VANTAGE
from Visavvi

SECURITY & COMPLIANCE

Vantage cloud-based asset management and monitoring for AV, UC and IT devices

visavvi
Part of the Saville Group

OUR COMMITMENT

During our illustrious history, we have always been associated with progression. Now, with the industry changing beyond recognition, we are leading a new kind of marketplace

Whilst being ahead of the curve in the IoT and Workplace Technology sector is important to Visavvi, we know that being a forward-thinking leader in this industry comes with a huge responsibility.

As we continue to innovate in the bring new products and services to the market, we need to make sure that we take every precaution to protect our assets and those of our partners and clients.

It is critical to Visavvi that the data shared between clients, suppliers and our employees remains safe and secure, this is why we take our in-house security very seriously.

Visavvi has worked through the requirements and implemented the processes necessary to gain our Cyber Essentials Plus certification. This demonstrates that our approach is security first, focusing on best practises in cyber security.

ABSTRACT

Vantage by Visavvi provides cloud-based asset management and monitoring for AV, UC & IT devices. Our aim is to free users from the challenges of managing the health and performance of their technology landscape.

Vantage provides a holistic view of our client's environment irrespective of manufacturer, make or model so that we can ensure;

- Your technology remains a business benefit and not a business disruption
- Your organisation benefits from increased service efficiencies through pro-active monitoring and resolving of issues remotely before meetings and users are impacted.
- As your technology partner, we are collectively making educated decisions around technology spend by using reliable and accurate usage and performance data.

If you are reading this whitepaper, you are probably an IT Manager or Network Administrator alike and the security of the networks you manage is your first concern.

Our core values and commitment to compliance lead processes is why the control measures we have in place promote the highest levels of security, availability and privacy.

In this white paper we will give you an overview on the three matters that, like you, we most about when developing our Vantage solution:

Security: This section is a walk-through of our security framework and provides you an overview of the main actions we take to keep your data safe and to continuously improve security.

Availability: Visavvi is devoted to making sure the service is always up & running, with minimal down time, even in the case of unexpected events or major disasters. In this section we describe the processes and best practice we follow.

Privacy: Visavvi has always been proactive in maintaining the privacy and data of its users, even before major regulations, such as GDPR came into law. In this section we describe how all data processed by Saville Group is treated.

TABLE OF CONTENTS

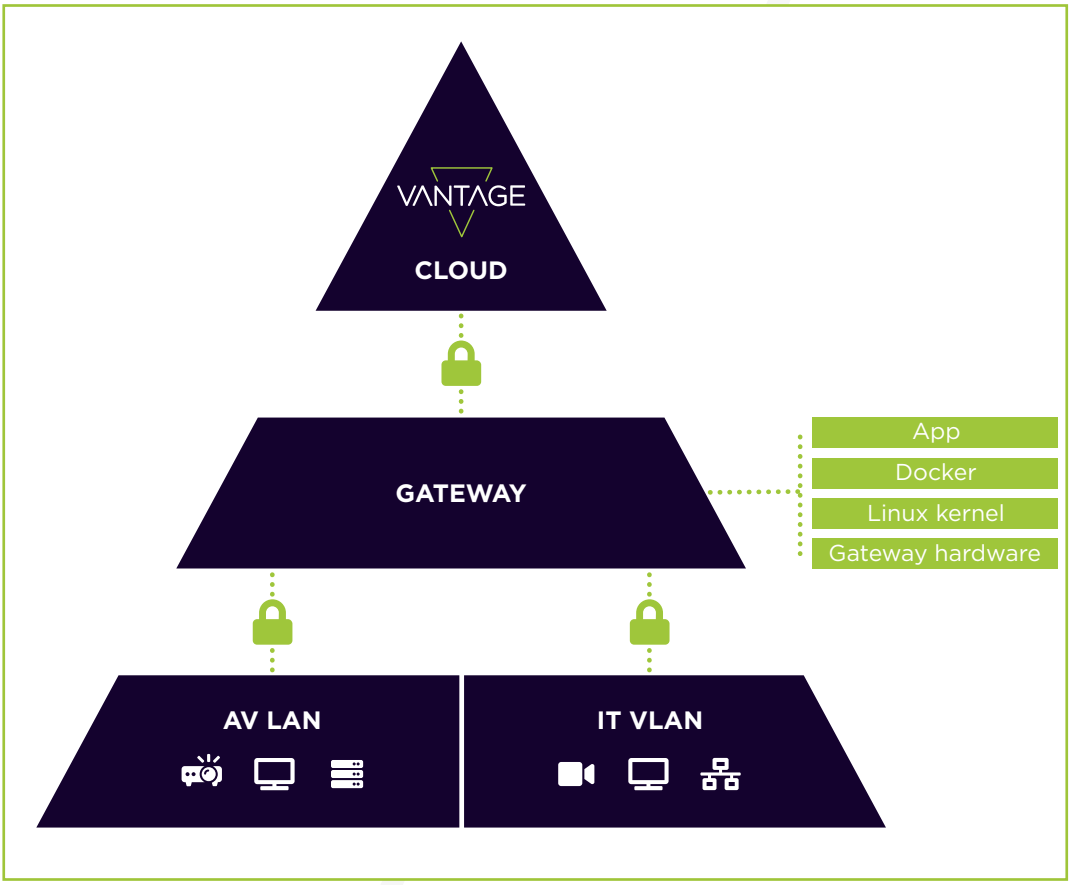
ARCHITECTURE

Vantage Infrastructure Overview

The Vantage cloud platform provides a secure method to access your AV equipment remotely. Devices can be access individually via temporary TCP tunnels or an ad-hoc VPN to the AV network. The remote connectivity allows devices to be continually monitored for issues and outages along with assisting with the triage and diagnostics in the event of an issue. Additionally, proactive maintenance such as updates and patches can be facilitated.

To achieve reliable and secure remote connectivity we deploy a Vantage gateway to the customers site. The Gateway will handle setting up secure tunnels to devices, relaying devices status updates and the discovery of devices on the network.

The main priority for the Vantage is security, that's why we ensure security best practices are followed at every layer of the service. Below we have detailed how we apply these practices at each level of our business.



PHYSICAL SECURITY

AWS

We use Amazon Web Services (AWS) to host our infrastructure. Workloads are hosted in the 'Europe London' region across multiple availability zones.

We follow the security best practice guidelines documented by Amazon to provide a secure and robust environment to host our service.

The AWS service implements a Shared Responsibility Model. This shared model delegates the certain responsibilities to AWS such as managing and controlling the components from the host operating system and virtualisation layer down to the physical security of the facilities in which the service operates. We assume responsibility and management of the guest operating system.

The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001 / ISO 27017 / ISO 2701
- ITAR
- FIPS 140-2
- MTCS Level 3
- HITRUST

More information regarding AWS security practices can be found here: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Offices

All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment and network infrastructure) are located, wherever possible and practical, in secured, climate-controlled rooms and/or in locked cabinets which may be accessed only by designated members of the IT Department.

IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised individual access to such locations for any reason.

DATA SECURITY

Data at rest

We use AWS Relational Database Service (RDS) to store client data. Our database instances are encrypted at rest using the industry standard AES-256 algorithm along with any underlying replicas or backups.

Data in transit

Communication to Vantage Portal

All communication to vantage.visavvi.com is encrypted via HTTPS and will display as a secure connection on your browser. We require TLS 1.2 or above with a modern cipher suite.

Gateway Communication to Vantage Cloud

Our gateway allows secure connectivity between your local devices and our cloud infrastructure without any inbound firewall requirements on the client side.

Gateways are monitored and updated via a secure OpenVPN connection. The VPN connects on port 443 and should work with your existing firewall rules.

All the commands to the Domotz Agent are sent over a secure channel (AMQPS - Advanced Message Queuing Protocol over Secure Socket Layer). Each agent/network has its own private channel, and this channel can only be accessed by that specific agent (the credentials to access to this channel are created at the moment of the Agent configuration, and it is only stored on premise within your Domotz device - e.g. Raspberry Pi, NAS, your own Server or the Domotz Box).

All the commands to the gateway are sent over a secure channel (AMQPS - Advanced Message Queuing Protocol over Secure Socket Layer). Each gateway has its own private channel, and this channel can only be accessed by that specific gateway.

Device Remote Access

Vantage has the ability to create a connection (HTTP or HTTPS, SSH or Telnet, RDP or VNC) to your remote devices. When a connection is created, a secure connection is established (Encrypted Overlay Network) between the remote network and our cloud.

You do not need to open any external port on the router to reach your remote devices. The solution for Remote Connectivity guarantees an additional level of security, given that all the supported protocols are encrypted when the data is

exposed on the public network. Therefore, even the data associated with Telnet and Http Remote Connections (which are inherently unencrypted), are secured on the public network by the encrypted channels.

Moreover, we have also provided a very secure way to connect to remote devices through a non-directly supported protocol (e.g. FTP, VNC and, in general, any proprietary TCP protocol). Even though the Open TCP Tunnel functionality does not guarantee the same level of encryption as the direct Remote Connectivity, we have protected the end–point of the secure channel allowing only connections coming from the specific calling public IP (which is the public IP of the client initialising the Remote Connection).

Similar mechanisms are in place for the VPN on Demand feature. With the additional layer of security offered by the fact that the only the user requesting to start a new VPN on Demand session will receive the OpenVPN configuration file required to start the session. Additionally, that configuration file contains a one-time key to connect to the OpenVPN server started on the fly.

NETWORK SECURITY

We leverage may of the tools provided by AWS to protect our network, these include:

- Distributed denial of service (DDoS) attacks - AWS leverages DDoS mitigation techniques developed from experience in hosting global e-commerce websites.
- IP spoofing - The AWS firewall infrastructure does not allow instances to send traffic with a source IP or MAC address other than the ones initially allocated.
- Port scanning - Unauthorised port scans are a violation of the Amazon EC2 Acceptable Use Policy (AUP). AWS reserves the right to investigate violations of this type and remove, disable access to, or modify any content or resource that violates this Policy.

All inbound ports on Amazon EC2 instances are close which makes make port scanning techniques ineffective.

Vantage uses regular vulnerability scanning via for all our externally exposed resources via Intruder.io. This information, along with proactive CVE monitoring allows us to mitigate potential security exploits.

APPLICATION SECURITY

Our developers view security as a number one priority and occurs at every level of our application design.

All of our applications are designed following the principals of the OWASP Foundation | Open Source Foundation for Application Security. We constantly monitor and protect against the most common application vulnerabilities including the OWASP Top Ten Web Application Security Risks | OWASP

We implement a code review process to ensure that our code quality is maintained, and security best practices are being followed.

Our code deployment pipeline requires multiple stages of sign off and is tested thoroughly in our staging environment before heading to our production servers. In addition to manual sign off, automated testing occurs throughout our pipeline.

All application updates are versioned and release notes are available documenting any important changes made to the platform.

OPERATIONAL SECURITY

The Vantage service is isolated from the Saville Group network and infrastructure. Only a subset of employees have access to Vantage resources and the principal of least privilege access is applied to all users who require access. All passwords are salted and hashed before storing.

All staff accounts implement a strong password policy with frequent password rotation, in addition all staff with access to Vantage have two factor authentication enabled by default.

We use AWS CloudWatch to monitor and log our services this gives us insight on any security, performance or availability issues. AWS CloudTrail is utilised to provide an audit log of all actions performed by Vantage administrators.

Vantage implements Infrastructure as code (IaC) as a process to deploy, manage and update its infrastructure. This allows any changes to be reviewed and authorised in the same way as our application code. This helps maintain infrastructure security whilst allowing us keep a strict change control procedure.

PERSONNEL SECURITY

Visavvi operates a rigorous online process for educating its staff and bringing partners onto its supply chain, namely Sitepass. The system tests the knowledge and understanding of our partners and employees with a focus on key areas including but not limited to:

- Visavvi's Health & Safety Policies
- Visavvi's GDPR Policies
- Visavvi's Anti-Bribery & Corruption Policies
- Visavvi's IT Security Policies

All staff and partners are required to watch a number of videos covering a broad range of topics followed by an online assessment, staff and partner are required pass the assessment and confirm they have read and understood the information before being further onboarded into the business.

DISASTER RECOVERY

Vantage is built on a distributed micro services architecture to minimise any single point of failure. This allows us to deliver a reliable and scalable service. All of our edge service are load balanced and each service has multiple redundancies.

Backups are taken regularly and are treated with the same security and privacy scrutiny as all our client data. Multiple disaster recovery protocols are in place and are tested to validate the procedure and improve the process to minimise any potential downtime.

We aim to provide a highly available service with 99.999% uptime.

Any issues can be reported via the standard Visavvi Service contact methods.

PRIVACY

We take the processing, storage and use of personal data seriously. As a business we value the information that our clients trust us with, and we are committed to going further than the letter of the law when it comes to adopting practice standards when handling your information.

Please see a copy of our full GDPR policy: https://www.saville.group/legal-compliance

PARTNER SECURITY

We utilise technologies from trusted partners to deliver our Vantage service. All partners are held to the strict security consideration we enforce on ourselves.

If you require more information regarding our partnerships, please contact your Visavvi representative.

VANTAGE GATEWAY SECURITY

Access Restrictions

The Gateway exposes SSH for monitoring and upgrading the underlying OS. The SSH connection is not designed to be used directly and is secured using an SSH key. All password-based authentication is disabled. It is not possible to login to the terminal locally on the device.

Network Requirements

The Vantage Gateway requires certain outbound network connectivity to function correctly. Internet access must be direct and not require a proxy or captive portal.

Port	Protocol	Destination	Direction
443	TCP	balena-cloud.com	Outbound
443	TCP	api-eu-west-cell-1.domotz.com	Outbound
443	TCP	portal.domotz.com	Outbound
5671	TCP	messaging-eu-west-cell-1.domotz.com	Outbound
32700-32849	TCP/UDP	sshg.domotz.co, us-east-1-sshg.domotz.co, us-west-2-sshg.domotz.com	Outbound
123	UDP	docker.com	Outbound
123	UDP	0.resino.pool.ntp.org	Outbound
123	UDP	1.resino.pool.ntp.org	Outbound
123	UDP	2.resino.pool.ntp.org	Outbound
123	UDP	3.resino.pool.ntp.org	Outbound
53	UDP	docker.io	Outbound

OS Platform

The Vantage Gateway OS is composed of multiple Yocto layers. The OS is an operating system optimized for running Docker containers on embedded devices, with an emphasis on reliability over long periods of operation in remote locations.

The OS userspace packages only provide the essentials for running containers, while still offering flexibility. The philosophy is that software and services always default to being in a container unless they are generically useful to all containers, or they absolutely can't live in a container.

For more information: www.yoctoproject.org

Update Processes

The Vantage Gateway updates both OS and applications automatically. Updates are loaded onto a secondary partition and tested before being applied to ensure a successful update. We update the Vantage Gateway OS frequently to protect against security vulnerabilities and instability.

COMPLIANCE

International Organisation for Standardization

ISO is an independent, non-governmental organisation that develops and publishes international standards, and through its members it brings together experts to share knowledge and develop voluntary relevant standards that support innovation and provide solutions to global challenges.

In simple terms, it is a series of frameworks that help run businesses effectively and for the good of all stakeholders. Our ISO certification is proof that we have been approved by an external body to comply to all the requirements of the standard.

At Visavvi, we have recently become re-certified for all of the following ISO UKAS Accredited Management Standards:

- IS0 9001:2015 Quality Management
- ISO 14001:2015 Environmental Management
- OHSAS 18001 Occupational Health & Safety Management

If you would like to read our certified Quality, Environmental and Health & Safety policies please see: https://www.saville.group/legal-compliance

Cyber Essentials

Visavvi has worked through the requirements and implemented the processes necessary to gain our Cyber Essentials Plus certification. This demonstrates that our approach is security first, focusing on best practises in cyber security.

Cyber Essentials is a UK government scheme supported by the NCSC (National Cyber Security Centre) that sets out five basic security controls to protect organisations from around 80% of common cyber-attacks.

The scheme's certification process is managed by the IASME Consortium, which licenses certification bodies to carry out Cyber Essentials and Cyber Essentials Plus certifications.

Cyber Essentials is designed to help organisations of any size demonstrate their commitment to cyber security – while keeping the approach simple.

This is achieved through the strengthening of five key areas:

- Securing of your Internet connection
- Securing of your devices and software
- Controlling access to your data and services
- Protection against viruses and other malware
- Keeping your devices and software up to date

APPENDIX

Vantage Gateway Hardware

1. Thermal Testing

1.1. As part of our commitment to only using high quality and reliable products Visavvi can confirm that the UP Squared Gateway used in the Vantage solution has undergone stringent thermal imaging analysis during production with AAEON Technology Inc.

For a copy of the results see: https://downloads.up-community.org/download/up2-test-and-certification/

2. Humidity Testing

2.1. As part of our commitment to only using high quality and reliable products Visavvi can confirm that the UP Squared Gateway used in the Vantage solution has undergone stringent thermal/humidity testing during production with AAEON Technology Inc.

For a copy of the results see: https://downloads.up-community.org/download/up2-test-and-certification/

3. Compatibility Testing

3.1. As part of our commitment to ensuring that the products we use as part of our Vantage solution are tested in a variety of applications Visavvi can confirm that the UP Squared Gateway has undergone extensive compatibility testing with a number of variables during production with AAEON Technology Inc.

For a copy of the results see: https://downloads.up-community.org/download/up2-test-and-certification/

4. Reliability Report

4.1. As part of our commitment to only using high quality and reliable products Visavvi can confirm that the UP Squared Gateway used in the Vantage solution has undergone stringent process of Reliability Prediction in an effort to determine its predicted failure rate.

For a copy of the results see: https://downloads.up-community.org/download/up2-test-and-certification/

5. Compliance

5.1. Declaration & Certificate of Conformity

5.1.1. The UP Squared Gateway used in the Vantage solution is confirmed to comply with the with the requirements set out in the Council

Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (2014/30/EU) and RoHS Directive (2011/65/EU). For the evaluation regarding the Directives, the following standards were applied:

EN 55032: 2015 / AC: 2016

CISPR 32: 2015 (Ed 2.0) / C1: 2016

EN 61000-3-2: 2014

EN 61000-3-3: 2013

EN 55024: 2010 + A1: 2015

IEC 61000-4-2: 2008; IEC 61000-4-3: 2006 + A1: 2007 + A2: 2010; IEC 61000-4-4: 2012; IEC 61000-4-5: 2014; IEC 61000-4-6: 2013; IEC 61000-4-8: 2009; IEC 61000-4-11: 2004

To see a copy of the official EU declaration and certificate, please see: https://downloads.up-community.org/download/up2-test-and-certification/

5.2. Certificate of RoHS Compliance

5.2.1. The UP Squared Gateway used in the Vantage solution is confirmed to comply with the requirements of the European Unions' Restrictions on the use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS) directive, 2011/65/EU.

To see a copy of the official EU certificate and test results please see: https://downloads.up-community.org/download/up2-test-and-certification/

5.3. REACH SVHC Declaration

5.3.1. To minimize the environmental impact and take more responsibility to the earth weive, Visavvi have confirmed with AAEON Technology Inc. that in reference to the model UPS-ALPC2-A10-0432 to date, based on suppliers data, that our product shipping to the EU territory comply with the restriction of SVHC (Substances of Very High Concern).

We can confirm that the product does not contain above the 0.1% weight (w/w) threshold of any Substance of Very High Concern (SVHC).

For more information about the SVHC candidate list, please refer to the ECHA official web page: http://echa.europa.eu/candidate-list-table

INGENIOUS BUSINESS COLLABORATION

0370 606 1100 // visavvi.com