Avanan for G Suite

Technical Overview

Contents

Intro

Avanan can offer visibility and protection unparalleled by proxy solutions, by connecting cloud-based versions of third-party security tools directly to the G Suite infrastructure using its native application programming interface (API).

Avanan offers best-of-breed cloudified security tools including:

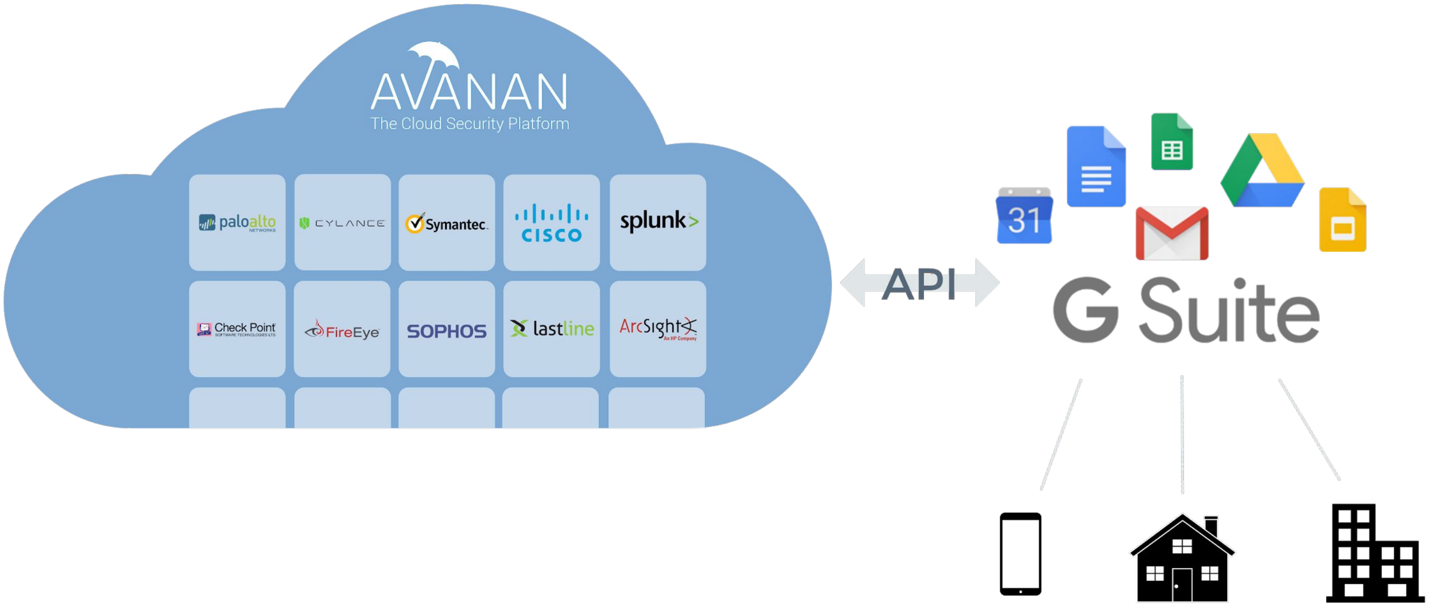
- Anti-Phishing
- Malware & Ransomware Detection
- Data Leakage Prevention
- Encryption
- Anomaly Detection
- Incident Response
- Automated Security Policies

How Avanan Works

The Endless Security Stack

Avanan finds the industry's best security technologies and wrap them in the Avanan API, standardizing all their user, file, event and policy information.

These security technologies can be deployed in a single click to secure every application in your G Suite environment.

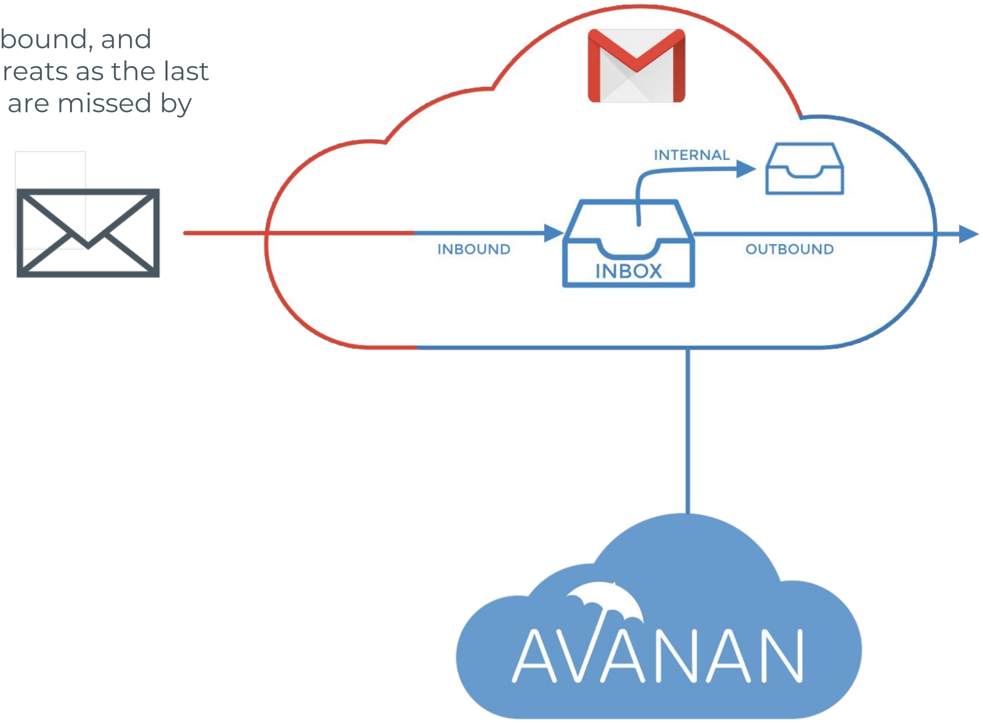


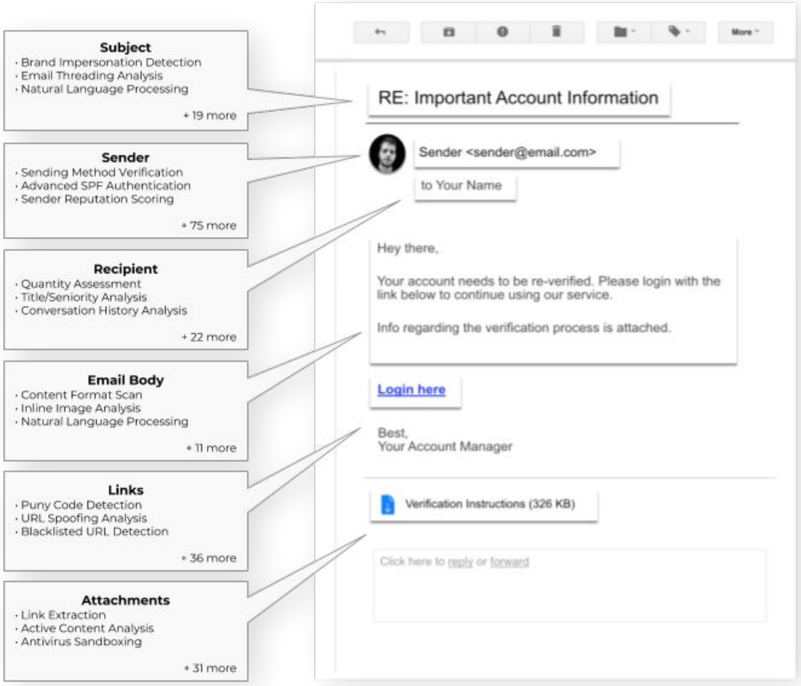
Complete Cloud Integration

Avanan connects directly to the native API of your G Suite environment. This provides both real time and historical information about every user, file, event and policy--not only of your users, but everyone that has access.

Email Security for Gmail

Avanan scans inbound, outbound, and internal emails, catching threats as the last layer of defense - after they are missed by Gmail's default security.





Subject
- Brand Impersonation Detection
- Email Threading Analysis
- Natural Language Processing

+ 19 more

Sender
- Sending Method Verification
- Advanced SPF Authentication
- Sender Reputation Scoring

+ 75 more

Recipient
- Quantity Assessment
- Title/Seniority Analysis
- Conversation History Analysis

+ 22 more

Email Body
- Content Format Scan
- Inline Image Analysis
- Natural Language Processing

+ 11 more

Links
- Puny Code Detection
- URL Spoofing Analysis
- Blacklisted URL Detection

+ 36 more

Attachments
- Link Extraction
- Active Content Analysis
- Antivirus Sandboxing

+ 31 more

RE: Important Account Information

Sender <sender@email.com>

to Your Name

Hey there,

Your account needs to be re-verified. Please login with the link below to continue using our service.

Info regarding the verification process is attached.

Login here

Best,
Your Account Manager

Verification Instructions (326 KB)

Click here to reply or forward

Avanan's email security technology analyzes 200+ indicators in every email to detect phishing attacks, malware and ransomware.

Data Security for Google Drive

Data Leak Prevention

Avanan uses cloud-native controls to enforce granular share policy by regulating collaboration rights for individual files or folders based upon its contents and context. Files can be deleted, quarantined or encrypted before they become available to the wrong users.

Malware Sandboxing

Avanan performs emulations in cloud sandboxes to analyze each file's behavior and detects malicious files before the threat reaches any endpoints, whether it is within shared folder, email, or cloud application. Unlike alternative malware testing methods (like proxies or MTAs), our sandbox integration provides a safe yet seamless experience for the end user with little to no delay/interruption.

Encryption

Avanan's policy-driven controls can encrypt documents automatically based upon content or context. Authorized users can open and edit the files without need for passwords, but maintain protection even if stored in a shared directory.

Predictive AI

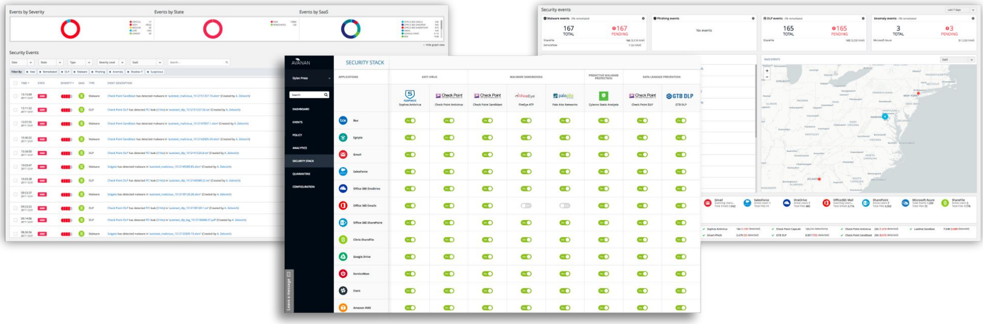
Avanan's AI tools perform statistical analysis on the contents of every file to predict which files may contain malware before they can be detected by other methods.

File Sanitization

Instead of relying on detection that is prone to false-negatives, file sanitization will replace the original file with a sanitized version of the file, maintaining its content and format but removing any macros and binary resources.

Avanan's granular policy controls allow you to set what gets sanitized, from banning certain file types to disallowing macros entirely.

Policy Automation



Monitor Only

Monitor only mode provides visibility into the cloud-hosted email leveraging G Suite's publicly available API. Scan results are provided from 60+ best of breed security tools. In this mode, manual and automated query based quarantines are available after delivery to the user mailbox.

Detect and Prevent

Detect and Prevent mode provides an increased level of protection that scans email in the user's inbox leveraging the G Suite APIs. This mode adds an automated policy action to quarantine malware, phishing attacks etc. based on the results of the best-of-breed security stack. In this mode user notifications and release workflows are available.

Protect (Inline)

Protect Mode provides the highest level of protection and scans emails prior to delivery to the end user's inbox. Leveraging the same G Suite APIs and implementing email rules, Avanan can scan email with a best-of-breed security stack to protect end users from malware, data leaks, phishing attacks and more. Scanning and quarantining takes place before email is delivered to the user's inbox. This mode insures that threats are detected and remediated before the user has access to the email.

Workflows and Notifications

Detect and Prevent Mode and Protect (inline) Mode both offer three separate workflows to manage Malware and Anti-Phishing attacks in the platform. The only difference is when the workflow is invoked. Detect and Prevent scans email after delivery of email to the user and Protect (inline) scan just prior to delivery.

Workflow Options

Malware

- User is alerted and allowed to restore the email
- User is alerted, allowed to requests a restore. Admin must approve
- Email quarantined. User is not alerted. Admin can restore

Phishing

- User receives the email with a warning*
- Email quarantined. Admin can restore
- Email Quarantined. User is alerted, allowed to request a restore. Admin must approve

Suspicious

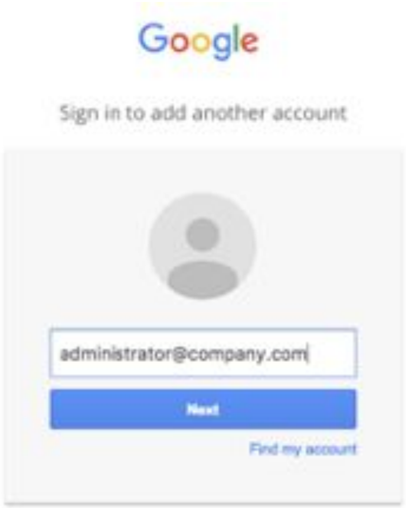
- User receives the email with a warning*
- Do nothing

** Advanced options are available to customize all manual generated messages and notifications to the end users.*

Authentication

Access to G Suite API is based on granting to the Avanan app in company's domain within Google Apps using the company's Google administrator account.

Procedure: Starting from the Avanan portal, the user integrates with G Suite. The Avanan platform then redirects the user to an authorization page on: https://accounts.google.com



Sign in to add another account

administrator@company.com

Using the company's Google administrator account, the user is redirected to the Avanan Cloud Security Platform app in Google Apps marketplace on: https://chrome.google.com/webstore

The company's administrator then install the Avanan Cloud Security Platform application which will enable Avanan to access the Gmail and Google Drive APIs on behalf of company's Google administrator.

Because the authentication and granting is done within the Google Marketplace service, Avanan never sees the company's admin credentials.

More information about Google's authorization process can be found below:

- Gmail API Authorization
- Google Drive API Authorization

Permissions

Avanan applications comply with the security guideline of *minimal permission* - requiring the minimal set of permissions required for its functionality. The Gmail and Google Drive APIs offer a range of tool permissions, but the minimum required permissions for the Avanan platform are:

Gmail

- E-mails (View and manage)
- View users on your domain
- Insert mail into your mailbox
- Manage mailbox labels
- View and modify but not delete your email
- View your emails messages and settings
- Manage your basic mail settings
- View and manage Pub/Sub topics and subscriptions
- View your email address
- View your basic profile info

Google Drive

- View the activity history of your Google Apps
- View your Chrome OS devices' metadata
- View your mobile devices' metadata
- View and manage the provisioning of groups on your domain
- View users on your domain
- Manage data access permissions for users on your domain
- View audit reports of Google Apps for your domain
- View usage reports of Google Apps for your domain
- View and manage the files in your Google Drive
- View your Google Drive apps
- View metadata for files in your Google Drive
- View the files in your Google Drive
- View your basic profile info

APIs

Gmail

Gmail offers a tremendous number of data APIs. (For the full list, see https://developers.google.com/gmail/api/v1/reference).

The Avanan platform uses the following resources:

- Messages
- Labels
- History of changes
- Attachments

Google Drive

Google Drive offers a tremendous number of data APIs. (For the full list, see https://developers.google.com/drive/v3/reference/).

The Avanan platform uses the following resources:

- Files and Folders metadata (not include file contents)
- Users and Groups metadata
- Permissions
- Changes (not include content of files changed)
- Channels
- Tokens
- Applications

Operation Modes

The Avanan Platform initiates by fetching all emails, attachments, files, and folders metadata in a *bootstrap* process. The bootstrap ensures the customer's dedicated virtual appliance has the same cloud state.

The cloud state used by Avanan tools are composed by the following entities:

Gmail

- Users
- E-mails
- Attachments
- Labels used in e-mails

Once the cloud state is saved, The Avanan Platform starts monitoring the changes for each user. To track each change for each user in the cloud, Avanan uses the following channels:

- Subscribe each user to Google Push Notifications for new messages (https://developers.google.com/gmail/api/guides/push)
- Fallback to polling each user history of changes, each minute if Push Notifications fails (https://developers.google.com/gmail/api/guides/sync)

Google Drive

- Users
- Groups and Memberships
- Tokens
- Apps
- Files and Folders
- Permissions

Once the cloud state is saved, The Avanan Platform starts monitoring the changes for each user. To track each change for each user in the cloud, Avanan uses the following channels:

- Subscribe each user to Google Push Notifications for changes (https://developers.google.com/drive/v3/web/push)
- Fallback to polling each user, each minute if Push Notifications fails (https://developers.google.com/drive/v3/web/manage-changes)
- Subscribe each user to Google Reports API to get its activities related to permissions, authorization to external apps and tokens. (https://developers.google.com/admin-sdk/reports/v1/get-start/getting-started)

Resolved Data

The following table lists the data that is retrieved from Gmail and Google Drive and how it is stored on the Avanan platform. Within Avanan's infrastructure, each customer receives a dedicated server environment, with each customer's data processed and stored within separate customer-dedicated virtual appliances. (There is no multi-tenancy.)

Data	How it is stored
User information: name, groups, phone, etc.	Saved in the customer-dedicated virtual appliance
Message/Attachment: name, size, hash, permissions, etc.	Saved in the customer-dedicated virtual appliance. Permission fields also point to the relevant users.
File/Folder: name, size, hash, permissions, etc.	Saved in the customer-dedicated virtual appliance. Permission fields also point to the relevant users.
Message/Attachment content	If a policy is configured to scan content for malware, DLP or other services that require file-scan, the content is downloaded to dedicated appliances, scanned and removed. The content is not cached or saved by Avanan. Only the scan result is saved in the customer-dedicated virtual appliance.
File Content	If a policy is configured to scan files for malware, DLP or other services that require file-scan, the file is downloaded to dedicated appliances, scanned and removed. The content is not cached or saved by Avanan. Only the scan result is saved in the customer-dedicated virtual appliance.
Activities: Send/Receive emails	Saved in the customer-dedicated virtual appliance
Activities: type (file, login, ...) user, item (file/folder), action (upload, download, share), time, IP, etc.	Saved in the customer-dedicated virtual appliance
Site data: domain name, company name, configuration params, etc.	The list of parameters configured in the corporate Google account that are relevant to the Avanan operation are saved in the dedicated virtual appliance.

About Avanan

The Avanan Cloud Security platform was developed to directly address the concerns associated with cloud adoption security. By employing a layered security approach, Avanan can catch security threats that a single security vendor would miss when used on its own. Deployed in minutes, the Avanan Platform is completely out of band, with no need for a proxy or endpoint agent.

info@avanan.com