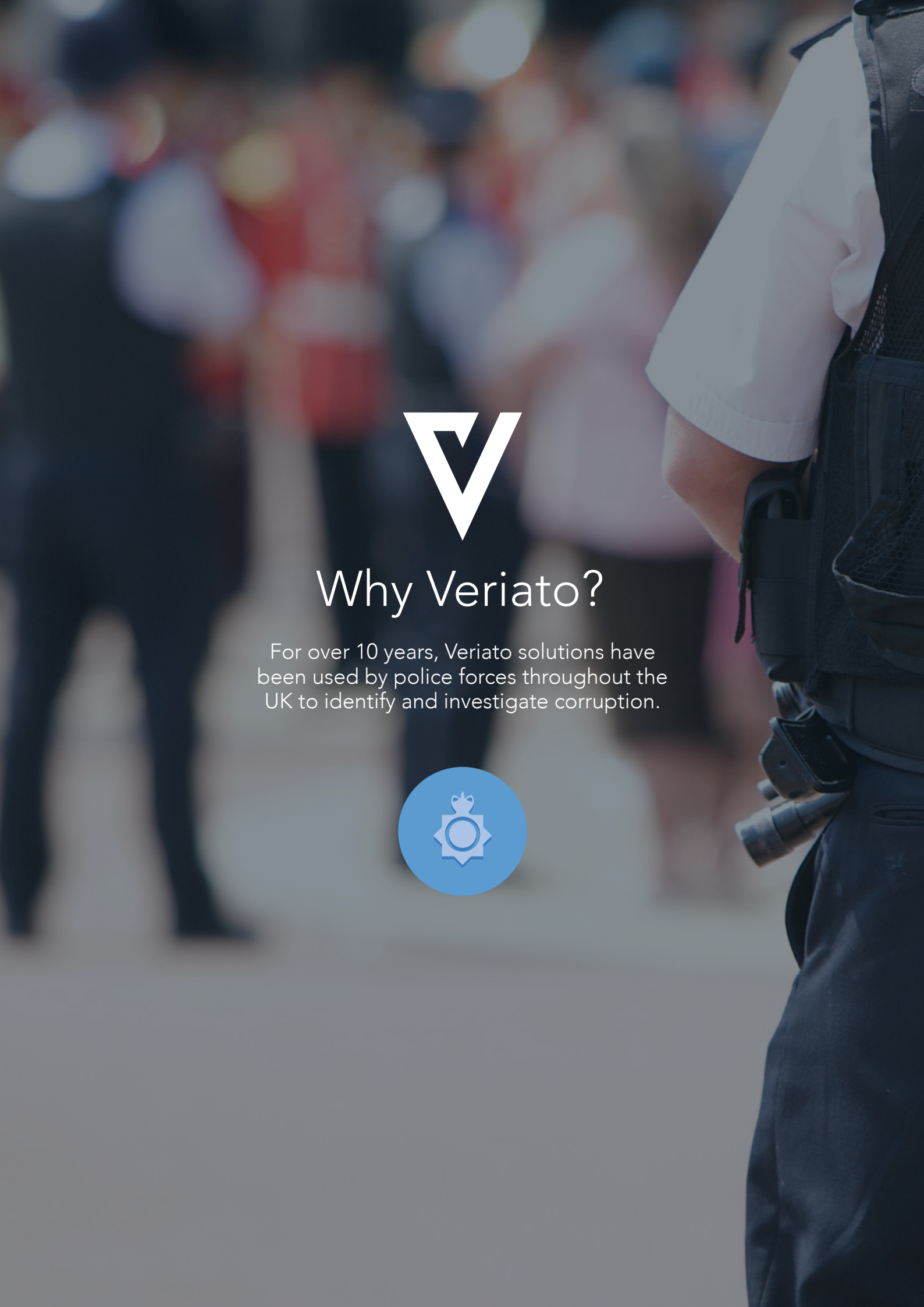


Why Veriato?

For over 10 years, Veriato solutions have been used by police forces throughout the UK to identify and investigate corruption.

Veriato produces software that collects and analyses human activity and behaviour, with alerting, reporting and review capabilities designed to enable early detection of problems and reduce the amount of time from detection through investigation to remediation.

IDENTIFYING CORRUPTION

According to Transparency International UK, 0.5% - 1% of UK police staff are corrupt

March 2015: (900,000 officers x 0.5% = 4,500 - 9,000 officers)[1]

In November 2014, HMIC published its force reports, which assessed the extent that forces have put in place arrangements to ensure its workforce acts with integrity.

The capability of UK institutions to tackle police corruption had progressed. However, HMIC condemned the relatively large number of investigations where no further action was taken, roughly two thirds of all investigations.

HMIC'S Mike Cunningham QPM noted that whilst many cases of police corruption are dropped due to being unfounded, "we cannot rule out that some of those allegations have not been properly inquired into or investigated."

Veriato collects detailed, context-rich information about user activity, and makes it available and understandable, without the need for expensive, specialized forensic expertise. With Veriato acting as a system-of-record, investigators are in possession of exactly the type of evidence they need to conclude investigations in a timely, accurate, cost and resource efficient manner.

[1] https://ico.org.uk/action-weve-taken/data-security-incident-trends/

Because Veriato solutions consistently deliver accurate evidence that stands up to challenge, they have been deployed in almost **40,000 organizations in more than 110 countries worldwide**. From household name companies through major educational institutions and government entities, Veriato is the system-of-record.

HMIC RECOMMENDATIONS & OBSERVATIONS[2]

Criminals seek information about themselves, competitors, investigations, tactics, prosecutions, witnesses, and intelligence sources to undermine law enforcement…

…forces that used the national assessment of the threat from corruption… had carried out a greater range of prevention activities, intelligence-gathering and investigations …are in a better position to understand the nature of the corruption threat they face and how best to respond to it.

…Disappointingly, we have found that fewer than half of all forces have an effective counter-corruption plan which demonstrates their understanding of the threat to their force from corruption, and their proposed activities to improve not only the prevention and identification of corrupt behaviours, but also their investigative capability …

…forces that do not have a process for using the range of information(data) that they hold miss opportunities to identify and prevent or investigate members of staff breaching the professional standards of behaviour or those susceptible to corruption …

…anti-corruption units should have the ability to conduct initial research on force computer systems including crime, intelligence and human resources systems…

…a small number of forces had anti-corruption units that were not staffed sufficiently to allow them actively to seek and gather intelligence about corruption.

Key Takeaway

The overwhelming majority of corruption investigations involve some element of unlawful access to data and information held on computer systems or disclosure of the information held on those systems. Monitoring the use of force computer systems is therefore vital in countering corruption. Communicating to the workforce that such monitoring takes place will help to discourage unauthorised access.

[2] Source: HMIC "Integrity Matters"

How can Veriato work for you?

By employing a combination of Veriato Recon and Veriato 360, you can implement a robust monitoring scheme - one that provides the vital insight into data and systems access required to counter corruption, without overtaxing your budget and infrastructure.

Veriato Recon is a unique offering; no other monitoring company offers anything like it.

Veriato Recon is an agent-based solution that performs two functions:

1. Collection and temporary storage of user activity data on the endpoint where the activity occurs

2. Analysis of user behavioral patterns and alerting on deviations from the norm that suggest a threat

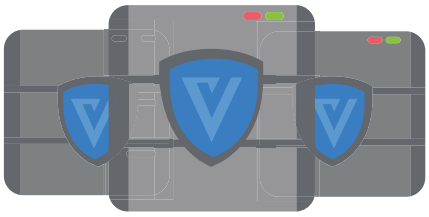
Veriato 360 levers the same agent, and performs these key functions:

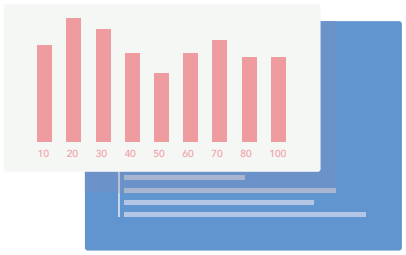
1. Extraction of the user activity data Veriato Recon has stored on the endpoint into a central database

2. Presentation of user activity data for use in investigations

Veriato has been in the business of watching and alerting on user actions since the late 1990's. We're proud of our track record, and we've applied lessons learned over the years to help us design a solution that possesses advantages our competitors can't match.

How can Veriato work for you?





Data Retention

Veriato Recon stores recorded user activity data securely and obsfucated on the endpoint. Data can be retained on the endpoint up to 90 days. This temporary retention supports the need to have detailed, context-rich activity history available when the need to conduct an investigation is discovered. The solution also stores meta data needed to maintain high quality behavioral baselines in a secure on-premise SQL database.

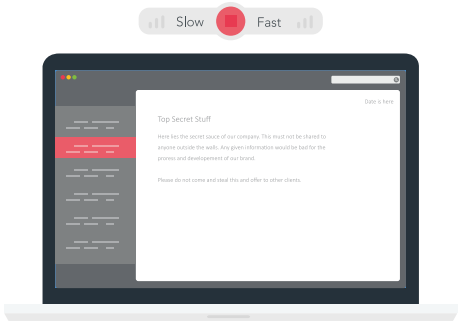
Veriato 360 stores recorded data in a secure on-premise database. Retention periods are customer configurable.

One of the most common questions asked at the onset of an activity and behavioral monitoring program is "how much storage will we need to deal with all of this data?" Please see "Storage Considerations on page 11" for a detailed look at the infrastructure requirements.

Data Analysis

Veriato Recon analyzes the user activity data collected, identifies behavioral patterns, and detects anomalies in established patterns that suggest risk or threat. The software looks for anomalies related to data access and movement, as well as psycholinguistic anomalies (changes in the way people communicate) that can act as early warning of elevated risk conditions. Veriato Recon is a User and Entity Behaviour Analytics solution.

How can Veriato work for you?



Data Capture

Veriato Recon and Veriato 360 lever a single, common endpoint agent to collect information and intelligence from the online and communications fabric of the organization. This agent has been refined since 1998, and has been deployed on millions of endpoints.

The agent records the activity you configure it to. The following options are available:

- Application / program usage
- Document tracking
- File transfers
- Network Activity
- Online searches
- Websites visited
- Email/Webmail/Chat/IM
- Login / Session Activity
- Keystrokes

The agent also captures screenshots, at fully configurable intervals. The Veriato data collector runs on Windows and Mac operating sstems, with coverage of the Android operating system set for Q4 2016.

Alerting, Reporting, and Review

Veriato Recon sends alerts when behavioural anomalies are detected. Alerts can be sent via direct integration to leading SIEM solutions, to any 3rd party solution that can ingest syslog, and via email to designated recipients

Veriato 360 sends alerts when customer defined events occur. Alerts can be sent via direct integration to leading SIEM solutions, to any 3rd party solution that can ingest syslog, and via email to designated recipients

The Veriato 360 dashboard enables use of Quick View panels that provide at-a-glance visibility into activity occurring within the organization. 100+ reports can be viewed, and / or scheduled for distribution to designated recipients. A global search capability enables rapid identification of event and activity data that meets the search criteria. Finally, video playback of captured screenshots is available, providing an exact record of what occurred.

THE VERIATO DIFFERENCE

Only Veriato can deliver the capabilities and advantages that Veriato Recon and Veriato 360 together offer. The two solutions are fully integrated, levering the same endpoint agent and operating out of the same database and central management console.

Employing a combination of these two offerings enables your force to deploy a robust monitoring program, with

- Significantly less infrastructure required than competing solutions
- A lower Total Cost of Ownership than competing solutions
- Integrated User Behavioral Analytics capabilities
- A proven track record of providing technology used successfully in support of investigations in literally thousands of organizations worldwide
- A proven track record supporting UK police forces
- A history of enhancing our solutions to meet the evolving needs of UK police customers
- The backing of a financially stable, growing technology company

TESTIMONIAL - VERIATO IN ACTION

Leicestershire Constabulary

A member of the staff at Leicestershire was responsible for a large-scale internal theft.

The defendant created a false alibi for themselves by fabricating an excuse to enter a secure limited access building: 'defendant' typed a simple sign to be placed in their vehicle 'when needed.' They wanted to laminate the sign and the laminator was in the secure building.

Whilst in the building they removed a key for a safe, which they used to steal from other premises.

According to Detective Sergeant Lee Ferguson of the Anti Corruption Unit, "Due to their expertise and knowledge of processes they were able to access large cash sums and remove without detection."

> "The software proved extremely useful to the prosecution case and resulted in guilty pleas."

To effectively cover their tracks, they needed a reason to re-enter the building to return the safe key. The defendant claimed that the sign they created and laminated contained a typing error, and they need to create and laminate a new copy without the error. This was the reason provided for re-entering the secure building to return the key.

Leicestershire ACU was able to prove the alibi false through use of Veriato 360. Keystroke recording, combined with screenshots recorded, unequivocally proved that there was NO typing error and the documents were identical. Though the defendant went through the theatre of the false alibi, they didn't include the typing error they claimed.

"The software proved extremely useful to the prosecution case and resulted in guilty pleas," said Ferguson.

- Contact details for DS Lee Ferguson can be made available at your request -

TECHNICAL INFORMATION

Storage Considerations

For a default recording profile, Veriato will record approximately 8 Mb per user per day (including screenshots captured every 30 seconds).

Policing guidelines (MoPI) suggest Police keep data used in an investigation for 6 years.

According to Transparency International UK, 0.5% - 1% of UK police staff are corrupt:

March 2015 (900,000 officers x (0.5% to 1%) = 4,500 to 9,000 officers)[3]

Policing guidelines (MoPI) suggest data used in an investigation be stored for 6 years. To provide an estimate of storage space required to support a recommended monitoring and retention program, we use two assumptions:

- the number of investigations conducted in total (including those resulting in a finding of no corruption) is either 5x or 10x the number of "corrupt officers" as per Transparency International UK
- each investigation involves 6 months worth of data

# OF OFFICERS	(0.5% X 5)	(1% X 5)	STORAGE SPACE REQUIREMENT (LOW)	STORAGE SPACE REQUIREMENT (HIGH)
5,000	125	250	1TB	2TB

# OF OFFICERS	(0.5% X 5)	(1% X 5)	STORAGE SPACE REQUIREMENT (LOW)	STORAGE SPACE REQUIREMENT (HIGH)
5,000	225	500	2TB	4TB

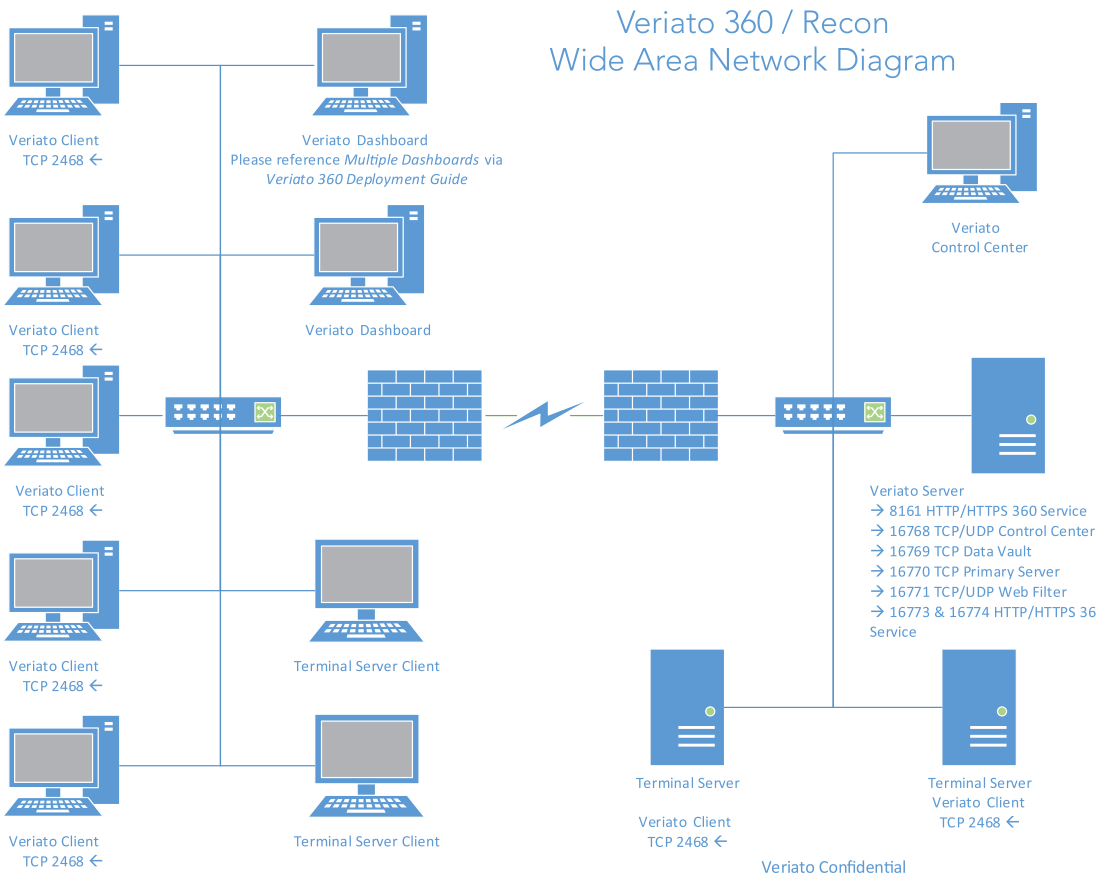
A key differentiator for Veriato is **Veriato Recon's** ability to securely, temporarily store user activity data on the endpoint that the activity occurred. This distributed storage architecture was designed to (a) insure that the detailed user activity data is available when needed to support investigations while (b) minimizing the resource impact on the IT infrastructure and budget. Other solutions Veriato has seen deployed within UK police forces require as much as 25 Mb of space per user per day, and do not have the ability to lever available storage on the endpoint to mitigate the overall additional storage requirement.

[3] https://ico.org.uk/action-weve-taken/data-security-incident-trends/

TECHNICAL INFORMATION

Architecture

Veriato employs a client-server architecture. The data collector or agent, commonly referred to as a "client recorder" in Veriato technical documentation, is deployed to the target machine (workstation, server or mobile device). Server-based components collect and store information from the target machines, where it can be analysed and reported on from a client-based application (the 'Dashboard'). Multiple instances of the Dashboard can be deployed. The 'Control Centre' application is used to deploy and manage agent recording and to administer the other components in the architecture.



TECHNICAL INFORMATION

Operating System Coverage

Veriato captures activity data taking place on Windows Server 2012 and 2008, Windows 10, 8, 7, and Vista, as well as Mac OSX 10.9 or higher. Support for Android will be released in early Q4 2016.

Authentication, Permissions, & Data Security

Windows (AD) authentication is used combined with RBAC provided by Veriato. Veriato 360 has a 'master' Dashboard user who is able to:

- Create other 'master' user accounts
- Create 'standard' user accounts, including restricting them to which recordings they can view
- Create and schedule reports
- Manage resources such as monitored computers
- Administer server components The 'standard' user can:
- Monitor and analyse recordings to which they have been granted access
- Modify charts and reports
- Change data filter criteria

Dashboard users require access permissions to the database that stores the recorded events as well as the network share where the screen snapshots and email attachments are stored.

The Control Centre application requires administrative and network access to all monitored end points (for Client Recorder control) as well as network access to other components for administration purposes. Note that the Control Centre is a single instance from which all client recorders are administered.

Client recordings are encrypted before being sent to the server data stores. Once stored in the database, access to event data is controlled through database authentication. Screen snapshots and email attachment are encrypted on the network share.

Veriato provides an Export Utility that allows client recordings to be exported from the database and flat file system to our propriety format. Since these files are viewable only with a Veriato Viewer chain of custody is maintained for any legal proceedings where recordings may be used as evidence.

Veriato

3rd Floor, Crossweys House
28-30 High Street
Guildford, Surrey
GU1 3EL United Kingdom

Phone +44 (0) 1483 662888
Fax +44 (0) 1483 243301
Hours: 9 AM to 5:30 PM GMT