

# Cloud Threat Analytics

Our Cloud Threat Analytics offering leverages a combination of technologies, our A.I. based SIEM, and our 24/7/365 US based SOC to detect both new and known cyber threats inside of SaaS applications. Our SOC team actively monitors user activity and behavior inside of SaaS environments, providing real time actionable notifications of security risks.

“

One of our biggest concerns (as we moved customers to Office 365) was extending our security to the cloud environment. The Solutions Granted Threat Analytics service was just what we needed. In the first two weeks of deployment, with one of our clients, the Solutions Granted Team caught a malicious login from another country. We were able to secure our customers immediately. Thanks to the Solutions Granted Team, for helping us better protect our customers.

— Todd Creek, CEO Dura-Tech

”



## KEY FEATURES

- 24x7 Cloud Monitoring across multiple SaaS platforms
- Managed Investigations to reduce alert fatigue
- Notifications within minutes to prevent the escalation of threats
- Powerful reporting of user behavior and events
- 1 year log retention

## MONITORED SaaS APPLICATIONS



**Find out what a true partnership with a security provider is like**  
with access to our team for not only visibility but response from our fully manned 24/7/365 SOC.

To learn just how good partnering with Solutions Granted can be, contact us today!  
**[sales@solutionsgranted.com](mailto:sales@solutionsgranted.com) - 703.565-2395**

## USER LOGIN ANOMALIES

### LOGINS FROM UNAPPROVED LOCATION

Notification of when an account is logged in from outside an approved location.

### CONDITIONAL ACCESS VIOLATION

Notification of when an account has been successfully accessed from a region where access is intended to be restricted. The event indicates that the account name and password have been used successfully and possibly by a malicious party.

## USER ACTIVITY ANOMALIES

### EMAIL FORWARDING RULES

Monitoring for rules that will forward emails to outside of the domain.

### MULTIPLE LOGIN CONNECTIONS FROM DIFFERENT IP ADDRESSES

Notification of when different IPs are logged in to the same account.

### USER RESTRICTION EVENTS

The default security policy has detected unusual activity on the account and has restricted email sending functionality.

## ADMIN ACTIVITY ANOMALIES

### ADMIN ROLE CHANGES

Notified when a user is added to an admin role.

### MULTI-FACTOR AUTHENTICATION CHANGES

Notification if a user's MFA is disabled due to a compromise or verification if an admin is abusing their role.

## LOGGED EVENTS

Account Logins (Successful, Failed)

File Events (Download, Deleted, Emptied from Recycle Bin, Permanent Deletion, Modified, Upload, Opened)

File Event Anomalies

File Sharing (External, Internal)

Password Resets

SaaS Integrations

User Account Creation & Deletion

Policy Events (Security Group Change, Security Policy Change)

Unknown Actor Trying to Access the Domain

Multiple Password Resets

Singular Account Locks



703.565.2395

Toll Free: 800.619.8481

[solutionsgranted.com](https://solutionsgranted.com)

[sales@solutionsgranted.com](mailto:sales@solutionsgranted.com)

POWERED BY: **SaaSAlerts**