud-centric security platform. Avanan's cloud governance platform offers share management, policy automation and compliance enforcement for the enterprise SaaS in a single, simple-to-use dashboard. Avanan has partnered with the leading security vendors to offer cloud-based versions of their best-of-breed technology. This report contains highlights of security-related findings in your cloud implementation after performing a security scan of your cloud. Here are the highlights :

1309	PCI and HIPAA violations
684	Files containing credit card, social security, or other PII
2555	Sensitive files are now in your cloud
981	Sensitive files shared with external users
612	Malicious files are now in your cloud
437	Corporate files publicly available
58,656	Files shared with external users
191,974	Files shared internally
2	New Shadow IT services detected

AVANAN

Cloud File Sharing

Collaboration

is vital to business, and providers like Office 365, Google and Box have made it easier than ever before. Your employees can share a document with partners and clients with just a click of the mouse or tap of the finger. Unfortunately, it is just as easy to let confidential information spread to the wrong hands.

Understanding the cloud sharing model is critical to maintaining data security, privacy and compliance.

The information below explains how the data is being shared in your cloud storage.

Publicly Shared

means that the files are accessible to anyone on the Internet, including search engines.

Shared with 3 party apps

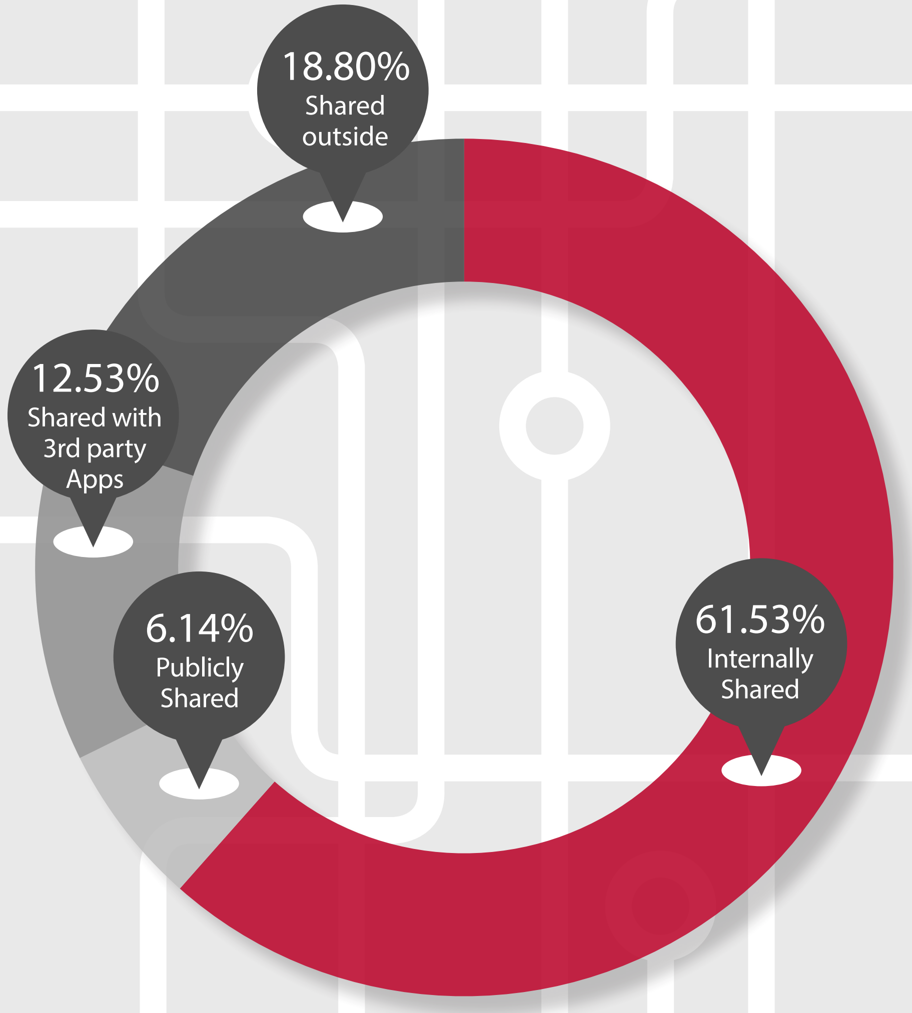
these are files accessible to applications authorized to view files on the cloud-drive.

Internally Shared

Files shared within the organization.

Shared Outside

Files that were shared with people outside the organization.

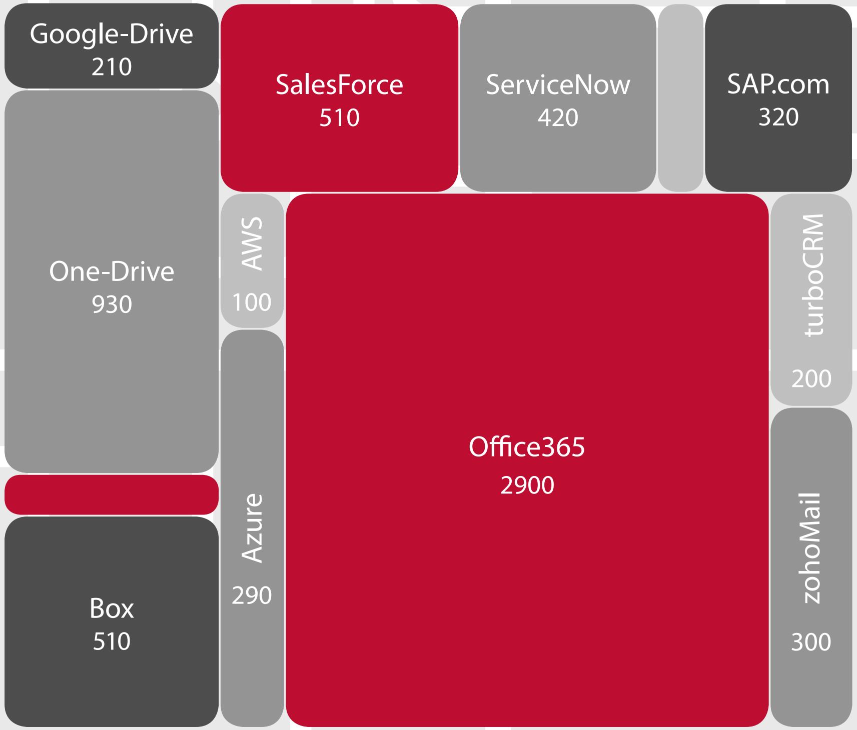


SHADOW-IT

Employees are using the cloud. They are more productive. They are communicating and collaborating using SaaS applications that make sharing easy. Unfortunately, they might be using unapproved cloud applications that are a threat to your confidential data. These unapproved SAAS applications are also known as “**Shadow-IT**”.

Users can easily connect **unapproved SaaS applications** to third-party SaaS by granting direct cloud-to-cloud access. Sometimes, these unsanctioned applications ask for more rights than IT might approve.

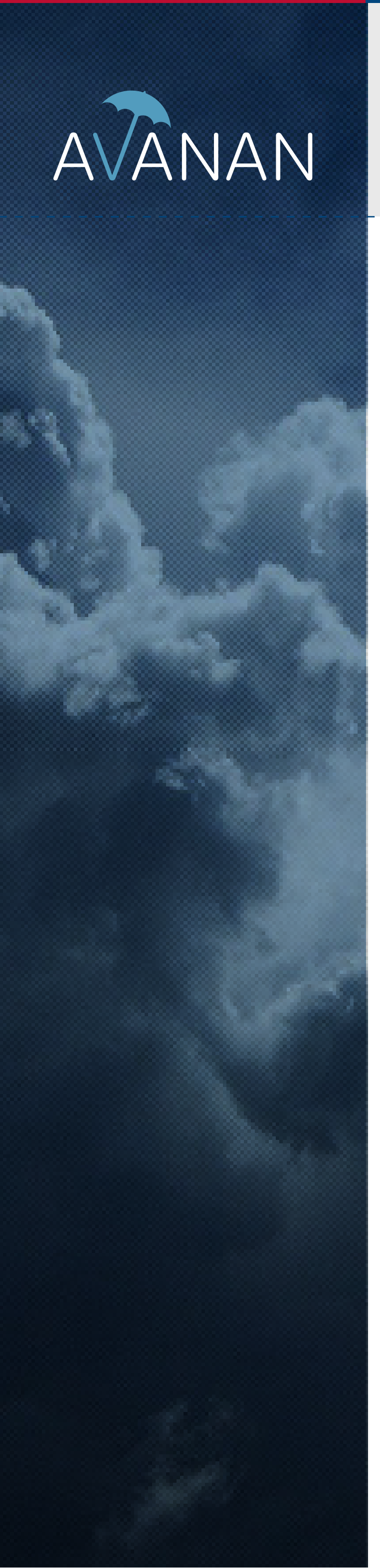
No matter if users connect to unsanctioned applications directly or cloud-to-cloud, it is important to understand which SaaS applications are used, what level of access was given and how many users are using these applications.



ACCESS-GEOGRAPHY

Your users are accessing the cloud from home, office, remote-offices and more. It is important to monitor where users are located to prevent unwanted connections. A login from an atypical location, or simultaneous connections from distant locations could indicate compromised credentials, used by remote attackers. The diagram shows the geographical location of these suspect connections.

Country	Attempts
Australia	10
Canada	2
Colombia	4
France	11
Gabon	17
India	38
Russia	73
Turkey	14



EMAIL SECURITY

Often, the first SaaS application is cloud-based e-mail and collaboration. Avanan uses best-in-class tools to scan inbound and outbound emails for data leakage and privacy compliance violations. At the same time, it scans every attachment for malware using multiple signature-based tools and advanced threat protection sandbox technology. Here is a short summary of what was found.

4140 Emails containing sensitive information

152299 Attachments scanned

317 Malicious Attachments

ANOMALOUS EVENTS

Avanan monitors the interactions with the cloud and identifies events that indicate a **potential threat to your data and to your business**. Avanan uses context-based behavior analysis to identify anomalous patterns and malicious intent.
The diagram below presents the initial findings:

GEO-suspicious login – Access from remote locations withing a short period of time – clear indication of compromised credentials.

Massive Downloads – Often indication of a compromised account used to steal data.

Massive Deletions – Indication for a malicious activity or ransomware.

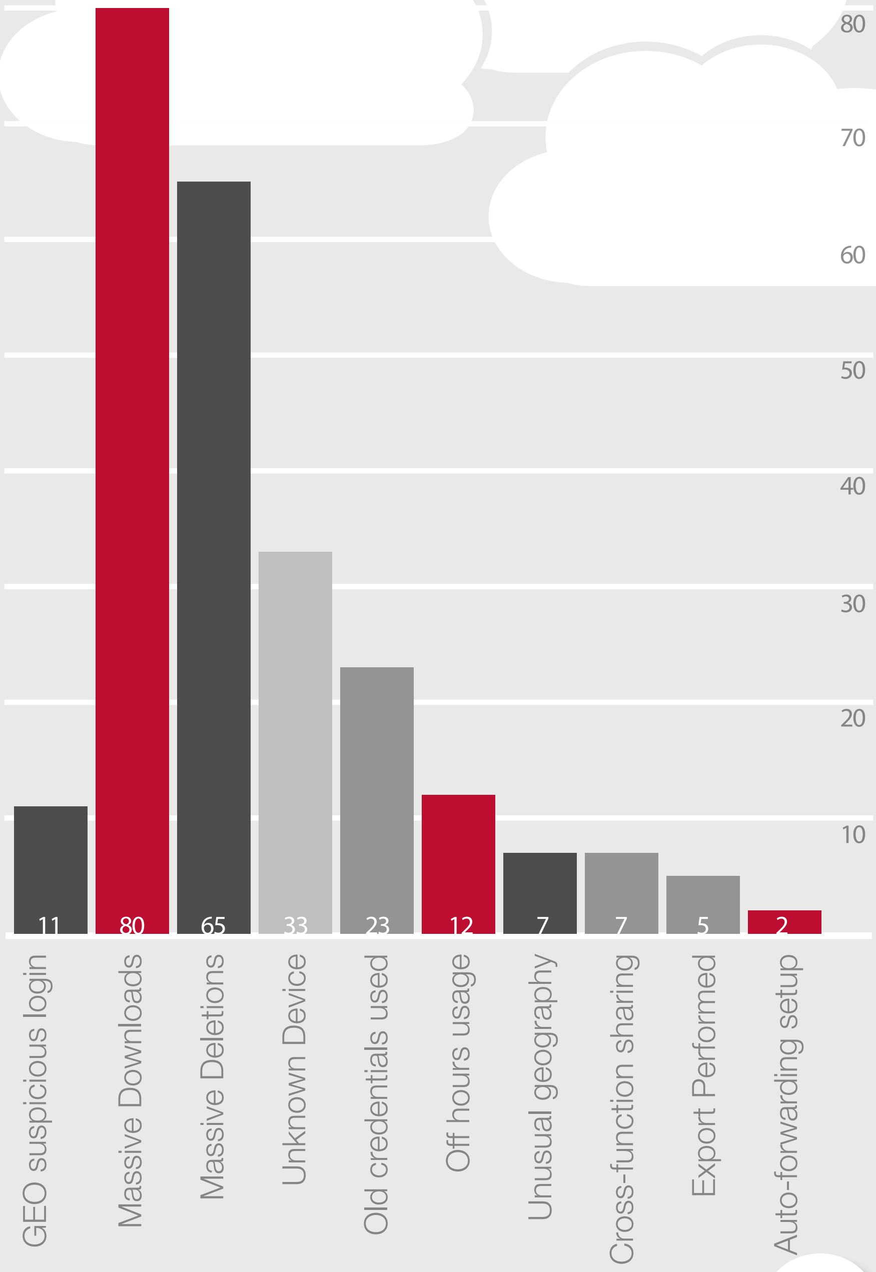
Unknown Device – Access by an unknown device can indicate compromised credentials.

Atypical Off-hours Usage – An unusual usage pattern can be a sign of compromised device credentials.

Cross-function Sharing – This indicates the flow of data between different organizational functions that is out of context. Depending on the type of data being shared, it could indicate an internal data leakage scenario.

Export Performed – A user performing a massive export of cloud data should be flagged and investigated if it is not normal behavior.

Auto-forwarding Setup – A typical, yet problematic configuration whereby users automatically forward their corporate emails to noncorporate accounts, resulting in data-leakage and compliance violations.



OFFICE365 SECURITY

Malicious Files

Office 365 is quickly becoming one of the most popular enterprise collaboration platforms. Users are uploading, downloading, creating and sharing content within Office 365 at an accelerating rate. Avanan uses best-of-breed antivirus and sandbox technologies to ensure that no malicious files enter the cloud and pose a risk to devices and data.

Antivirus tools are used to detect malware-infected files by searching for known virus ‘signatures’. To achieve maximum coverage, Avanan users multiple antivirus engines at once.

Sandbox tools are used to detect new/unknown threats. These technologies use virtual machines to actively inspect the behavior of a file once opened. Sandbox scanning is critical for preventing targeted attacks, often known as APT – (Advanced Persistent Threats).

Check Point
SOFTWARE TECHNOLOGIES LTD.

612 Malicious files found by Check Point Threat Emulation

Symantec.

412 Malicious files detected Symantec Anti-Virus engines

FireEye

612 Malicious files found using sandbox technology by FireEye

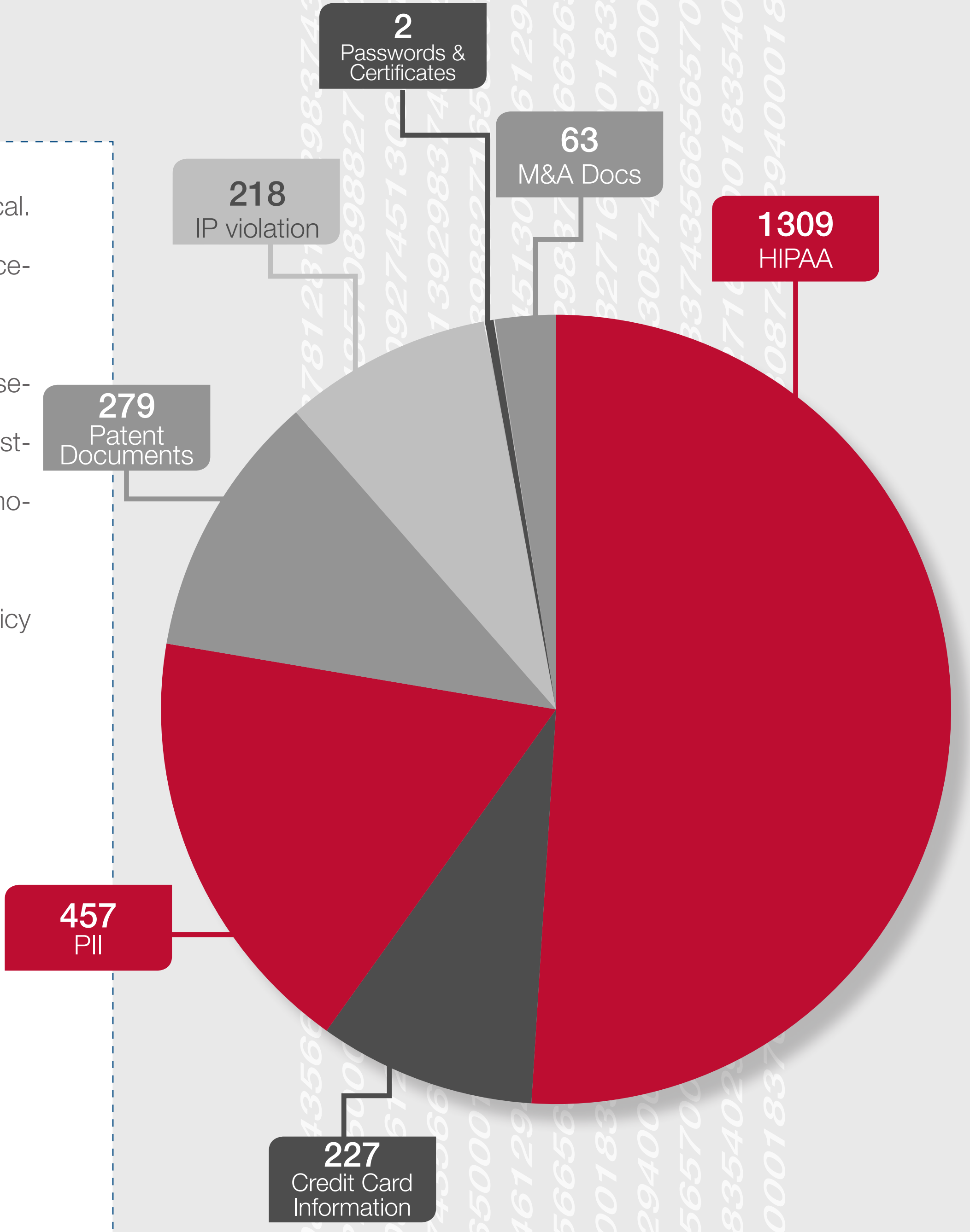
AVANAN

DATA-LEAKAGE

Understanding who has access to corporate data is critical. This is especially true for the cloud – where data-leakage scenarios are frequent and hard to detect.

Data classification is critical for this process – to eliminate false-positives and allow automatic remediation. Avanan uses best-of-breed DLP classification engines to scan both data-in-motion and data-at-rest.

When combined with contextual user, group and share policy information, it is easy to identify compliance threats.


Passwords & Certificates
M&A Docs
IP violation
HIPAA
Patent Documents
PII
Credit Card Information