GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

U

UEBA: How User and Entity Behavior Analytics Works

UEBA compares current user and entity activity with baselines and peer behavior. An anomaly raises a question for investigation; it is not proof of compromise.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	3 min

User and entity behavior analytics (UEBA) uses identity, endpoint, network, cloud, application, and data-access events to model expected activity and highlight meaningful deviations. “Entity” expands the older term UBA beyond people to devices, service accounts, applications, workloads, and other resources.

UEBA is an analytics capability, not a verdict engine. A high risk score helps prioritize an investigation; it does not establish intent or prove that an account is compromised.

How UEBA works

1. **Collect:** ingest reliable authentication, authorization, endpoint, network, cloud, and data events.
2. **Resolve entities:** connect usernames, devices, IP addresses, sessions, and service identities to the correct records.

3. **Build context:** learn normal hours, locations, devices, resources, volumes, sequences, and peer-group behavior.
4. **Detect deviations:** apply statistical models, rules, machine learning, and threat context to new activity.
5. **Aggregate risk:** combine related anomalies into an entity timeline or score for analyst review.
6. **Learn from outcomes:** tuning and investigation feedback reduce noise and expose missing telemetry.

Microsoft's current UEBA guidance similarly emphasizes learned behavior, anomalies, entity context, and investigation.

What UEBA can help detect

- a valid account signing in from an unusual device and immediately accessing sensitive data;
- a service account beginning interactive use or touching systems outside its role;
- unusual privilege changes followed by mailbox rules, token creation, or bulk download;
- a device scanning peers or contacting resources it has never used;
- insider misuse that stays within valid credentials but departs from role and peer behavior;
- a sequence of individually low-severity events that becomes suspicious when correlated.

UEBA vs. SIEM, EDR, and identity protection

A SIEM collects and correlates events. EDR records and responds to endpoint behavior. Identity protection evaluates sign-ins and accounts. UEBA can analyze data from all of them and add longitudinal behavior and peer context. Many modern platforms embed UEBA, so it may not be a separate product.

UEBA does not replace log collection, access control, MFA, EDR, or incident response. Models cannot detect what their source data does not record, and automation should not disable an employee or production service solely because of an unexplained score.

Practical deployment workflow

1. Choose a small set of high-value use cases and define the decision each alert should support.
2. Onboard accurate identity, administrator, endpoint, cloud, and sensitive-data sources; verify clocks and retention.
3. Document entity ownership, peer groups, service accounts, expected travel, maintenance windows, and seasonal work.
4. Run in observation mode, measure false positives, and tune narrow causes rather than excluding entire teams.
5. Create investigation playbooks that retrieve the raw events behind each model result.
6. Enable automated containment only for well-tested, reversible cases with safeguards.

How to investigate an alert

Confirm the identity and asset first. Review the baseline period, peer comparison, original events, device health, authentication method, privilege level, data accessed, and activity before and after the anomaly. Ask whether travel, a new role, automation, software deployment, or missing telemetry explains it. Preserve the result and feed confirmed benign or malicious outcomes back into tuning.

Limitations and privacy

- new employees and rare but legitimate work may have weak baselines;
- model drift and organizational change can raise noise;
- vendor scores may be difficult to explain without raw evidence;
- behavior records can reveal sensitive employment and personal information;

- retention, access, acceptable use, and human review require documented governance.

Measure confirmed detections, investigation time, source coverage, repeat false positives, and missed incidents—not the number of anomalies generated.

UEBA FAQ

Does UEBA require AI?

No single algorithm defines UEBA. Products may combine rules, statistics, peer analysis, and machine learning.

How long does baselining take?

It depends on the behavior, data quality, seasonality, and product. Continue using deterministic detections while baselines mature.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com