

Cloud and Email Security

Because Cloud is the new Endpoint

Anti-Phishing and Anti-Malware with AI and Machine Learning because email is the No. 1 method used by hackers, your customers need the strongest protection against malware and phishing. Avanan's patented security connects to the cloud via API and blocks malicious emails before they reach the Inbox. It also protects collaboration apps; including Onedrive, ShareFile, Slack, many others. And, with its 5-minute deployment, **Avanan is easy to install.**

“

When looking for an anti-phishing solution everything we initially found had too many false positives and required too much management. Solutions Granted suggested their AVANAN solution and it has been terrific. Almost zero false positives and incredibly easy to setup and manage. It's been months since I had to go in and release an email. Also, we use the geo location feature to consistently present value to our clients which has been helpful.

— Isaac Levy, CTO. Blueswitch

”



MULTI-TENANCY CONSOLE

Easy to use and manage platform

CONSUMPTION BASED

Simple self-provisioning

FULL-SUITE PROTECTION

Security for all your collaboration apps

PROTECTION FROM

Ransomware, account takeover, BEC, supply chain attacks

SUPERIOR CATCH RATE

99.2% reduction in phishing attacks reaching the Inbox

UNIQUE ALGORITHM

Looking for over 300 indicators of phishing

Find out what a true partnership with a security provider is like

with a true enterprise cloud solution that works for MSP's - and priced for MSP's with a consumption model.

To learn just how good partnering with Solutions Granted can be, contact us today!

sales@solutionsgranted.com – 703.565-2395

ANTI-PHISHING

Most phishing attacks that bypass standard email security are zero-day threats coming from legitimate senders. To catch more of these advanced attacks, Avanan developed a unique machine learning algorithm that analyzes each aspect of an email, looking for over 300 indicators of phishing. The indicators analyze every piece of the email using features like Natural Language Processing (NLP), user impersonation detection, brand impersonation detection, sender spoof detection and more.

The algorithm also baselines the communication used in the organization, focusing on specific language and words. This allows SmartPhish's processing power to be tailored to the organization it protects, resulting in more accurate detections. The admin and end users can continuously train the AI by marking certain emails "clean" and others "malicious." Avanan's customer-specific configuration also learns from historical emails. Avanan's ability to fine-tune the AI is key to accurately identifying attacks and drastically reducing business disruptions.

ANTI-MALWARE

Avanan scans every link in the body of an email and within files, recursively looking for malware. Multi-vendor protection lets admins choose from AV and sandboxing vendors like FireEye, Check Point, Sophos, Palo Alto, SonicWall, Lastline and more. Data show that Check Point Avanan has the highest security effectiveness in the malware category.

Avanan's release-from-quarantine workflow allows admins to deploy the strictest anti-malware policies. When suspicious files are quarantined, users can ask to release them, and the admin can review a full sandbox report and threat emulation video that shows exactly what actions the malware takes when it is opened. This helps admins make informed decisions that take the needs of users into account.

DLP AND COMPLIANCE

Avanan offers best-of-breed DLP tools, such as Symantec and GTB. Our DLP policy can sync with on-prem DLP and existing DLP rules. When the end user sends a message where data leakage was identified, flexible workflows determine if the content is quarantined, the user is alerted, and/or the file is encrypted with IRM.

Avanan uses the industry's most advanced tools to identify and mark files containing confidential, financial, and personally identifiable information, including credit card numbers, social security numbers, and bank routing numbers. When necessary, Avanan adds a -classified suffix to the end of confidential messages or files. Avanan automates the encryption of sensitive files whether shared internally, via email, or public share without deploying new infrastructure, using protocols you already know and trust. It's compliant with PCI, FISMA, HIPAA, SOX, FERPA and GDPR.

FORENSIC TOOLS

Avanan's rich reporting is available at a glance on the dashboard homepage, and its custom queries are flexible, which speeds up the pace of a forensic search. Admins can search by sender, subject, recipient or attachment name. Within the query tool, admins can click on any "Sender" or "Recipient" to see a user profile detailing their top collaborators, whether they are internal users or external partners, and if their account is enabled with Avanan.

Avanan presents users with detailed alert messages, promoting a culture of security at every organization. Users can report threats, learn about potential attacks from automated alerts, and request emails to be restored from quarantine (pending admin approval). Clicking on "Subject" reveals an email profile, with detailed information on the email header, attachments and all the links in the body and attachment. The query enables admins to quarantine individually or en masse. To investigate threats further, admins can select "Analytics" in the main navigation or document the restore requests submitted by users whose attachments have been flagged as potentially malicious.

ACCOUNT TAKEOVER PROTECTION

Avanan has a unique combination of abilities. From real-time prevention, historical breach detection, and adaptive false positive filtering, Avanan provides the most advanced account takeover protection.

Upon deployment, Avanan automatically baselines safe behavior on a per-user, per-company basis. Avanan captures historical information to create a model of each user, as well as an organization's custom threat profile.

Avanan also provides a login map showing both suspicious and safe logins. When a suspicious login is detected, Avanan automatically sends alerts. Each alert can easily become a geo-restriction static layer, blocking all logins from where the specific business would normally not be conducted.

Within each SaaS, Avanan monitors over 100 event indicators and correlates them to identify compromised accounts. Machine learning algorithms use these indicators to find attacks and filter out false positives.



703.565.2395

Toll Free: 800.619.8481

solutionsgranted.com

sales@solutionsgranted.com

POWERED BY:  AVANAN