SONICWALL

Cloud Threat Analytics

Our Cloud Threat Analytics offering leverages a combination of technologies alongside our AI-based SIEM and our 24/7 Security Operations Center (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 Cloud Threat Analytics service was just what we needed. In the first two weeks of deployment, with one of our clients, the SonicSentry team caught a malicious login from another country. We were able to secure our customers immediately. Thanks to the SonicSentry 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

Microsoft

Google Workspace

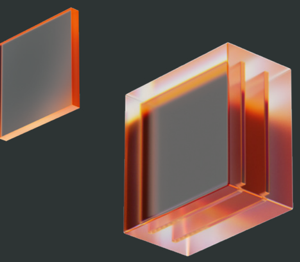
ITGlue

salesforce

slack

Dropbox

ninjaOne



Discover what true partnership with a security provider is like: Increase visibility across your ecosystem and access rapid response from our fully manned 24x7x365 SOC.

To learn about the wide range of benefits enjoyed by SonicWall SecureFirst partners, contact us today!
partnerdevelopment@sonicwall.com

MONITORED EVENTS AND NOTIFICATIONS

USER LOGIN ANOMALIES

LOGINS FROM UNAPPROVED LOCATIONS

Receive a notification when an account is logged in from outside of approved locations.

CONDITIONAL ACCESS VIOLATION

Receive a notification when an account has been accessed from a region where access is intended to be restricted. An event like this could indicate that the account name and password has been used successfully 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

Receive a notification 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

Receive a notification whenever a user is added to an admin role.

MULTI-FACTOR AUTHENTICATION CHANGES

Receive a notification if a user's MFA is disabled due to a compromise or admin troubleshooting. This can help identify insider threats and admins that may be abusing their role by disabling MFA as part of troubleshooting.

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

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®