



White Paper | August 2020

# **The Ava Reveal difference – identifying and managing insider risks in a privacy-first world**

## Summary

Stricter data protection laws have made safeguarding sensitive information a priority for many organizations. However, this gets complex when your security controls include user activity monitoring.

With Ava Reveal's industry-leading solution of pre-built data minimization techniques, such as pseudonymization and anonymization (partial and full redaction), you can now detect and mitigate threats while maintaining the confidentiality of users.

## What is personal data?

Personal data allows you to identify a particular person—for example, by name, identification number, or a combination of factors, such as job title and location.

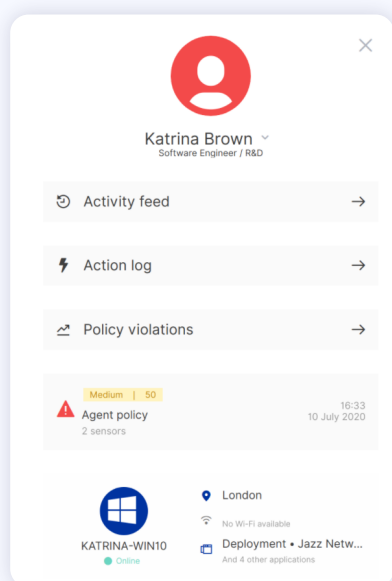
## What data minimization techniques are available?

Pseudonymization replaces identifying information with realistic, artificial data. For example, a user's first and last name would be replaced with a fictitious first and last name which operators could refer to during threat investigations.

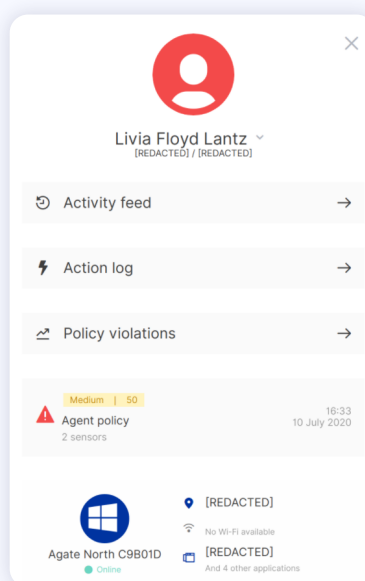
Anonymization redacts or removes identifying information from the operator's view. Anonymized data, for example, includes the user's email address, department, and title as well as sensitive fields within security events, such as a user name within a file

path. By employing pseudonymization and anonymization, operators can uncover risks in your organization, but cannot attribute events to particular users. Personal data that has been anonymized is no longer considered personal data and, for example, is no longer governed by the GDPR.

Ava Reveal combines the two data security techniques allowing you to protect the identity of your users without disrupting operator workflows.



Cyber Passport without anonymization and pseudonymization enabled.



Cyber Passport with anonymization and pseudonymization enabled.

## Why maintaining data protection is important

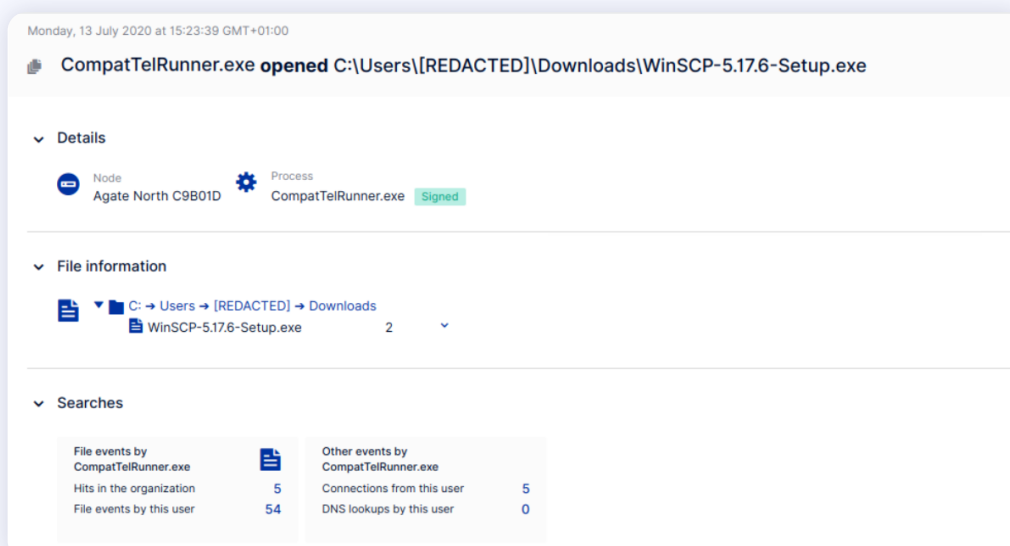
Ava takes privacy seriously and complies with various regulations, including GDPR. GDPR encourages applying technical measures to protect personal data for the following reasons:

- **Article 6 (1) (f)** permits processing personal data for legitimate interests, with protecting information security regarded as such (article 49).
- **Recital 49** states while maintaining information security is regarded as a legitimate interest, organizations are still obliged to apply technical and organizational measures to protect personal data, and are also required to apply additional
- “technical measures” to ensure that the security measures themselves maintain the protection of personal data. Such measures include, inter alia, minimization, and pseudonymization of personal data.
- **Article 25 (1)** makes data minimization and pseudonymization a central feature of the requirement for data protection by design and by default.
- **Article 32 (1) (a)** makes pseudonymization as well as encryption a technical technique for ensuring the security of processing personal data.

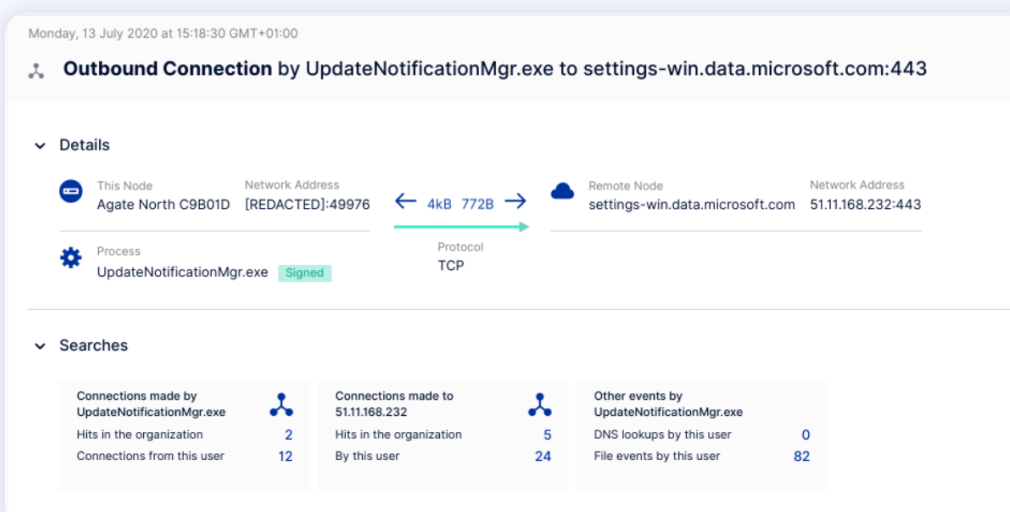
## The Ava difference

- Reveal strikes the careful balance between hiding identifying information and allowing you to see key data to protect your organization. For example, Reveal does not remove all sensors and events. However, Reveal redacts or masks the personal data within them.
- Reveal allows operators to be assigned a role with the “Pseudonymization” perspective. Higher privileged operators can view users’ true profiles to respond to incidents.
- This, with minimal impact to the usefulness of the event logs thus enabling operators to continue monitoring suspicious behaviors.
  1. **Pseudonymization** (e.g., Name Surname -> Joe Snow)
  2. **Full redaction** (e.g., the monitored node’s IP address)
  3. **Partial redaction** (e.g., in a file or directory path, “/Users/[REDACTED]/G:\My Drive\Compliance GDPR”
- The mapping between artificial identifiers and real personal data is not available to any operators, meaning pseudonymization is secure.
- Using artificial identifiers is a powerful way of hiding personal data, because it maintains referential integrity and means that the activity of a single user or device can be tracked and investigated, without knowing who they are or what device they are.
- All the Reveal features, such as policy reports, sensors, actions, cases and power searching are available, allowing full threat detection and mitigation without revealing personal data.

The screenshot on the following page illustrates the minimization techniques in use. Where pseudonymization has been implemented, the username, department, personal computer name are replaced with aliases. Where anonymization has been implemented, information is hidden with minimum effect to the usefulness of the data in hand.



A partly redacted (anonymized) event in pseudonymization mode.



A fully redacted (anonymized) event in pseudonymization mode.

Pseudonymization and anonymization allow operators to work effectively—hunting for threats and making initial incident analyses—without compromising the privacy of users. Operators with this access can also collaborate with higher-privileged operators who have

complete visibility of user information and can take action if required.

Even though pseudonymization masks identifying information, in smaller organizations it might still be possible to attribute events to users.

## Conclusion

With our data protection and minimization techniques enabled, Reveal is a powerful solution that can help you identify, manage, and prevent threats, and objectively investigate incidents using the data that matters.

### Sources

1. Article 6 (1) (f) <https://gdpr-info.eu/art-6-gdpr/>
2. Recital 49 <https://gdpr-info.eu/recitals/no-49/>
3. Article 25 (1) <https://gdpr-info.eu/art-25-gdpr/>
4. Article 32 (1) (a) <https://gdpr-info.eu/art-32-gdpr/>



Unified Security

Ava is a global technology company with offices in the UK, Norway, and the USA. We exist because we believe that we can create a better, smarter way to deliver security.

We inject intelligence into our approach to security and all our solutions. We help organizations see, understand, and act on their surroundings to protect their people, business, and reputation in real-time.

We founded Ava Cyber in 2016 and Ava Video in 2018 and the two companies merged in 2020 to become a unified security provider with extensive capital investment from Ubon Partners.

To learn more about our innovative solutions, and how you can enjoy proactive security, visit our website or schedule a demo with a member of our sales team at: **[sales@ava.uk](mailto:sales@ava.uk)**.

**[www.ava.uk](http://www.ava.uk)**