Summary brochure - September 2020

Ava Reveal

Human-centric security in a privacy-first world

Ava Reveal

Preventing insider risks with a human-centric solution

Companies tend to overestimate the impact a malicious outsider has on an organization. What the malicious outsider wants–direct access to sensitive data–is exactly what insiders such as employees, contractors, and third parties have by design, and hence here lies the real risk.

As malicious insiders are responsible for the costliest data breaches, and human error is considered the main cause of data breaches, Reveal is designed with human behavior in mind. Reveal strengthens your defense against insider risks–malicious, careless, and accidental.

Make your IT security come alive

Autonomously train your workforce on the organization's Information Security Policy or Acceptable Use Policy. Incident-based training rectifies bad cyber hygiene practices and unwanted behavior, e.g. downloading dangerous files from Chrome, visiting HTTP or unauthorized websites, inserting unauthorized USB storage devices, and connecting to unsecure or open Wi-Fi networks. The training replaces the need for costly and inefficient periodic, classroom training sessions where you have to take employees away from their day-to-day work.

Reveal identifies emerging security threats by gathering and analyzing millions of events each day against a series of sensors:

- Machine learning sensors
- Behavioral analytics sensors
- Policy sensors

As Reveal Agents continuously record events, specific models of behavior are built for users over time. These models enable Reveal to recognize abnormal and suspicious activity and raise alarms for perceived threats.

Security analysts can protect against a breach or attack by initiating actions. Depending on the severity of the threat, analysts can take a screenshot of a user's computer screen, kill and block connections to a device, or lock a device's keyboard and mouse.

What our customers use Reveal for

Identify and manage insider risks

Protect against data loss

Bridge compliance gaps

Make the static IT policy come alive

Secure the remote workforce

Key features

Two powerful methods of detection coupled with immediate response.

Policies

Automate threat detection and response from day 1 with Reveal's policies. Reveal offers: both out-of-the-box (OOTB) and configurable policies that you can customize to align with your IT policies and security needs. Examples include:

- Detection of sensitive content sent/received via email*, copied from desktop applications, and transferred over video conferencing applications or to USB.
- Use of hacking, steganography, and other unauthorized tools
- Use of unsecured networks or connections
- Clearing of Windows event logs

Use policies for educational purposes—for example, displaying an on-screen message to a user upon connecting to an unsecured public Wi-Fi network, informing them that they are violating the corporate policy.

*Microsoft Outlook is supported on Windows. Other applications and platforms will be added in the future.

Machine learning

Reveal's breakthrough machine learning combines multiple algorithms that monitor user, entity, and network behavior to detect security threats. Examples include:

- DNS exfiltration and machine-generated DNS
- Keyboard typing pattern
- Unusual networks (phone tethering)
- Excessive printing

The machine learning generates statistically robust models of behavior from various time series datasets. This approach enables machine learning to build models that are tailored to each individual in an organization and achieve better predictive performance.

Real-time actions

Locks a computer if malicious intent is identified.

Isolates an infected computer or server to prevent malicious software from spreading.

Takes a screenshot to capture an image of a user's desktop.

Displays message to prompt an end user with a custom message.

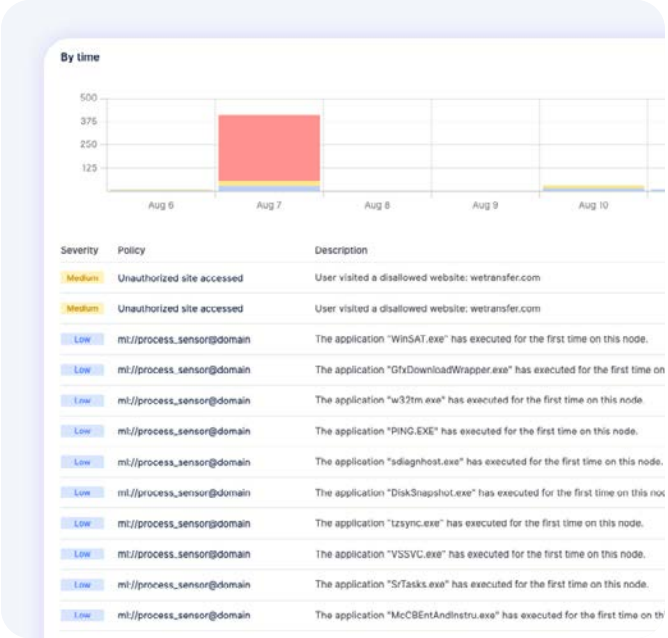
Real-time alarms

Instantly get alerted when threats are detected by machine learning, policy, and behavioral analytics sensors. To ease the investigation into perceived threats, the Alarms page shows key details for each alarm, such as severity score, the time and date the alarm was raised, and motion screenshots if activated.

Easily understand relevant user behavior

Reports dashboard

Understand and transform your security posture with interactive sensor reporting by measuring threat risk, implementing new security strategies, and ensuring success. Use the policy reports to see which sensors were triggered the most across your organization and by whom, so you can assess the effectiveness of your existing security controls and identify areas for improvement. For example, a commonly breached policy could highlight cyber hygiene training gaps. After strengthening this part of your corporate security training program and further educating users, you could track their progress by verifying policy breaches decrease. To share security information with the executive team and others, reports can be exported to CSV.



Event monitoring

Reveal monitors a range of events to capture malicious and non-malicious behavior. For example, Reveal lets you monitor:

- Browser activity with the Reveal Browser Extension that allows you to be informed when a user visits URLs and uploads and downloads files.
- File activities, including when a file is opened, modified, closed, executed, deleted, or renamed. Reveal also provides details such as filenames, process-level information, and the local and external drives from which files were accessed.
- Keystrokes to automate your defense against keystroke injection attacks, unauthorized access, and more. Keystroke monitoring enables Reveal to identify security risks based on the manner and rhythm of typing on a keyboard.
- DNS requests, including the DNS answer and answer type, network addresses (destination and source), the communication protocol used, and process-level information, such as binary names and paths.
- Clipboard to detect when users copy or cut text from an unauthorized site, copy text from an unauthorized application, and paste text to an unauthorized site.
- Application usage, including which applications a user has open, when an application is in the foreground versus the background, and the usage duration.
- Activity to cut usage-based licensing costs driving unnecessary costs by identifying misused applications.
- Geographical locations using location mapping and Wi-Fi landscaping data.
- Wi-Fi to keep you informed of the wireless networks users connect to – thereby detecting when a user connects to Wi-Fi and identifying the SSID and BSSID.
- Printing activities, including the size, date and time of the print job, the filename, the number of pages, the printer name, and the printer port.

Network monitoring and interception

See and control network activity between devices across your organization. Reveal provides network information for connections made between managed computers to provide a layer of visibility into access control, making sure computers are not accessing or attempting to access unauthorized nodes. Reveal also provides network information for connections made between managed computers and external hosts to identify connections to unexpected locations that could either be malicious or not compliant with GDPR.

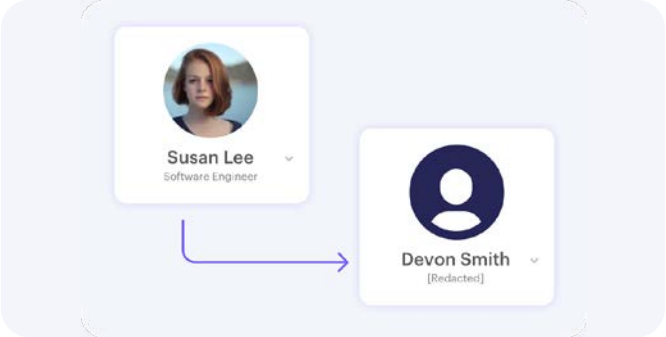
Email monitoring and blocking

Know who users are emailing, what is being shared, and block sending of sensitive attachments and intellectual property. The monitoring of inbound and outbound email activity for Microsoft Outlook protects against data loss and phishing.

Privacy-friendly insider risk solution

Pseudonymization and anonymization

With Ava Reveal's industry-leading solution of pre-built data minimization techniques, such as pseudonymization (information replaced with realistic, artificial data) and anonymization (information is hidden), you can detect and mitigate threats without compromising the privacy of your users, in accordance with legislation, e.g. GDPR.



Get the full picture during threat hunting—even without policy violation

A full paper trail during an incident investigation–even if data is deleted or evidence is destroyed during an attack. All the data is available in one place.

Power Search

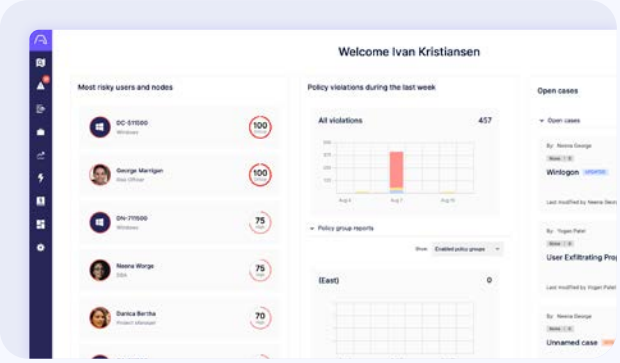
Reveal makes forensics and threat hunting easy where you can uncover user details in seconds. With robust search functionality, meaning you can hunt for threats across your network quickly and effectively. No query language knowledge is needed to search for a specific historical context. Ensure you comply with government and industry regulations by notifying the supervisory authority within a given timeframe after discovering a data breach.

Cyber Passport

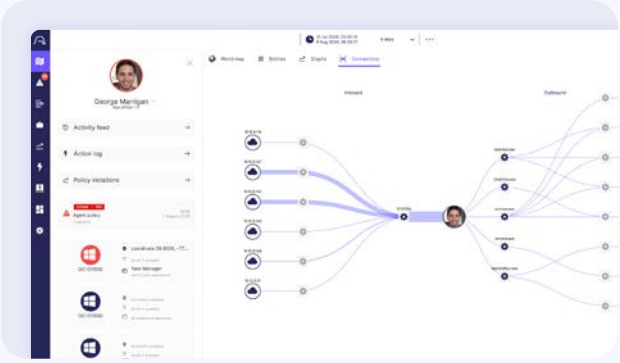
The Cyber Passport gives you powerful insight into users no matter where they are in the world. The Cyber passport attributes all data collected to a specific user, including general details about the entity, the Activity feed, the action log, policy violations, alarms, associated entities, and graphical representations of event data.

Different views

Reveal offers a range of useful views for risk mitigation and threat hunting.



Landing page: An at-a-glance view of suspicious users and managed nodes, recent policy violations, and active cases.



Connections view: The view enables you to virtually walk across the network, viewing a user or node's incoming and outgoing connections and related processes.

Cases

Uncover and remediate threats with ease using Cases. Designed to simplify threat hunting and forensic analysis, cases enable operators to identify suspicious events requiring investigation, and then collaborate on investigations for more informed decision-making and rapid response.

- Build a case over time by proactively adding events requiring investigation.
- Collaborate across team individuals can add alarms, sensors, events, comments, links, photos, and screenshots.

Activity Feed

The Activity Feed displays a stream of all user activities in logical sequence, including Wi-Fi connection, print, browser, file, and integration events, as well as connections, logins, DNS lookups, USB events, applications, and more.

Ava Analyst Services

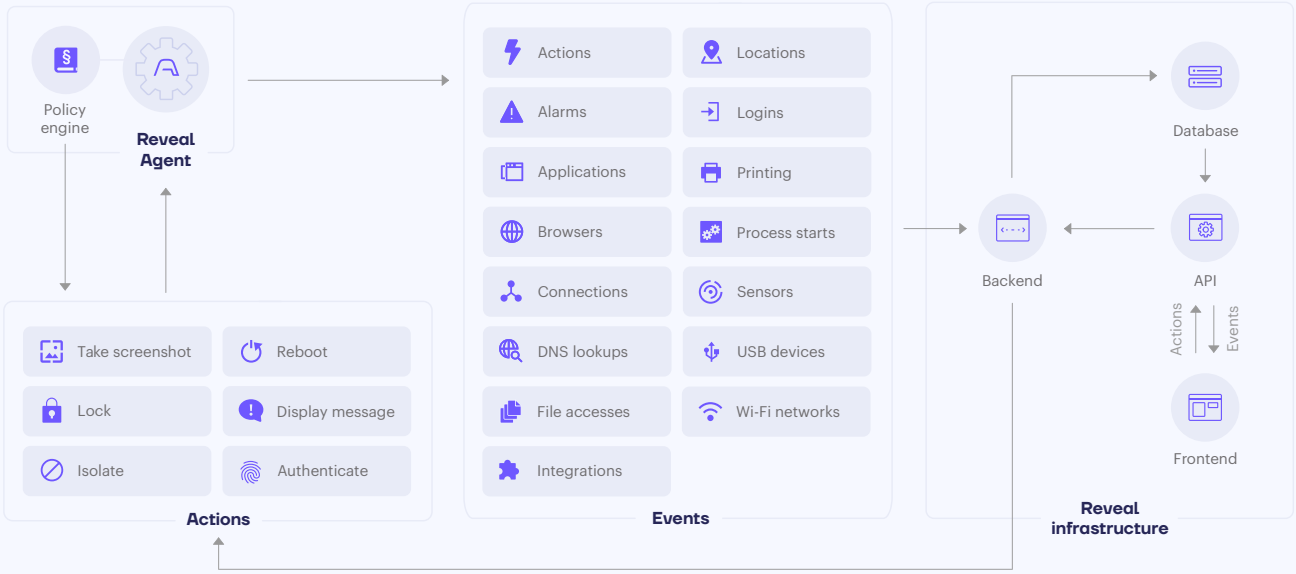
Ava's Analysts are experienced cybersecurity specialists with strong backgrounds in protective monitoring, CIRT, and threat intelligence with demonstrable security incident response experience.

Lean on our experts to:

- Boost your team's threat hunting with structured and unstructured analysis.
- Enhance the level of visibility and understanding of potential threats or incidents findings.
- Tailor the solution to your specific requirements by designing specific watchlists and customizing policies.

Try Reveal 30 days for free at www.ava.uk/cyber/trial

How it works



The Reveal Agent is deployed to Windows, macOS, and Linux computers and servers, both on-premises and in the cloud, where it collects granular behavioral information and reports it back to the Reveal Infrastructure for security threat analysis. The Reveal Agent spools events when there is no network connection and provides them to the Reveal Infrastructure upon reconnecting.

OS	Supported versions
Windows	• Windows version 7+ • Windows Server 2008 R2+
macOS	• OS X El Capitan 10.11+
Linux	• Red Hat Enterprise Linux 7+ • CentOS 7+ • Ubuntu 16.04 LTS and 18.04 LTS • Debian 8+

Unified Security

Ava exists 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 get the whole picture of their surroundings to protect their people, business, and reputation in real-time.

To learn more about our innovative solutions, and how you can enjoy proactive security, visit our website.

www.ava.uk