

SmiKar Adds Insider-Risk Monitoring to SharePoint Online with Burrow

Burrow watches Microsoft 365 and SharePoint activity, alerts teams to insider risk, and keeps every record in the customer's own Azure storage.

MELBOURNE, VIC, AUSTRALIA, August 5, 2026 /EINPresswire.com/ -- [SmiKar Software](#) has expanded [Squirrel](#), its Microsoft 365 archiving platform, with [Burrow](#): an add-on that monitors SharePoint Online activity and flags behavior that looks dangerous, without the cost and complexity of a full SIEM.

As Microsoft 365 estates grow, so does the difficulty of knowing what is happening inside them. Most organizations can only piece together user activity after something has already gone wrong, and standing up a full security information and event management (SIEM) platform to watch SharePoint is heavy, expensive, and slow. Burrow closes that gap. It continuously monitors

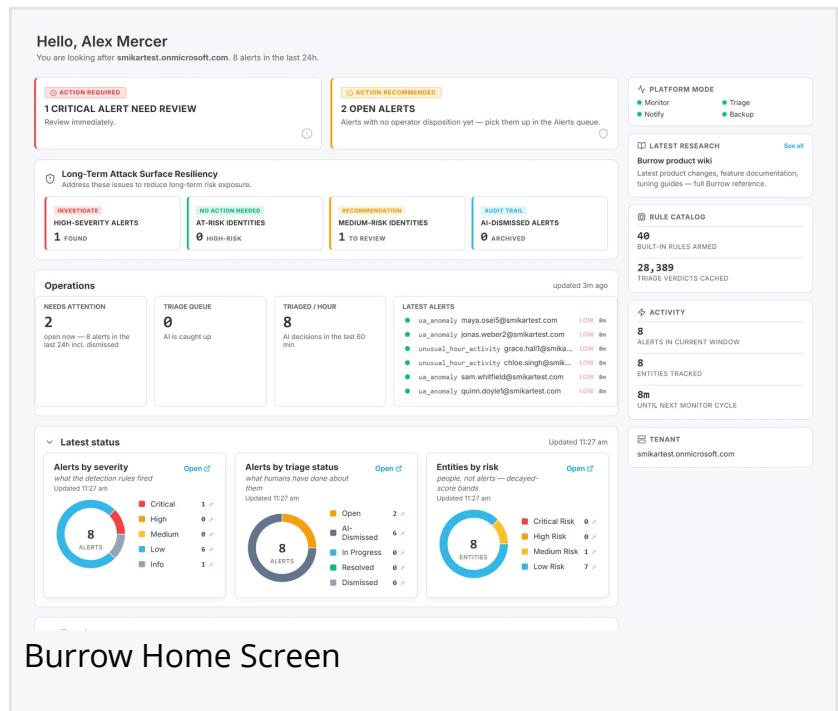
“

Burrow is about seeing risky activity as it happens, in plain language, and keeping the evidence in your own hands. It is your data, in your Azure, always.”

Mark Smith, Founder, SmiKar Software

security team can understand and act on in seconds, rather than a raw log entry to decode.

Burrow is also built to cut alert fatigue. Detections pass through layered analysis that combines



Burrow Home Screen

activity across SharePoint Online and raises alerts when it detects behavior worth attention, such as mass downloads, unusual access, or risky external sharing.

Every Burrow alert is built to be acted on, not just logged. Each one lands in the Burrow dashboard and is emailed to the people who need to see it, carrying a severity level, the specific MITRE ATT&CK technique it maps to, the evidence that triggered it, and a plain-English summary of why it matters, with automated checks that verify the figures against the source data. The result is an alert a busy IT or

deterministic rules, behavioral comparison against a user's own history and their peers, and an AI step that turns the facts into readable prose. Noise is filtered out before it reaches the team, so the alerts that land are the ones that matter.

For investigations, Burrow includes Hunt, a search built for HR, legal, and compliance teams. Users can look up a person and a date range and immediately see downloads, shares, permission changes, and access events in SharePoint, making it straightforward to answer questions such as whether someone ever accessed a particular site, produce an external-sharing audit, or export a point-in-time activity history for a case.

Like the rest of the platform, Burrow follows the principle that sets SmiKar apart: customers keep their own data. Audit records are held in the customer's own Azure storage, so organizations retain full ownership and control, with no third-party vendor holding a copy. Burrow is delivered as a fully managed service and needs only one-time, read-only consent to begin.

Burrow is an add-on for Squirrel, SmiKar's SharePoint archiving platform, and sits alongside the company's departed-user archiving product, Chipmunk. Squirrel archives inactive SharePoint content into the customer's own Azure storage, cutting storage cost while keeping files searchable and self-service restorable, and remains compatible with Microsoft Purview. Chipmunk preserves the Microsoft 365 data of

Behaviour exceptions

Silence — expected activity from these accounts is auto-downgraded or suppressed.

Tell the AI triage worker "This user + category combo is expected" so matching alerts get auto-downgraded without a Burrow AI call. Use for service accounts and well-known benign patterns. Wildcards (*) supported on the user pattern.

ADD EXCEPTION

Examples: appsharepoint* + ua_anomaly (SharePoint automation accounts hit many UAs) · svc-* + unusual_hour_activity (service accounts run 24/7) · backup-* + * (suppress all alerts for backup automation)

user_pattern (wildcard ok)

*

downgrade

reason (shows in audit log)

Add

ACTIVE EXCEPTIONS 2

appsharepoint*

SUPPRESS

Signed in from a country not seen before on this account. The s...

Remove

appsharepoint

SUPPRESS

Signed in from a country not seen before on this account. The s...

Remove

History

Disposition audit trail — every status change on every alert

analyst contains...

All statuses

alert key contains (user|category)...

82,192 entry/entries page 1 of 411

WHEN	STATUS	BY	ALERT KEY	NOTE
2d ago	ACK	alice.morgan@smikartest.com	elena.rossi@smikartest.com/risky_s...	inline change from alerts list

Prev

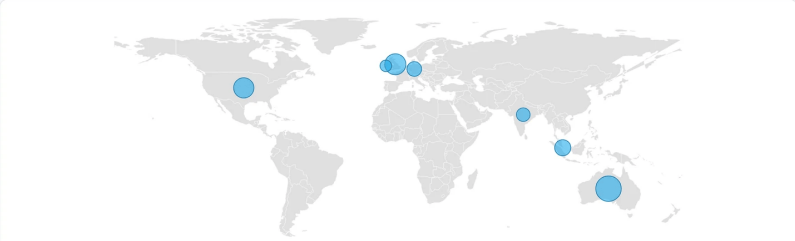
Next

User Exceptions

Known Networks

auto-learned corporate egress

A network here has been seen signing in for 3+ different users, so Burrow treats it as shared corporate infrastructure — an office gateway, VPN, or cloud proxy (e.g. Zscaler) — not one person's location. These are excluded from per-user sign-in geo, so they never trigger a "new country" alert. Click a country on the map to filter, or a network row to see who signs in from it.



Shared egress points by country (dot size = users). Click a dot to filter the table.

7 shared network(s) · updated 05/08/2026, 9:40:00 am

☐ show networks still learning

Search network / country...

CSV

NETWORK	COUNTRY	DISTINCT USERS	LAST SEEN	STATUS
283.0.113.0/24	AU	68	2026-08-05T09:31:00	shared egress — excluded
198.51.100.0/24	GB	41	2026-08-05T09:28:00	shared egress — excluded
192.0.2.0/24	US	37	2026-08-05T09:22:00	shared egress — excluded
283.0.113.128/25	SG	19	2026-08-05T08:57:00	shared egress — excluded
198.51.100.64/26	DE	14	2026-08-05T08:41:00	shared egress — excluded
192.0.2.128/25	IN	11	2026-08-05T08:12:00	shared egress — excluded

Known User Networks

System Activity

25 of 412 entries · last 48h

What Burrow has been doing on your behalf — emails sent, alerts quietened (and why), scan cycles, incidents scored, and self-healing actions. Read-only.

All

Emails

Suppressed

Scans

Incidents

System

filter — user, rule, reason...

2026-08-05

09:38:12

Emailled data_exfiltration_high -- henry.novak@smikartest.com

5m ago

09:35:02

SharePoint scan wrote alerts (18KB)

8m ago

09:30:44

Suppressed mass_deletion_med -- app@sharepoint - entity_exception

13m ago

09:27:19

Incident scored high -- rosa.iglesias@smikartest.com (4 alert(s) across 2 rule(s))

16m ago

09:22:07

Suppressed unusual_hour_activity -- maya.osei@smikartest.com - below_min_severity

21m ago

09:18:33

Emailled incident card -- rosa.iglesias@smikartest.com

25m ago

09:14:51

Azure AD scan wrote alerts (6KB)

28m ago

09:06:28

Suppressed risky_sharing_external -- liam.fraser@smikartest.com - auto_downgrade

37m ago

09:00:15

Health probe passed for all background services

43m ago

08:53:40

Suppressed behavioral_deviation -- elena.rossi@smikartest.com - lim_dismissed

50m ago

08:45:22

SharePoint scan wrote alerts (31KB)

58m ago

08:38:09

Emailled anon_link_used -- priya.nair@smikartest.com

1h ago

08:27:55

Suppressed ransomware_signature -- SHAREPOINT\system - entity_exception

1h ago

08:13:31

Incident scored low -- jonas.weber@smikartest.com (3 alert(s) across 3 rule(s))

1h ago

07:59:04

SharePoint scan wrote alerts (12KB)

1h ago

07:42:18

Suppressed aad_password_spray -- ip.203.0.113.44 - auto_downgrade

2h ago

07:21:47

Restarted a background service after it stopped responding

2h ago

06:58:12

Emailled malware_in_library -- tara.mcbride@smikartest.com

2h ago

06:40:38

Azure AD scan wrote alerts (9KB)

3h ago

06:15:26

Suppressed data_exfiltration_med -- chloe.singh@smikartest.com - cooldown

3h ago

Burrow System Activity Monitor

departed employees so licenses can be reclaimed without losing information.

"Most tools tell you what happened after something goes wrong," said Mark Smith, founder of SmiKar Software. "Burrow is about seeing risky activity as it happens, in plain language, and keeping the evidence in your own hands. Everything we build follows the same rule: it is your data, in your Azure, always."

Founded in 2015, SmiKar Software is a Microsoft Partner listed on the Azure Marketplace, specializing in Microsoft 365 data management. Its products help IT, security, and compliance teams at organizations worldwide control storage cost, preserve information, monitor activity, and stay in command of their own data.

Burrow is available now as an add-on for the Squirrel platform. To learn more, visit smikar.com.

About SmiKar Software

SmiKar Software builds purpose-built tools for Microsoft 365 and SharePoint Online, helping organizations reduce storage cost, preserve data, and monitor activity while keeping everything in their own Azure environment. Founded in 2015 and a registered Microsoft Partner on the Azure Marketplace, SmiKar serves organizations worldwide across finance, healthcare, government, engineering, and more. Learn more at smikar.com.

Contact: sales@smikar.com

Mark Smith

SmiKar

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/931804296>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.