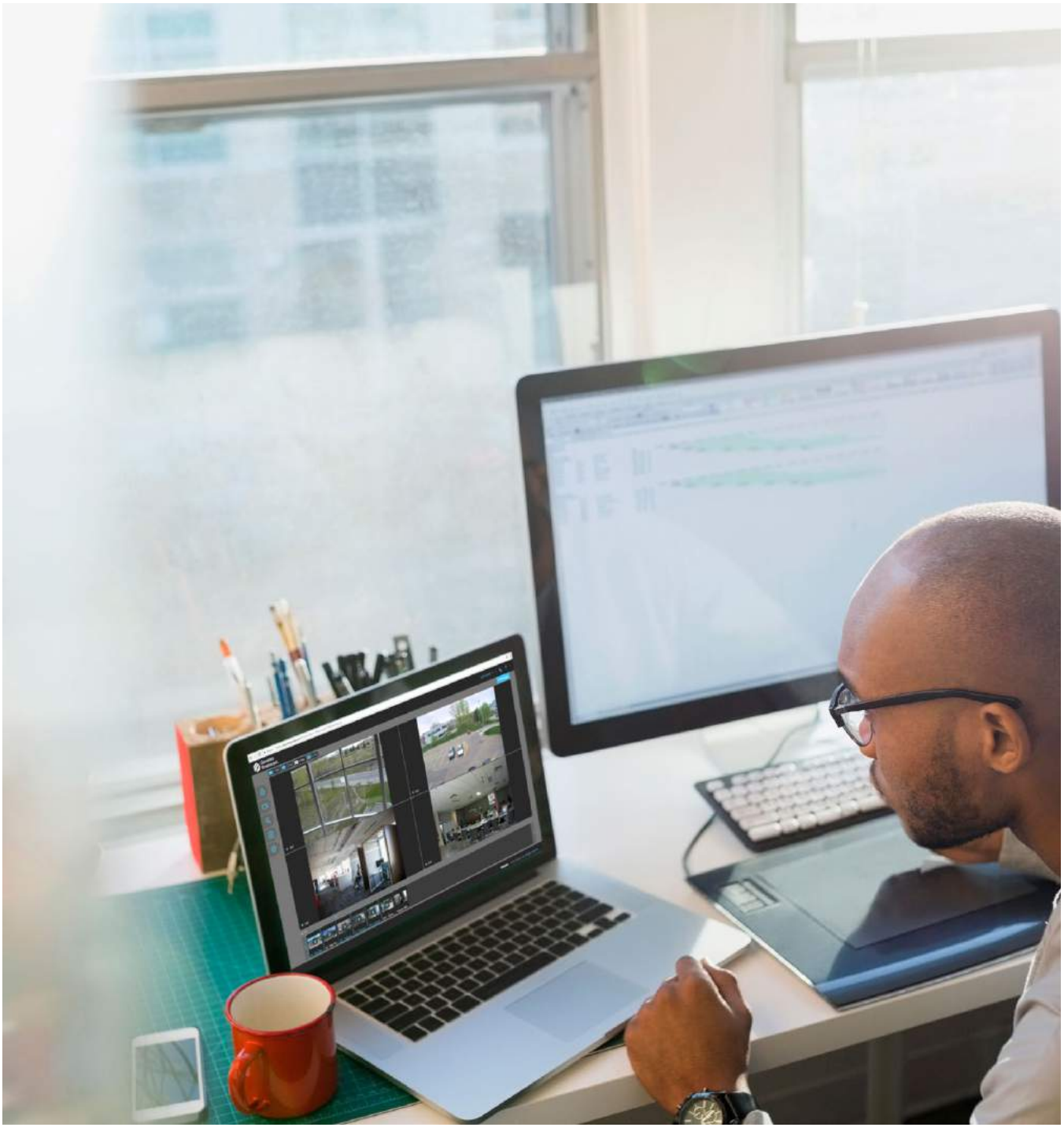
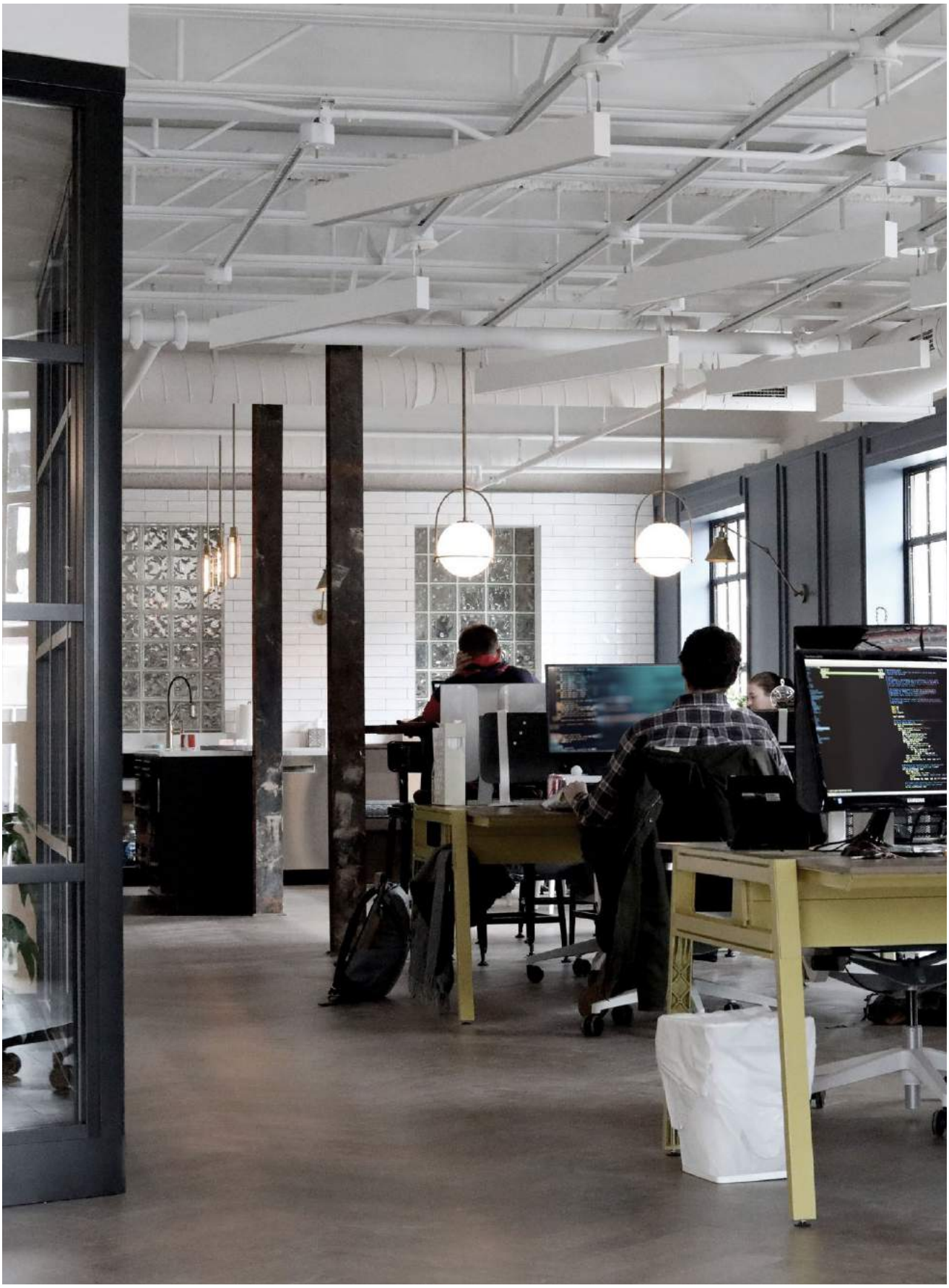
Whitepaper

Security in the cloud

How Stratocast keeps your video safe



Genetec™



Contents

1

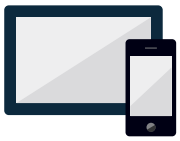
Introduction

Genetec Stratocast™ is a cloud-based video monitoring system that makes the adoption of network video security solutions easy and allows you to connect to your business wherever you go. Using the Microsoft Windows Azure cloud-computing platform, Stratocast eliminates the need for on-site servers. As a result, installation time is reduced and you can begin monitoring your premises quickly.

Using video surveillance equipment such as IP (Internet Protocol) cameras or analog cameras, you can record video on your edge recording video unit or in the Stratocast cloud. If recording on your video unit, the video is recorded continuously, whereas if recording in the Stratocast cloud, you can choose to record either continuously or only when motion is detected. From your laptop, tablet, or smartphone, you can then watch live and recorded video that is safely stored in the cloud. In addition, through Genetec Federation™, Security Center users can view and control all Stratocast cameras from their local installation of Security Desk. The following diagram illustrates how Stratocast works to keep you connected to your business, wherever you go.

Smartphones and tablets

Android
and iOS



Outbound	Port usage
TCP 18100 TCP 18101-19101	Control command Video streaming port

Security Center Federation

Hybrid cloud and
on-premise systems

Outbound	Port usage
TCP 5500 TCP 556	Control command Video streaming port

Video surveillance

IP video units
and appliances

Outbound (Axis)	Port usage
TCP 80, 443, 8080, 8081 TCP 21011 - 21050	Communication Camera video streaming

Outbound (Vivotek)	Port usage
TCP 80, 443, 22000 TCP 22001 - 22050	Communication Camera video streaming

Web application

IE, Firefox and Safari
Windows and Mac

Outbound	Port usage
TCP 80, 443 TCP 943 TCP 443, 4530	Portal page Security validation port Video streaming port

Flow of information

- Encrypted communication (TLS, HTTPS or SSH) and password authentication
- Encrypted video stream (TCP)
- H.264 video stream

Security is crucial for us at every level of development and operations. Based on industry best practices, our engineers embed security standards into the development lifecycle and operations. This whitepaper focuses on the cloud architecture and the operational security of the platform as well as the security capabilities of the customer portal. The video and camera security of Stratocast are also discussed.

2

Cloud architecture

Stratocast is deployed on the Microsoft Azure cloud platform. This platform, with its industry-recognized security, securely stores data that our customers entrust us with. Microsoft Azure has been audited against SOC 1, SOC 2, and SOC 3 standards. Audits are conducted in accordance with SSAE 16 and ISAE 3402 standards. Certifications are regularly updated and can be provided. Stratocast and Azure are also compliant with ISO 27001:2013.

The service architecture is built for high availability and scalability, allowing customers to enroll and record as many cameras as needed without impacting the service. There are no constraints limiting the maximum amount of data that can be stored in Azure, as datacenters are provisioned with enough capacity to ensure that they meet growing demand. This architecture, coupled with the robustness of the underlying Microsoft Azure Cloud, allows Genetec to provide a 99.5% SLA.

Stratocast availability and access to video is backed by a 99.5% uptime guarantee.

2.1 Security controls

Stratocast and Azure adhere to a rigorous set of security controls that govern operations and support. Genetec and Microsoft deploy a combination of preventive, defensive, and reactive controls including the following mechanisms to help protect against an unauthorized developer and/or administrative activity:

- Tight access controls, including a mandatory two-factor authentication
- Combinations of controls that enhance independent detection of malicious activity
- Multiple levels of monitoring, logging, and reporting
- Security reports are used to monitor access patterns and to proactively identify and mitigate potential threats
- Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made
- Automatic patching of the operating systems and applications running in the cloud

Additionally, the Genetec and Microsoft teams conduct background verification checks of certain operations personnel and limit access to applications, systems, and network infrastructure based on the level of background verification.

2.2 High availability

Azure facilities are designed to run 24×7×365 and employ various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

2.3 Redundancy

Stratocast video is stored in triplicate, within the same datacenter, ensuring the redundancy of critical data and mitigating the impact of hardware failure.

2.4 Control of data location

Knowing and controlling the location of an organization's data can be an important element of data privacy, compliance and governance. Customers can specify the geographic area where their recordings are stored. Through this approach, recordings are replicated within a defined region for redundancy but are not transmitted outside the customer's desired geographic boundaries.

3

Operational security

As a trusted provider of security solutions for a considerable number of government agencies and high-profile public and private organizations worldwide, we take compliance with local regulations very seriously. This, of course, includes the laws pertaining to data security and protection of privacy in the regions where we sell our products and services. Additionally, to ensure that all customer data is stored and used in an appropriate and secure manner, Stratocast is certified with the ISO 27001:2013 information security standard. The ISO 27001 standard is a framework of policies and procedures including legal, physical, and technical controls that address cyber security risks. These policies and procedures are part of the Information Security Management System (ISMS) at Genetec, that has been audited and certified by the ISO organization. Below is an excerpt of some of the relevant portions of it.

This system allows us to assess threats in real-time and react to them in a timely manner.

3.1 Secure development policy

Genetec is conscious that security is something that has to be embedded in the development practices and not something that can be added after the fact. Consequently, the Stratocast Software Development Lifecycle (SDL) includes specific activities, pertaining to cyber security, that have to be completed in order to release each new version of Stratocast. These activities are defined in the secure development policy and include:. secure design review performed on a periodic basis, manual or automated security testing, and penetration testing performed by a 3rd party auditor.

3.2 Incident management and disaster recovery

It can be challenging to react appropriately to a cyber security incident when it happens, if nothing has been prepared for it beforehand. To avoid this, we have instilled a well-established incident management plan describing appropriate responses. This includes among others: the criteria defining the severity of an incident, the roles and responsibilities of each stakeholder involved in the management of that incident, the incident lifecycle, and the service level objectives.

In a similar fashion, it's best practice to establish a disaster recovery plan in the event of external service outages. Stratocast has a well thought out plan that reduces any negative impacts on its customers.

3.3 Intrusion detection and prevention

In order to get real-time status updates, an intrusion detection and prevention system is used. Powered by the Microsoft Azure platform, this system allows us to assess threats in real-time and react to them in a timely manner.

3.4 Service monitoring

Genetec subscribes to a variety of feeds and services including Checkpoint, Microsoft, Mandiant, and Hyphen. Based on the nature of evolving threats, Genetec adapts its controls as often as necessary. Stratocast is monitored constantly on all core functionalities and a team of first responders take action as soon as they are notified.

4

Portal security

4.1 Authentication

Authentication is the process of establishing the identity of a user trying to connect into Stratocast. Stratocast doesn't use an internal mechanism in order to authenticate a user but rather leverages several external identity providers including Microsoft, Google, and Yahoo. The authentication process on the Stratocast Portal uses a combination of Web Services Federation (WS-Federation) and OpenID Connect. The specifics on how to authenticate a user are delegated to the external identity provider and usually include username and password, and typically support multi-factor authentication. Application and user sessions have built-in time-outs and lockouts after a certain period of inactivity in order to avoid unauthorized access.

4.2 Authorization

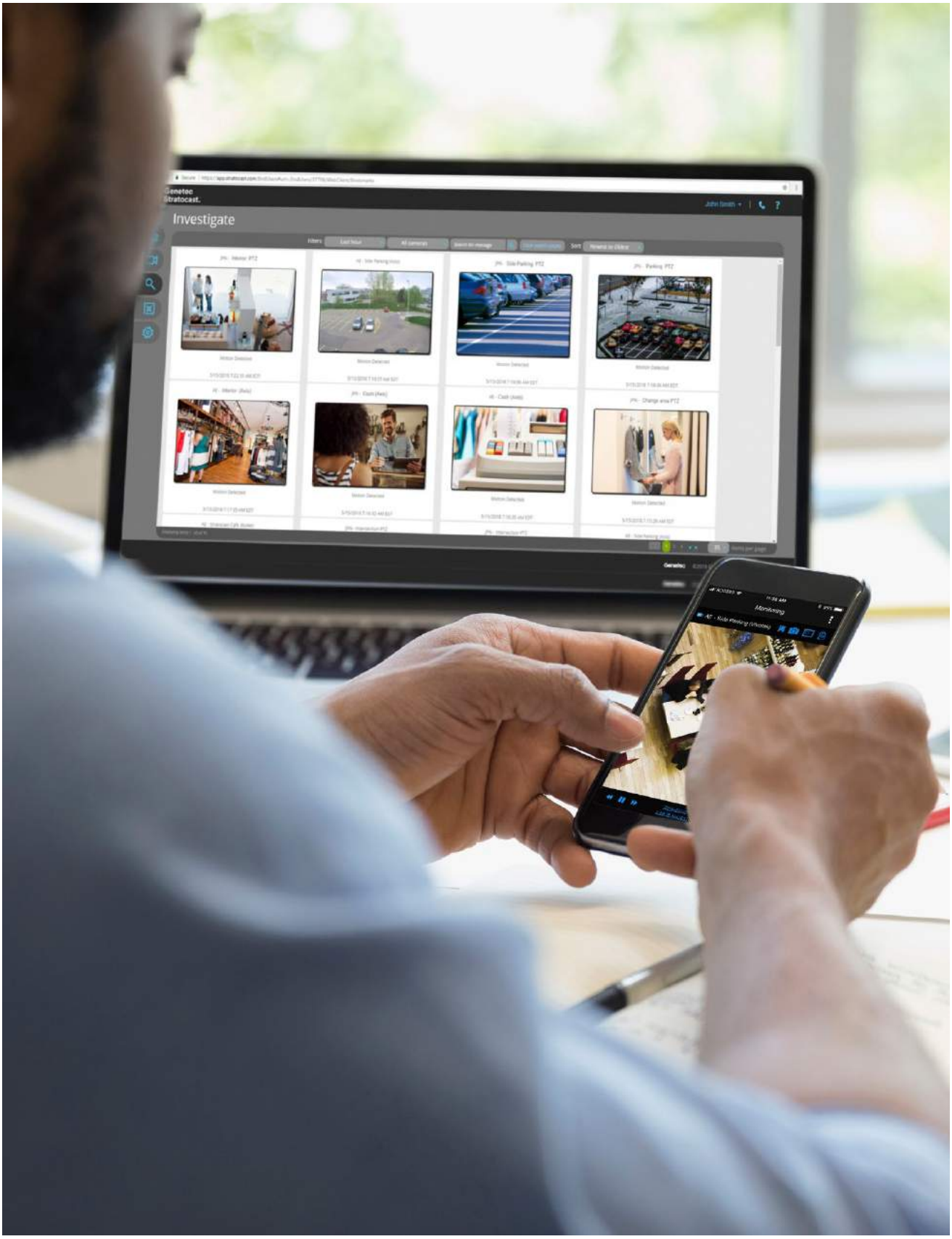
Authorization is the process of establishing what rights a user has. A user level defines a set of access rights in the system. There are currently 4 user levels: Integrator administrator, Integrator user, Client administrator, and Client user. User levels are assigned every time a user is created. Please refer the Stratocast Integrator Guide to get the complete list of tasks that each user level is allowed to perform. User authorization is enforced using security tokens.

4.3 File and data encryption

Data at rest is stored redundantly on Microsoft Azure's infrastructure and encrypted using AES-256 encryption standards. The encryption keys are managed securely through the Azure Key Vault.

4.4 Communication encryption

Data in transit and communication with the platform is secured using HTTPS. X.509 certificates are used for authentication to ensure that only trusted parties have access to data in Stratocast. This ensures the confidentiality and the integrity of the information and mitigates malicious attempts to intercept or alter communication in transit.


Genetec
Stratocast.
Investigate
Monitoring

5

Communication security

5.1 Camera

All communications (video, command and control) between the cameras and our servers is secured through an encrypted channel. The communication channel between the cameras and the platform can differ depending on the type of camera manufacturer. Although the protocols in use differs, the security of the channel is always a priority. At the moment, Stratocast provides 2 separate methods for connecting cameras to the platform.

The Axis cameras use the TLS 1.2 protocol with Client Authentication. Each camera has its own Client Certificate with a 2048 bit RSA key. Our servers use a Server Certificate with a 4096 bit RSA key.

All other types of cameras compliant with Stratocast use the Stratocast Control Protocol in conjunction with the SSH2 protocol. Each camera has a 2048 bit public and private key pair. To establish the secure channel, the key exchange is done with either one of the following: Diffie-Hellman Group14-SHA1 or Diffie-Hellman Group1-SHA1. The encryption is done with either AES 256-ctr, AES192-ctr or AES 128-ctr.

5.2 Web client

The Stratocast platform provides its users with the ability to view their video in real-time or in playback, directly from their browser. To achieve security in transporting the video data from the platform to the users' browser, Secure Web Sockets (WSS) are used. With this technology, man-in-the-middle attacks are greatly reduced.

It is possible to use an older version of the webclient that uses a Silverlight component to stream the video. The communication channel between the client application and the server is done through an encrypted channel. The channel uses RSA 1048 bit public-private key pair encryption to negotiate an AES 256 bit encryption key. The video is then encrypted with the latter.

5.3 Mobile devices

It is possible to access the Stratocast platform from a native application for mobiles devices. These devices communicate with the Stratocast platform securely through the use of HTTPS with TLS 1.2.

Established in 1997, Genetec is the global leader in unified security platforms, with a broad offering across a range of security specialties.

Video surveillance: Achieve greater situational awareness and enhance security within your city with the ability to share cameras across agencies and organizations, providing a common operational picture and improving incident response time.

Access control: Heighten your organization's security, effectively respond to threats, and make clearer and timelier decisions with a unified, IP-ready platform, whether deploying a new access control system or updating an existing installation.

Automatic license plate recognition: Automate the detection of vehicles of interest, increase parking enforcement efficiency and accelerate public safety investigations through the ability to share license plate data with selected agencies and partner organizations, without forfeiting ownership and privacy.

Operational decision support: Create efficiency for incident handling and decision making with advanced workflows that guide operators from situation alerts through policy-based procedures to detailed case compilation export.

Collaborative investigation management: Simplify case management and speed up investigations with a platform that allows you to centralize digital evidence and securely collaborate with investigators, outside agencies and the public.

Cloud services: Extend the capabilities of your on-premises security system and reduce IT costs with highly scalable, on-demand cloud services that allow your city to easily cope with rapidly changing security requirements and operate with greater efficiency.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

STRATWP_WPIEN