IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SAMSCLOUD, LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	C.A. No. _____
	)	
GENETEC INC.,	)	**JURY TRIAL DEMANDED**
	)	
Defendant.	)	

PLAINTIFF'S COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Samscloud, LLC ("Samscloud" or "Plaintiff") files this Complaint against Defendant Genetec Inc. ("Genetec" or "Defendant") for infringement of U.S. Patent Nos. 11,468,757 (the "'757 patent") and 12,154,421 (the "'421 patent").

THE PARTIES

1. Plaintiff Samscloud is a Texas LLC founded in 2017 with an address at 11131 Carriage Lake, Houston, TX, 77065.

2. On information and belief, Defendant Genetec Inc. is a corporation organized under the laws of Canada, with its principal place of business located at 2280 Alfred-Nobel Blvd., Montreal, Quebec, Canada, H4S 2A4. Genetec may be served with process via its registered agents and via its corporate officers.

JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others.

4. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. On information and belief, Genetec is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Delaware Long Arm Statute, due at least to its substantial business in this State and judicial district, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this State and this judicial district and, thus, submits itself to the jurisdiction of this Court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of the State of Delaware and this judicial district, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Delaware residents and residents of this judicial district vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. Authorized Genetec dealers provide Genetec video surveillance installation and services in Delaware: for example, Delaware dealer Advantech has contracted with the State of Delaware to provide Genetec video surveillance products. *See Vendor Details – A3 Communications Inc. DBA Advantech*, STATE OF DELAWARE, *https://mmp.delaware.gov/Vendor/Details/11486#* (last visited July 20, 2026); *Pricing Information*, STATE OF DELAWARE, https://bidcondocs.delaware.gov/DTI/Copy%20of%20DTI240048-BLDG_SECURE_PS2.xlsx (last visited July 20, 2026) (naming Genetec as a source of equipment used in the project). Genetec also has broader activity in the State of Delaware related to its other products and features, which include features designed to recognize Delaware license plates, indicating their intended use in the state. *See AutoVu SharpOS Release Notes 11.0*, GENETEC, https://downloadcenter1.genetec.com/products/AutoVu/Sharp/11.0/EN.AutoVu%20SharpOS%20Release%20Notes%2011.0.pdf, at 9 (Apr. 29, 2015). Additionally, on information and belief,

contract bid documents submitted by Genetec reflect that Genetec's "East Region" of its sales force covers Delaware. *See Genetec, Inc. Information*, OMNIA PARTNERS, https://www.omniapartners.com/suppliers-files/E-J/Genetec/Contract_Documents/R250204/25-02_Genetec_Response_2024_11_14_Combined_Redacted.pdf (Nov. 20, 2024).

6. Defendant also maintains commercial websites accessible to residents of the State of Delaware and this judicial District, through which Defendant promotes and facilitates sales of the Infringing Products. For example, on information and belief, Genetec partners with local Delaware entities to sell and utilize the Infringing Products with associated add-ons. *See WallControl 10 for Genetec Security Center*, DELAWARE AUDIO VISUAL, https://catalog.delawareav.com/avcat/ctl8327/index.cfm?manufacturer=datapath&videos=15704 (last visited July 15, 2026).

7. Thus, Defendant has established minimum contacts with the State of Delaware and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

8. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b), (c) and 1400(b) because (i) Defendant has done and continues to do business in this district; (ii) Defendant has committed and continues to commit acts of patent infringement in this district, including making, using, offering to sell, and/or selling accused products in this district, and/or importing accused products into this district, including by internet sales and sales via retail and wholesale stores, and/or inducing others to commit acts of patent infringement in this district; and (iii) Defendant is a foreign entity. 28 U.S.C. § 1391(c)(3) provides that "a defendant not resident in the United States may be sued in any judicial district." *See also Brunette Machine Works v. Kockum Industries, Inc.*, 406 U.S. 706 (1972) (holding that venue is proper pursuant to 28 U.S.C. §§ 1391 and 1400(b) when Defendant is a foreign entity).

THE ASSERTED PATENTS AND TECHNOLOGY

9. Gary Baker is the sole inventor of the Asserted Patents: the '757 Patent and the '421 Patent, both titled "Systems and methods for facilitating supervision of individuals based on geofencing." The Asserted Patents both share a priority date at least as early as March 5, 2019. The '421 Patent is a continuation-in-part of the '757 Patent.

10. Mr. Baker is the CEO, founder, chairman, and managing member of Samscloud. Samscloud sells products and services covered by the Asserted Patents, which Samscloud advertises via its website, samscloud.io.

11. The Asserted Patents are directed toward systems and methods for creating a grid-based geofence and supervising individuals within the geofenced area. The systems and methods utilize a combination of various types of devices to generate the geofence as seen, for example, in the Abstract for the '757 Patent:

> Accordingly, the method may include receiving, using a communication device, a parameter from a supervisor device associated with a supervisor and a geographical location from the supervisor device. Further, the method may include analyzing, using a processing device, the geographical location based on a security parameter and generating a geofence corresponding to a geographical area based on the analyzing. Further, the method may include receiving, using the communication device, supervisee data associated with a supervisee from a supervisee device. Further, the method may include analyzing, using the processing device, the supervisee data based on the geofence and generating a supervision notification based on the analyzing of the supervisee data. Further, the method may include transmitting, using the communication device, the supervision notification to the supervisor device.

12. The Asserted Patents describe supervision systems and methods that involve creating a geofence comprising a grid in which each grid box is also geofenced, tracking the location of individuals within the geofence and the grid boxes, and implementing various supervision and alert features to protect supervisees within the geofenced area. The Asserted

Patents describe a claimed combination of dedicated elements and processes that were not, at the time of invention, well-understood, routine, or conventional.

13. An exemplary embodiment is shown in Figure 42 of each of the Asserted Patents:

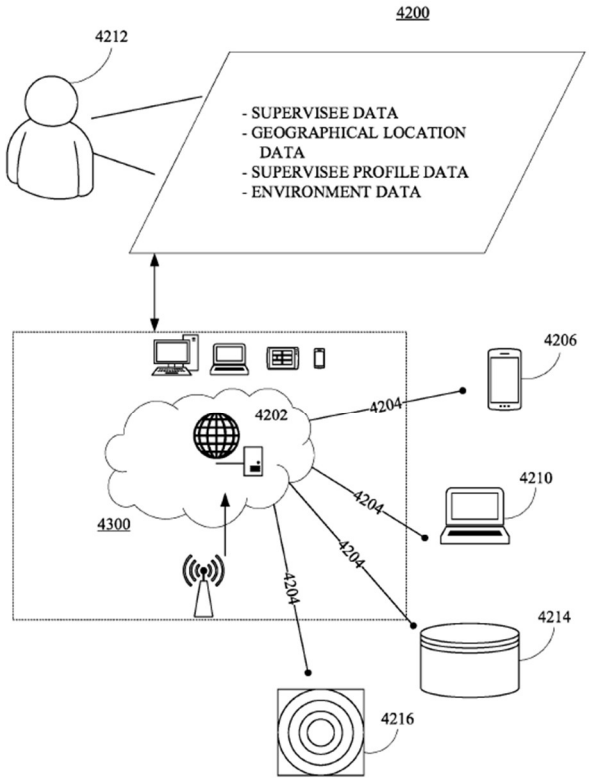


FIG. 42

14. Defendant makes, uses, sells, has sold, and/or offers for sale in the United States products ("Infringing Products") that are not made or licensed by Samscloud and that infringe the Asserted Patents.

15. Defendant markets its Infringing Products specifically extolling the functionality of the Asserted Patents. As one example, Genetec advertises that its Security Center suite of products utilize detailed mapping, location tracking, and geofencing. *See Security Center SaaS*, GENETEC, https://www.genetec.com/products/unified-security/security-center-saas (last visited July 15, 2026).

16. Further, Genetec integrates "Collaborative Response Graphics" provided by Critical Response Group ("CRG") into the Security Center suite of products; CRG's graphics incorporate building blueprints and utilize grid-based geofencing to supervise individuals. *See Genetec*, CRG, https://www.crgplans.com/integrations/genetec/ (last visited July 15, 2026); *Collaborative Response Graphics* ®, CRG, https://www.crgplans.com/collaborative-response-graphics/ (last visited July 15, 2026).

17. On information and belief, all of Genetec's Security Center suite of products that are made, sold, offered for sale, or used in the United States within the statutory period are Infringing Products, including but not limited to Security Center SaaS, Omnicast, and Plan Manager. The product names listed in this complaint are exemplary and not exhaustive.

COUNT I

(Infringement of the '757 Patent)

18. Plaintiff incorporates and re-alleges the allegations contained in paragraphs 1 through 17 herein by reference.

19. The '757 Patent entitled "Systems and methods for facilitating supervision of individuals based on geofencing" was duly and legally issued by the U.S. Patent and Trademark Office on October 11, 2022, from Application No. 16/810,703, published at US2020/0286355 on September 10, 2020, claiming priority to provisional application 62/814,097 filed on March 5, 2019. A true and accurate copy of the '757 Patent is attached hereto as Exhibit A.

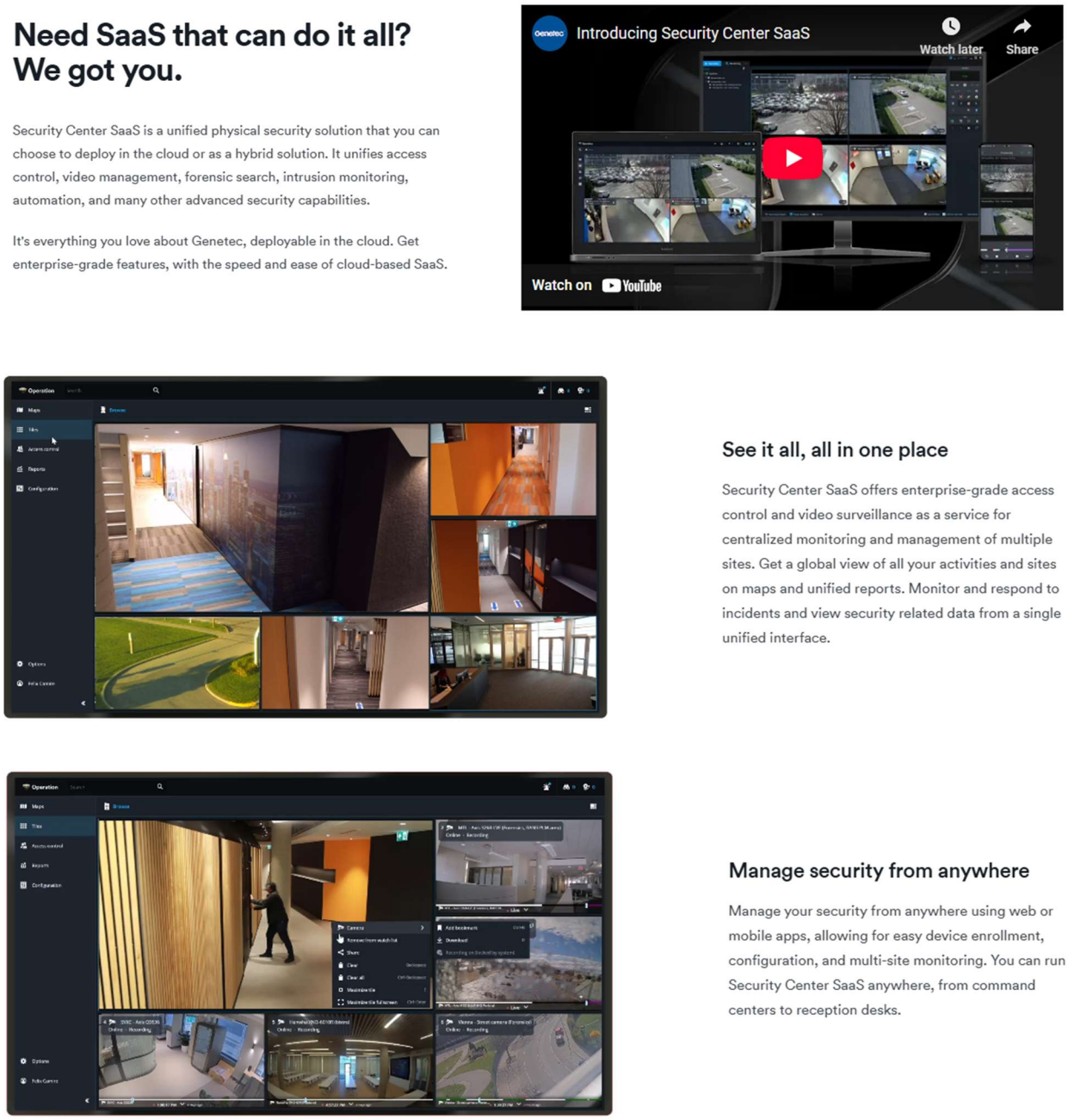
20. Each and every claim of the '757 Patent is valid and enforceable, and each enjoys a statutory presumption of validity under 35 U.S.C. § 282.

21. Samscloud exclusively owns all rights, title, and interest in and to the '757 Patent and possesses the exclusive right of recovery, including the exclusive right to recover for past, present, and future infringement.

22. Claim 1 of the ’757 Patent recites:

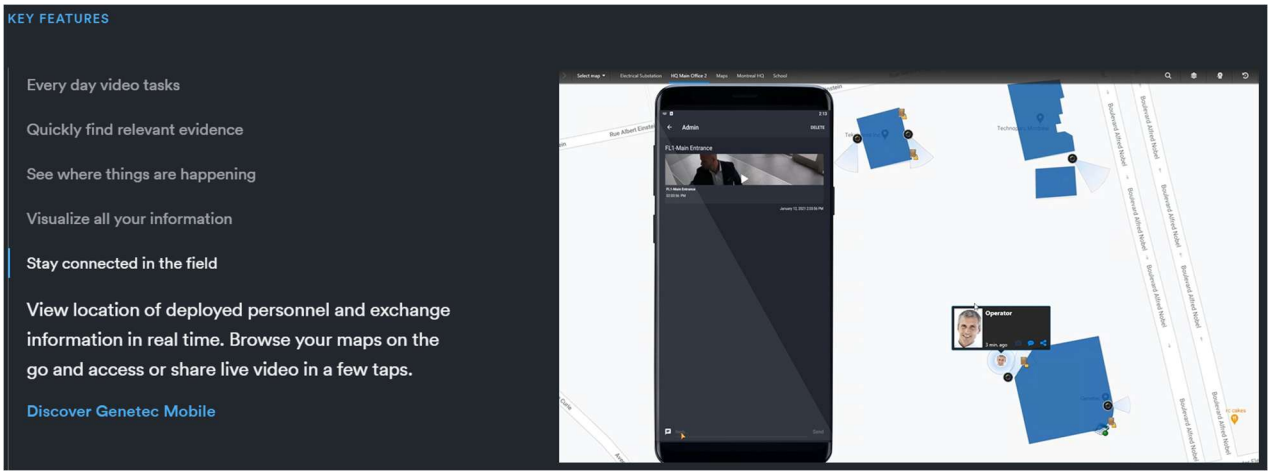
A method for facilitating supervision of individuals based on geofencing, the method comprising:
receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor;
receiving, using the communication device, a geographical location from the at least one supervisor device;
analyzing, using a processing device, the geographical location based on the at least one security parameter;
generating, using the processing device, a geofence corresponding to a geographical area based on the analyzing;
receiving, using the communication device, at least one supervisee data associated with a supervisee from at least one supervisee device;
analyzing, using the processing device, the at least one supervisee data based on the geofence;
generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data;
transmitting, using the communication device, the supervision notification to the at least one supervisor device; and
storing, using a storage device, the at least one supervisee data and the supervision notification, wherein:
the geofence is characterized by a geofence area corresponding to the geographical area, wherein the geofence comprises a plurality of geofence grid boxes associated with the geofence area, wherein each geofence grid box is characterized by a grid box geofence area of the geofence area, wherein the method comprises:
receiving, using the communication device, at least one grid parameter from the at least one supervisor device, wherein the processing device is further configured for:
analyzing, using the processing device, the at least one grid parameter;
determining, using the processing device, the grid box geofence area based on the analyzing of the at least one grid parameter; and
generating, using the processing device, a number of geofence grid boxes based on the determining.

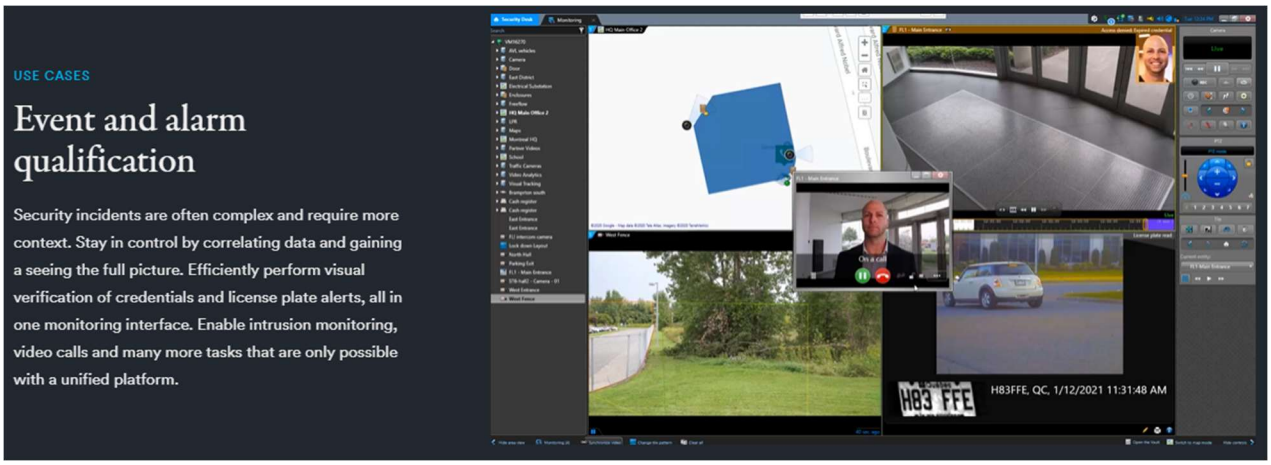
23. Each Infringing Product is configured to perform a method for facilitating supervision of individuals based on geofencing. For example, Genetec’s Security Center SaaS platform supervises individuals:



Source: *Security Center SaaS*, GENETEC, https://www.genetec.com/products/unified-security/security-center-saas (last visited July 15, 2026).

24. Further, on information and belief, the methods performed by the Infringing Products are based on geofencing. For example, Genetec's website shows that the Security Center Products track employee locations and video sources based on virtual boundaries showing the geographical locations of buildings and other important areas (*i.e.*, geofences):



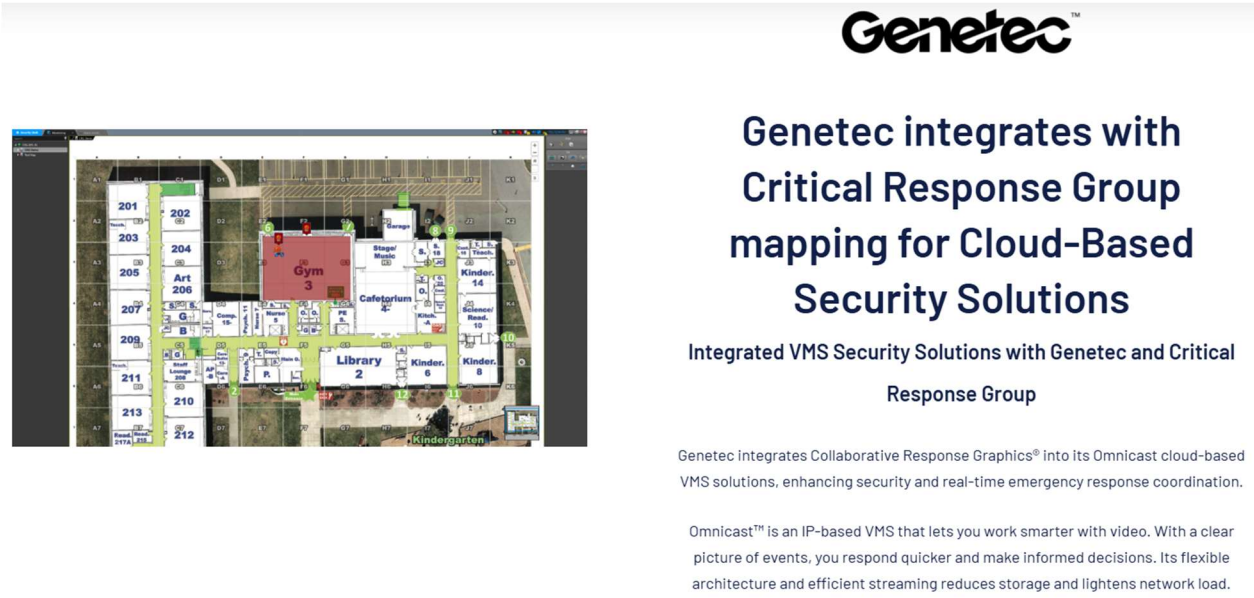


Source: *Genetec – Modern User Experience*, GENETEC, https://www.genetec.com/products/unified-security/omnicast/user-experience (last visited July 15, 2026).

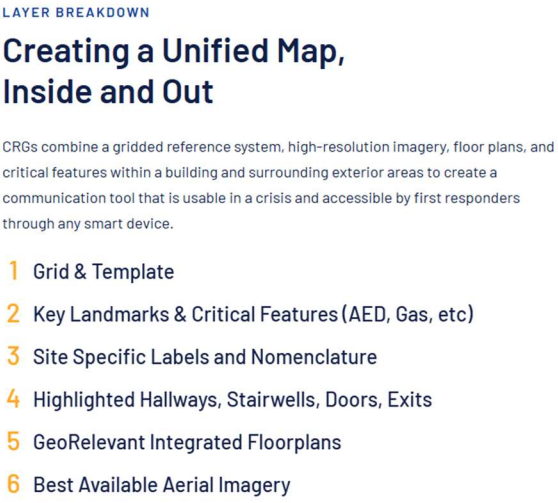
25. On information and belief, each Infringing Product is configured to receive security parameters from supervisor devices. For example, as discussed above regarding events and alarms and as seen further below, the Infringing Products receive and utilize a number of security parameters and geographical information, including parameters relating to alarms, credential verification, and security personnel locations:

Source: *Genetec – Modern User Experience*, GENETEC.

26. On information and belief, each Infringing Product is also configured to receive geographical locations from supervisor devices. For example, Genetec has partnered with Critical Response Group ("CRG") to integrate CRG's "Collaborative Response Graphics" and utilize "GeoRelevant integrated floor plans" and geospatial data (*i.e.*, geographical locations) to provide detailed maps and location information to users:

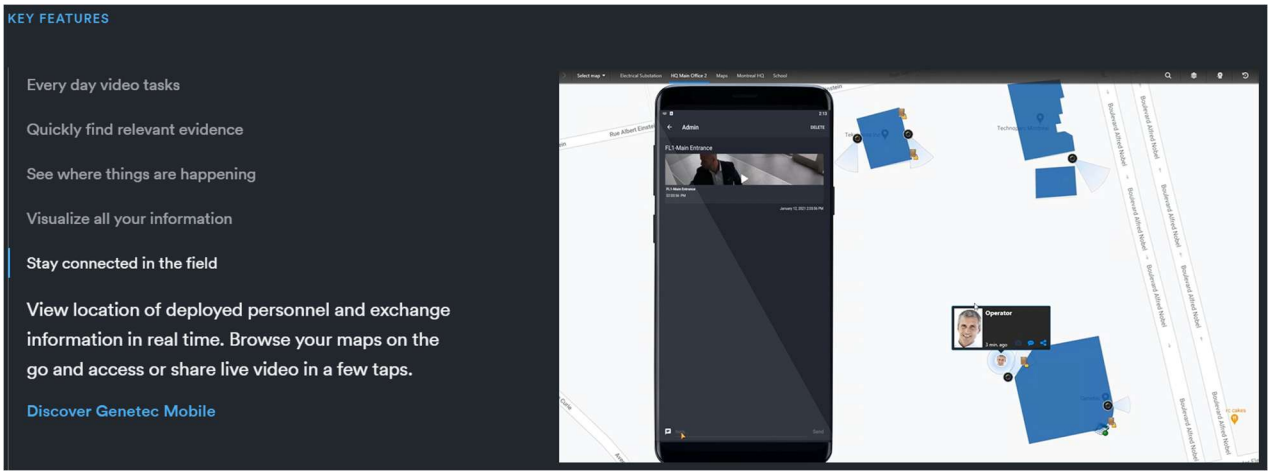


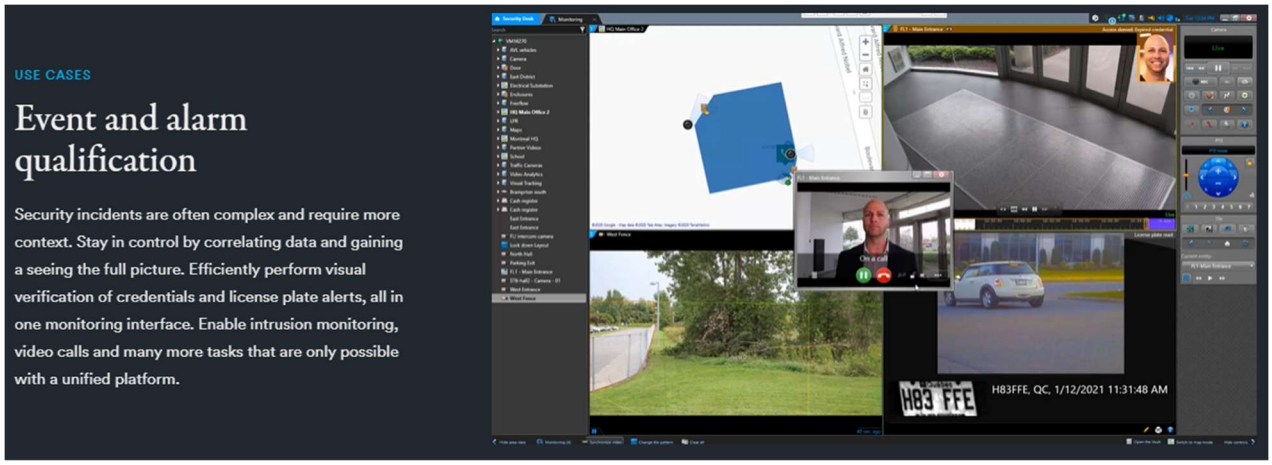
Source: *Genetec*, CRG, https://www.crgplans.com/integrations/genetec/ (last visited July 15, 2026).



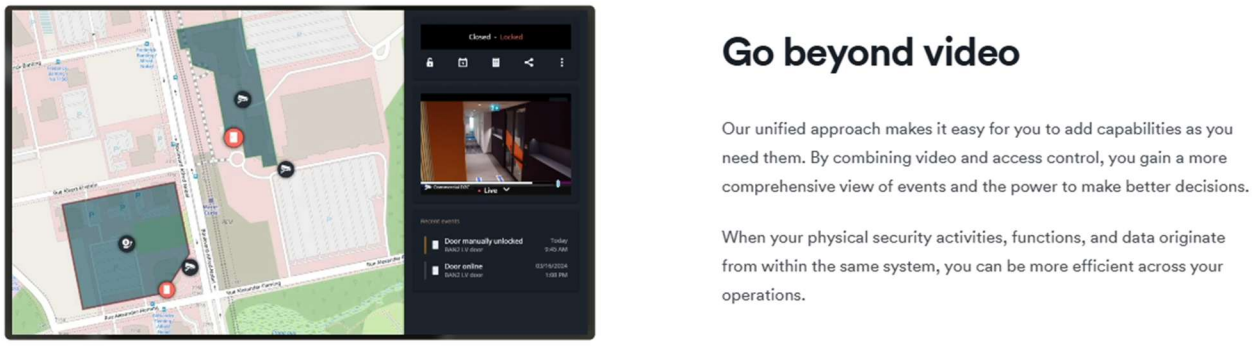
Source: *Collaborative Response Graphics* ®, CRG, https://www.crgplans.com/collaborative-response-graphics/ (last visited July 15, 2026).

27. On information and belief, each Infringing Product is configured to analyze the geographical location based on the security parameters and generate a geofence corresponding to a geographical area based on the analyzing. For example, the Infringing Products enable viewing security-related information according to their geographical locations including, for example, personnel, cameras, doors, alarms, and building perimeters. The Infringing Products display this information on a map with virtual, geo-fenced boundaries:





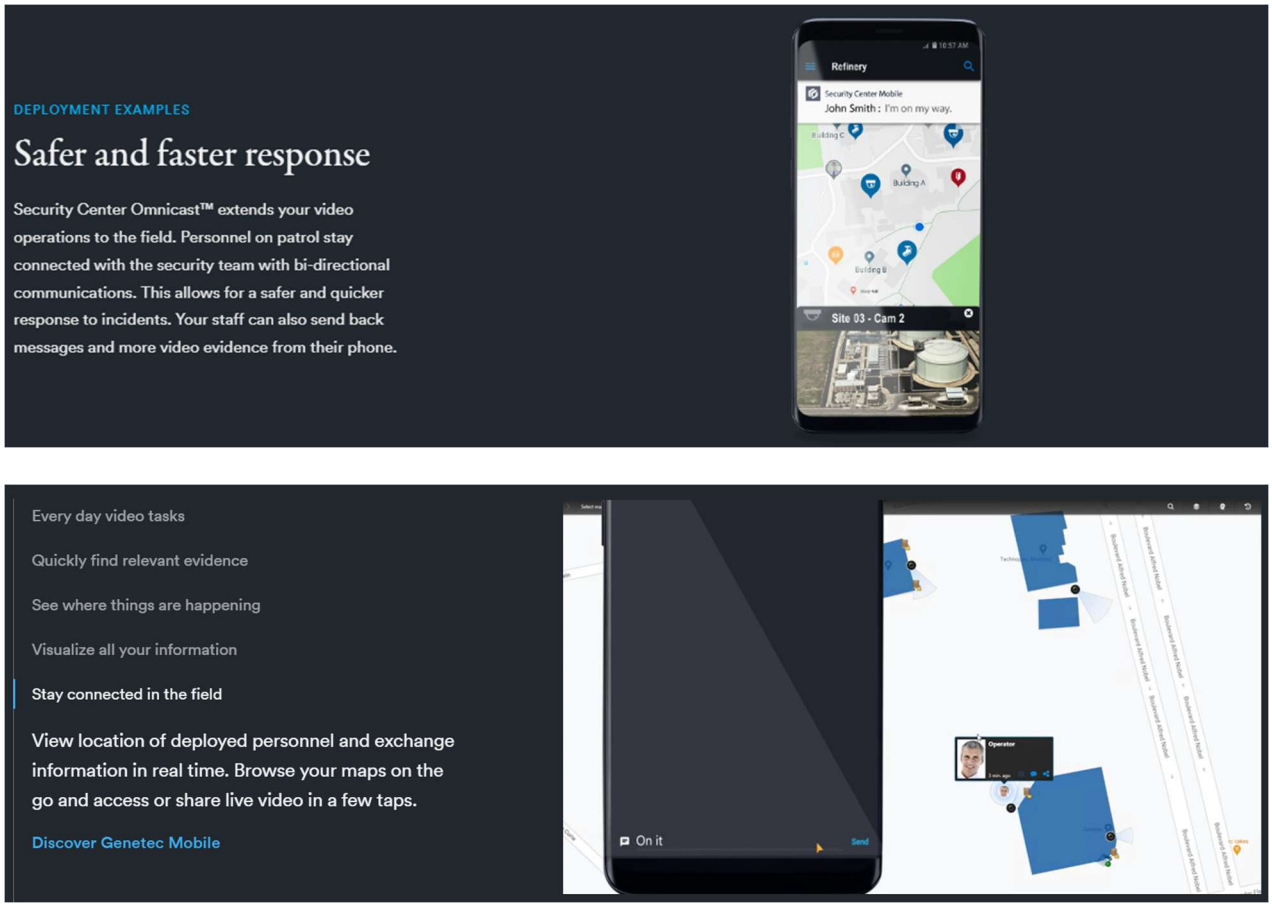
Source: *Genetec – Modern User Experience*, GENETEC.



Source: *Video Surveillance as a service*, GENETEC, https://www.genetec.com/products/unified-security/vsaas (last visited July 15, 2026).

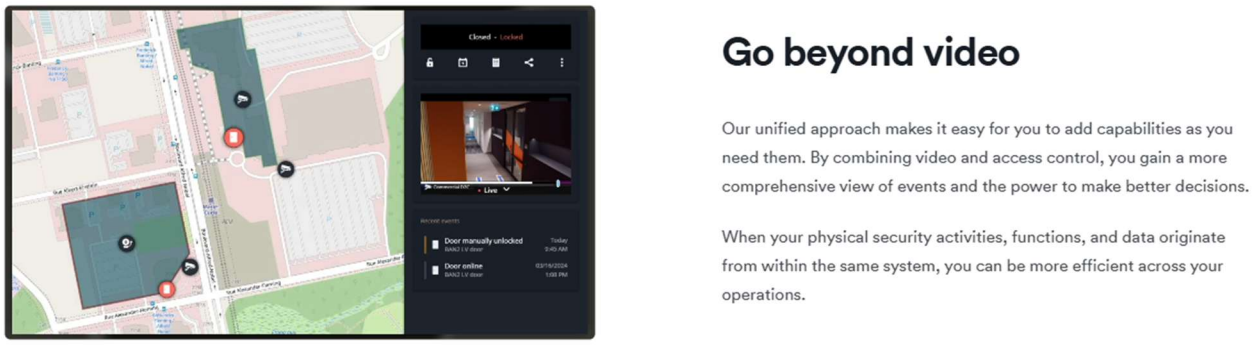
28. Each Infringing Product is configured to receive supervisee data and analyze it based on the geofence. For example, the Infringing Products enable "bi-directional communications" between security personnel and admins, transferring supervisee data (*e.g.*, data

associated with security personnel and/or individuals they are monitoring) to the servers and the admins, including exchanging messages "in real time" while supervisees are tracked within the geofenced geographical area:



Source: *Genetec – Modern User Experience*, GENETEC.

29. As another example, admins utilizing the Security Center Products can see locations, device activations, video feeds, and other supervisee data with respect to geographical location and within geofenced boundaries:



Source: *Video Surveillance as a service*, GENETEC.

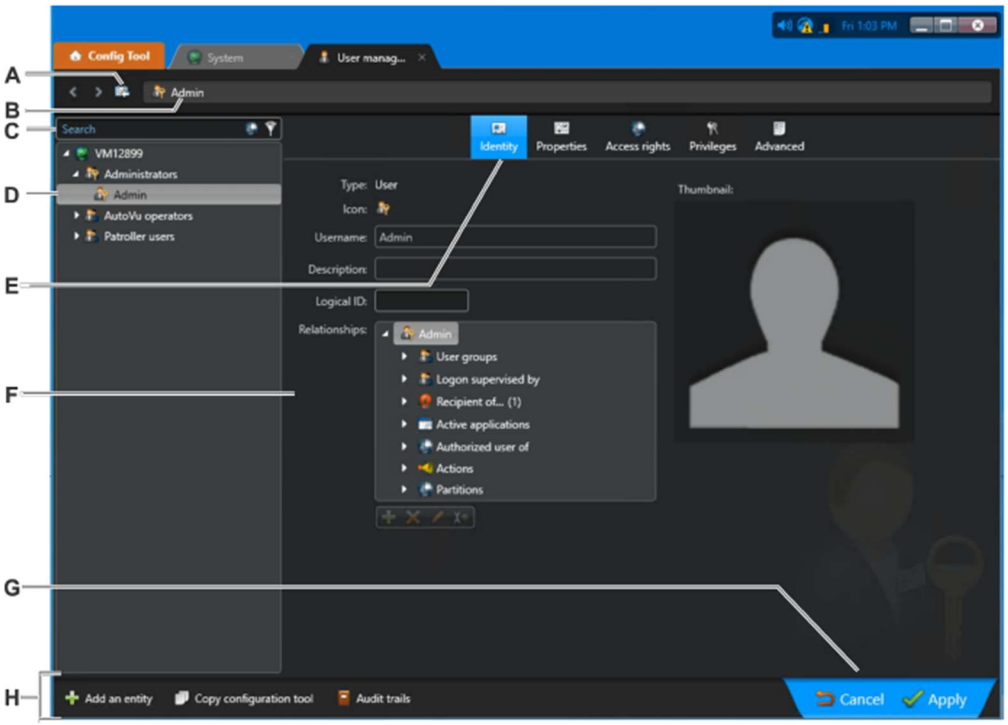
30. On information and belief, the Infringing Products generate supervision notifications based on the analysis and transmit notifications to supervisor devices. For example, as discussed above, these notifications can include, but are not limited to indications of personnel locations, event reports, alarm notifications, and bi-directional communications with deployed personnel.

31. As another example, the Infringing Products also transmit and store supervision notifications and supervisee data, including stored access and alarm history as well as recorded videos:

Administration task workspace overview

Administration tasks are where you create and configure the entities required to model your system.

This section describes the common elements of most administration tasks. The *User management* task is used in the following example. You can open the *User management* task by typing its name in the search box on the home page.



A	**Entity history**	Use these buttons to browse through recently used entities within this task.

Source: *Security Center Administrator Guide 5.10*, GENETEC, at 18 (June 12, 2023).

Managing video archives

You must work with your video archives to ensure that the recordings are always available to assist an investigation.

Security Center stores surveillance video as *video archives*. You control where the archives are stored and how long they are retained. To ensure your video is properly archived and available when you need it, you must perform the following tasks:

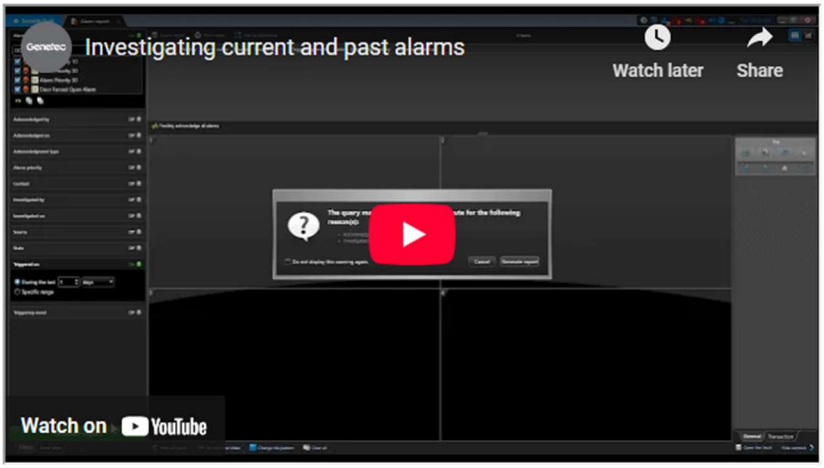
- Check the archive storage requirements to ensure you have enough room for your video recordings.
- If storage performance is an issue, consider distributing the archive storage over multiple disks.
- Regularly monitor how much disk space you have left to ensure there is always sufficient space for new recordings.
- When required, free up disk space by deleting older video files, shortening retention periods for cameras, and so on.
- Ensure the recordings are properly archived, easily accessible, and secure. You can:
  - Transfer video recordings from cameras or other edge devices to your video archives.
  - Copy video archives from one Archiver role to another.
  - Back up video archives to protect them from loss.
  - Restore video archives from a backup to an Archiver.
- Protect important video files from being automatically deleted.
- Protect important video files from tampering by adding digital signatures.
- Audit the archive storage by reviewing the video file properties.
- If required, manage the effects of Daylight Savings Time on your video archives.
- Import external video files to Security Center.

Id. at 636.

Investigating current and past alarms

You can search for and investigate current and past alarms, using the *Alarm report* task.

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

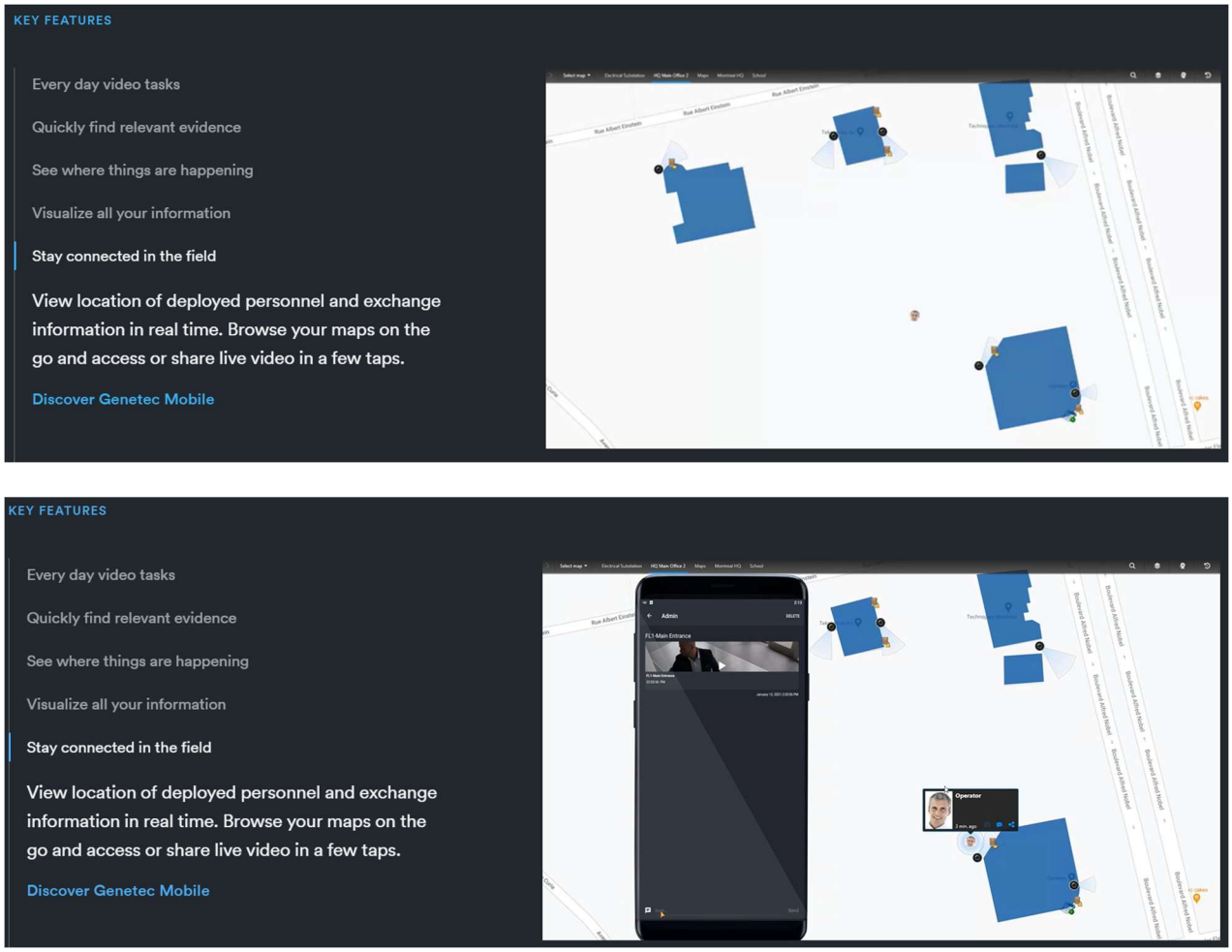


What you should know

In Security Desk, you can investigate the alarms that were triggered during the last week or since your last shift. You can also investigate major events that happened in your system (by only selecting critical alarms), who acknowledged a specific alarm, and why. You can also review the video associated to an alarm, which can then be exported and sent to law enforcement as evidence.

Source: *Security Center User Guide 5.12*, GENETEC TECHDOC HUB, https://techdocs.genetec.com/r/en-US/Security-Center-User-Guide-5.12/Investigating-current-and-past-alarms (last visited July 15, 2026).

32. On information and belief, each Infringing Product also generates a geofence that is characterized by a geofence area corresponding to the geographical area and comprises geofence grid boxes within the geofenced area. For example, as discussed above, the Infringing Products track supervisees on geofenced maps. Further, on Genetec's website, Genetec displays a clip showing a supervisee's icon moving in a stutter-step motion across a map, suggesting that the supervisee is moving from box to box within the gridded geofence:



Source: *Genetec – Modern User Experience*, GENETEC.

33. Additionally, on information and belief, Genetec enhances its grid-based geofencing via its partnership with CRG, using CRG's "Collaborative Response Graphics." CRG advertises the grid-based nature of its Collaborative Response Graphics as a key feature of the product, including a "gridded reference system" created by incorporating "key landmarks," "critical features," "site specific labels," "aerial imagery," and other parameters for determining how to establish the grid:

LAYER BREAKDOWN

Creating a Unified Map, Inside and Out

CRGs combine a gridded reference system, high-resolution imagery, floor plans, and critical features within a building and surrounding exterior areas to create a communication tool that is usable in a crisis and accessible by first responders through any smart device.

1. Grid & Template
2. Key Landmarks & Critical Features (AED, Gas, etc)
3. Site Specific Labels and Nomenclature
4. Highlighted Hallways, Stairwells, Doors, Exits
5. GeoRelevant Integrated Floorplans
6. Best Available Aerial Imagery

Source: *Collaborative Response Graphics* ®, CRG.

34. On information and belief, the Infringing Products are configured to receive at least one grid parameter. For example, as discussed above, Genetec's advertising shows maps comprising security personnel information as well as geographical location information. Further, the Infringing Products use grid-based geographical information gathered and created through the Collaborative Response Graphics technology obtained via Genetec's partnership with CRG:

Genetec™

Genetec integrates with Critical Response Group mapping for Cloud-Based Security Solutions

Integrated VMS Security Solutions with Genetec and Critical Response Group

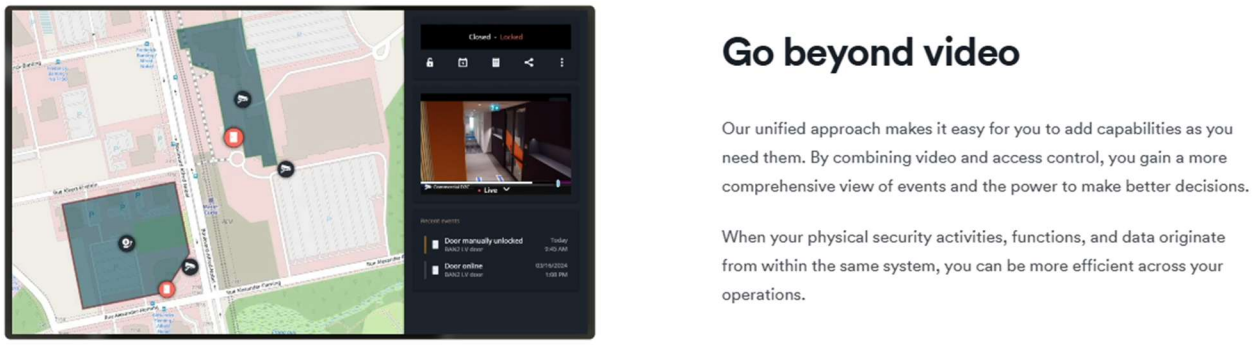
Genetec integrates Collaborative Response Graphics® into its Omnicast cloud-based VMS solutions, enhancing security and real-time emergency response coordination.

Omnicast™ is an IP-based VMS that lets you work smarter with video. With a clear picture of events, you respond quicker and make informed decisions. Its flexible architecture and efficient streaming reduces storage and lightens network load.

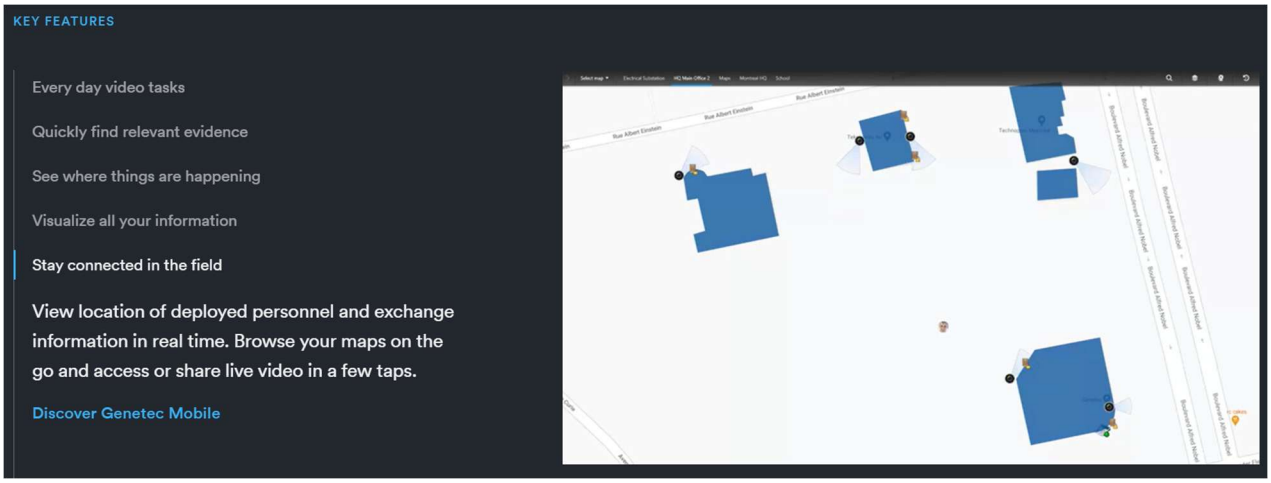
Source: *Genetec*, CRG.

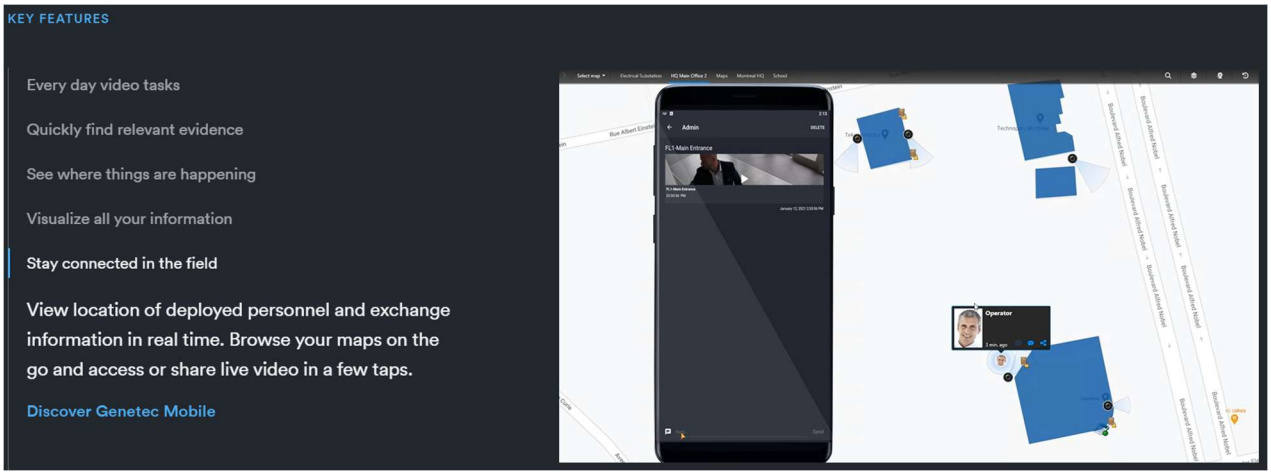
35. On information and belief, this geographical and security information constitutes grid parameters used by the Infringing Products.

36. On information and belief, the Infringing Products are configured to analyze grid parameters, determine a grid box geofence area based on the grid parameters, and generate geofence grid boxes accordingly. For example, as discussed above, Genetec's advertising for the Infringing Products shows maps comprising geographical information and security personnel moving across grid boxes on those maps—indicating that the Infringing Products use the grid parameters to generate grid boxes:



Source: *Video Surveillance as a service*, GENETEC.





Source: *Genetec – Modern User Experience*, GENETEC.

37. On information and belief, the steps described above are performed by Defendant's servers, which are installed locally on customer's computers and deployed on-premises at customers' campuses, through cloud-based servers to customers' remote locations, or a hybrid of both:

About servers

Feb 13, 2017

In Security Center, a server entity represents a computer on which the Genetec™ Server service is installed.

> IMPORTANT: Server names must be 15 characters or fewer. Security Center truncates all server names longer than 15 characters, causing errors when the system tries to access those servers.

Server entities are automatically created when the Security Center Server software is installed on a computer, and that computer is connected to the *main server* of your system.

Main server

The main server is the computer that hosts the *Directory* role. All other servers (expansion servers) on the system must connect to the main server in order to be part of the same system.

You can have only one main server on a Security Center system.

Expansion servers

An expansion server is a computer that you add to your system to increase its overall computing power. An expansion server must connect to the main server, and can host any role in Security Center, except the Directory role.

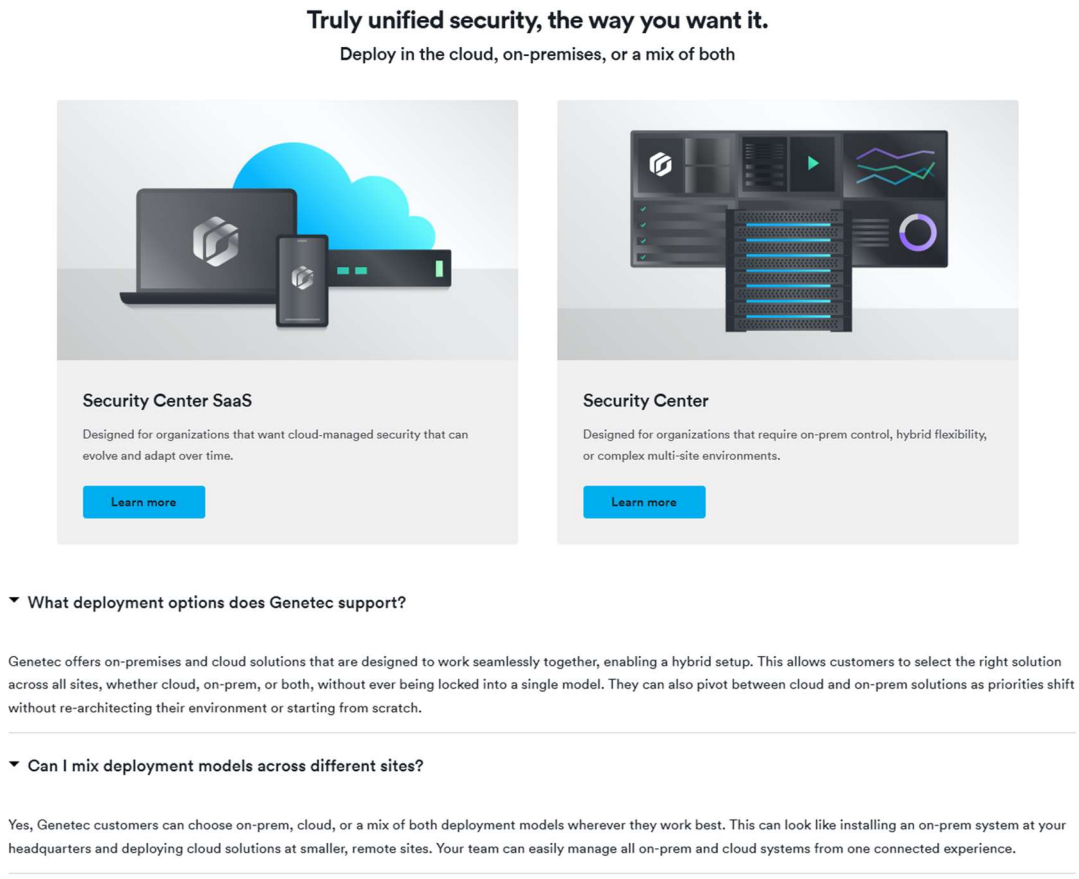
You can increase the computing power of your system at any time by adding more expansion servers to your pool of resources.

Genetec™ Server service

The Genetec™ Server service is a Windows service that is automatically installed when you install Security Center Server on a computer.

Security Center Server and the *Genetec™ Server* service must be installed on every computer that you want to include in the pool of servers available for Security Center. After the *Genetec™ Server* service is installed, you can change its password and other settings using the *Server Admin* web application.

Source: *Security Center Administrator Guide 5.12 | About Servers*, GENETEC TECHDOC HUB, https://techdocs.genetec.com/r/en-US/Security-Center-Administrator-Guide-5.12/About-servers (Feb. 13, 2017)



Source: *Security built for choice*, GENETEC, https://www.genetec.com/choice (last visited July 19, 2026).

38. Defendant has been and is now directly infringing, literally and/or under the doctrine of equivalents because without authority it makes, uses, offers to sell, sells, and/or imports within the United States the patented invention of one or more claims, including at least claim 1 of the '757 Patent. Defendant is therefore liable to Samscloud for patent infringement under 35 U.S.C. § 271(a).

39. Further, Defendant's customers and end users who offer for sale, sell, and/or use the Infringing Products directly infringe at least claim 1 of the '757 Patent.

40. Furthermore, Defendant has been and is now liable under 35 U.S.C. § 271(b) for actively inducing infringement of one or more claims including at least claim 1 of the '757 Patent. Genetec has had actual notice of the '757 Patent since at least its receipt of Samscloud's complaint. Despite such knowledge, Genetec has intended that its customers and end users infringe the '757 Patent by selling, offering for sale, importing, and/or using the Infringing Products in the United States, and has actively induced such infringement by instructing users in the United States to practice '757 Patent claims in their user manuals, posted videos and/or other materials with knowledge of the '757 Patent as set forth in this complaint and with knowledge of the '757 Patent since at least the time Genetec became aware of the '757 Patent.

41. As a result of Defendant's infringement of the '757 Patent, Samscloud has suffered and continues to suffer damages. Thus, Samscloud is entitled to recover from Defendant the damages Samscloud sustained as a result of Defendant's wrongful and infringing acts in an amount no less than a reasonable royalty, together with interest and costs fixed by this Court under 35 U.S.C. § 284.

42. Defendant's infringement of the '757 Patent was, is, and continues to be deliberate and willful. Moreover, Genetec was and is on notice of the '757 Patent at least as early as the filing of the Complaint in this lawsuit, yet continued and continues to infringe the '757 Patent.

COUNT II

(Infringement of the '421 Patent)

43. Plaintiff incorporates and re-alleges the allegations contained in paragraphs 1 through 42 herein by reference.

44. The '421 Patent entitled "Systems and methods for facilitating supervision of individuals based on geofencing" was duly and legally issued by the U.S. Patent and Trademark Office on November 26, 2024, from Application No. 18/045,781, published at US2023/0056959

on February 23, 2023. The ’421 Patent is a continuation-in-part of the ’757 Patent and also claims priority to provisional application 62/814,097 filed on March 5, 2019. A true and accurate copy of the ’421 Patent is attached hereto as Exhibit B.

45. Each and every claim of the ’421 Patent is valid and enforceable, and each enjoys a statutory presumption of validity under 35 U.S.C. § 282.

46. Samscloud exclusively owns all rights, title, and interest in and to the ’421 Patent and possesses the exclusive right of recovery, including the exclusive right to recover for past, present, and future infringement.

47. Claim 1 of the ’421 Patent recites:

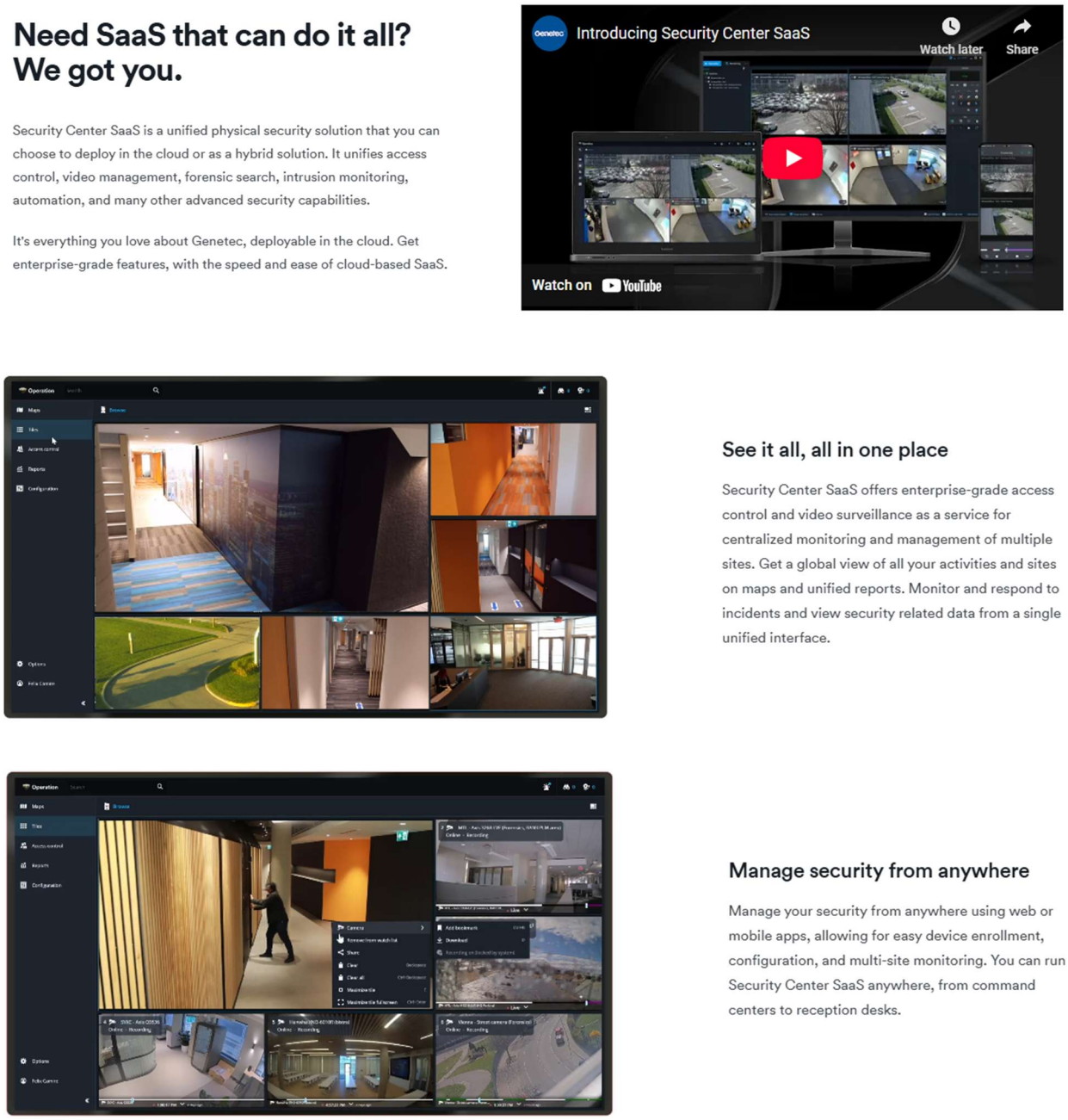
> A method for facilitating supervision of individuals based on geofencing, the method comprising:
> receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor;
> receiving, using the communication device, a geographical location from the at least one supervisor device;
> analyzing, using a processing device, the geographical location based on the at least one security parameter;
> generating, using the processing device, a geofence corresponding to a geographical area based on the analyzing;
> receiving, using the communication device, at least one supervisee data associated with a supervisee from at least one supervisee device;
> analyzing, using the processing device, the at least one supervisee data based on the geofence;
> generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data;
> transmitting, using the communication device, the supervision notification to the at least one supervisor device; and
> storing, using a storage device, the at least one supervisee data and the supervision notification, wherein:
> the geofence is characterized by a geofence area corresponding to the geographical area, wherein the geofence comprises a plurality of geofence grid boxes associated with the geofence area, wherein each geofence grid box is characterized by a grid box geofence area of the geofence area, wherein the method comprises:
> receiving, using the communication device, at least one grid parameter from the at least one supervisor device,
> analyzing, using the processing device, the at least one grid parameter;

determining, using the processing device, the grid box geofence area based on the analyzing of the at least one grid parameter; and
generating, using the processing device, a number of geofence grid boxes based on the determining.

48. Claim 22 of the ’421 Patent recites:

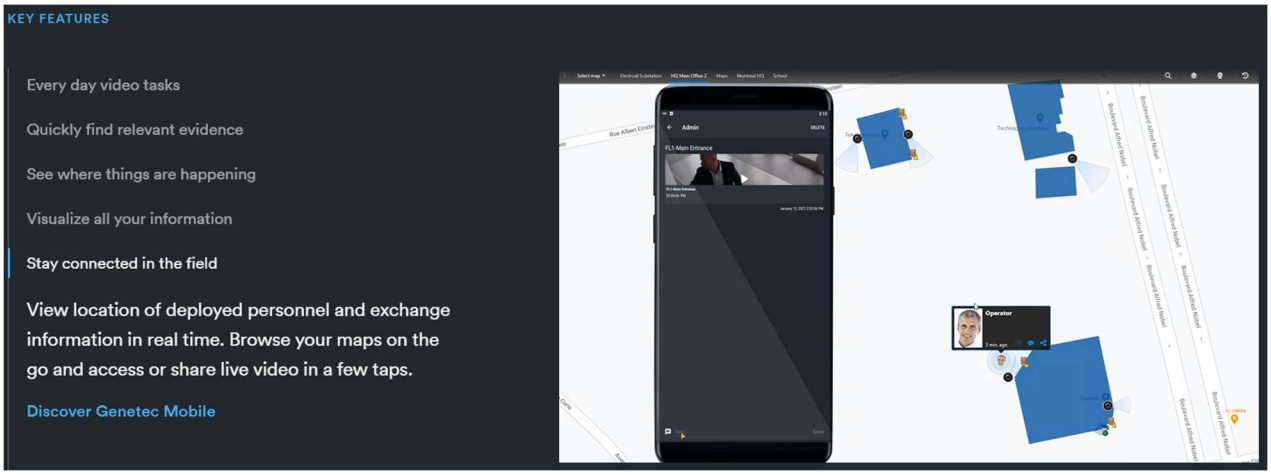
A method for facilitating supervision of individuals based on geofencing, the method comprising:
receiving, using a communication device, at least one security parameter from at least one supervisor device associated with at least one supervisor;
receiving, using the communication device, a geographical location from the at least one supervisor device;
analyzing, using a processing device, the geographical location based on the at least one security parameter;
receiving, using the communication device, at least one supervisee data associated with a supervisee from at least one supervisee device;
analyzing, using the processing device, the at least one supervisee data based on the geographical location;
generating, using the processing device, a supervision notification based on the analyzing of the at least one supervisee data;
transmitting, using the communication device, the supervision notification to the at least one supervisor device; and
storing, using a storage device, the at least one supervisee data and the supervision notification, wherein:
the at least one supervisee device comprises at least one sensor,
wherein the at least one sensor is configured for detecting at least one signal made by the supervisee,
wherein the at least one sensor is configured for generating the at least one supervisee data based on the detecting,
wherein the supervisee data comprises audio and video recordings;
wherein the at least one sensor is selected from one or more nearby sensors based on the most proximal nearby sensor by geographical location in real-time; and
wherein the at least one sensor tracks the supervisee as the supervisee moves between the one or more nearby sensors.

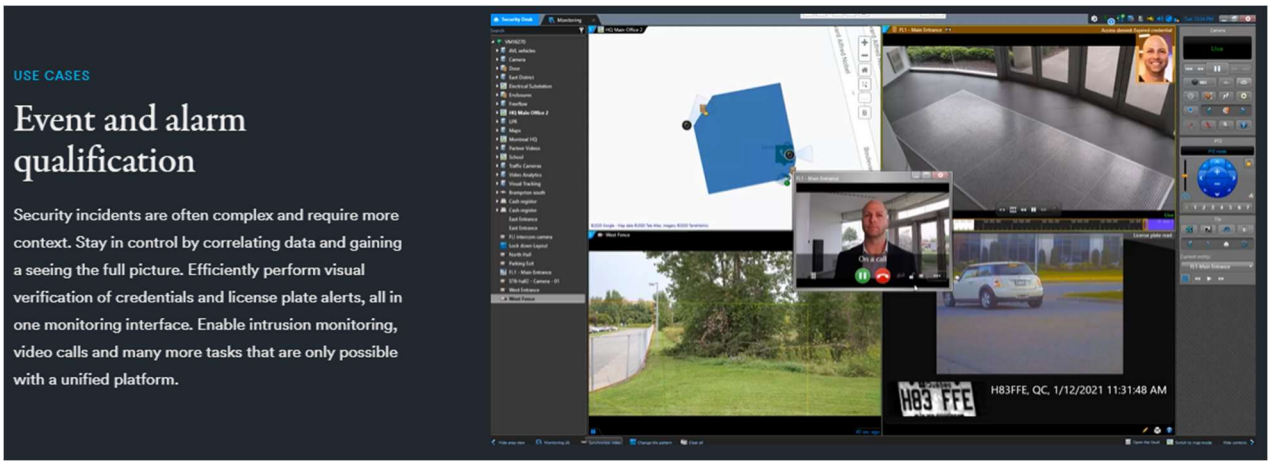
49. Each Infringing Product is configured to perform a method for facilitating supervision of individuals based on geofencing. For example, Genetec’s Security Center SaaS platform supervises individuals:



Source: *Security Center SaaS*, GENETEC, https://www.genetec.com/products/unified-security/security-center-saas (last visited July 15, 2026).

50. Further, on information and belief, the methods performed by the Infringing Products are based on geofencing. For example, Genetec's website shows that the Security Center Products track employee locations and video sources based on virtual boundaries showing the geographical locations of buildings and other important areas (*i.e.*, geofences):



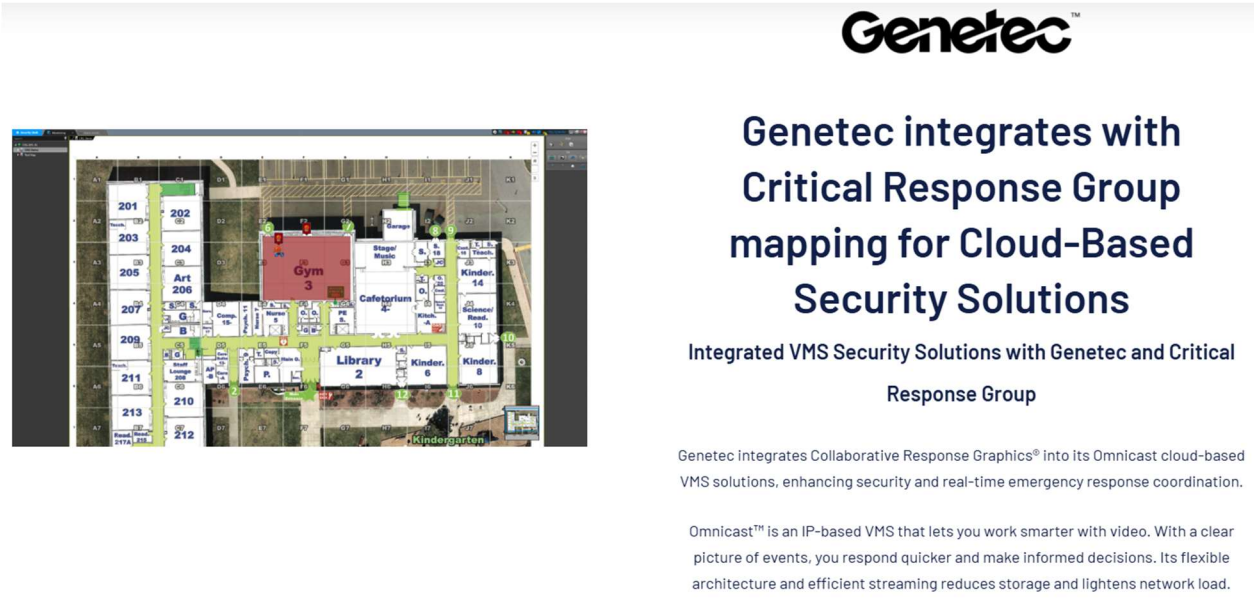


Source: *Genetec – Modern User Experience*, GENETEC, https://www.genetec.com/products/unified-security/omnicast/user-experience (last visited Mar. 6, 2026).

51. On information and belief, each Infringing Product is configured to receive security parameters from supervisor devices. For example, as discussed above regarding events and alarms and as seen further below, the Infringing Products receive and utilize a number of security parameters and geographical information, including parameters relating to alarms, credential verification, and security personnel locations:

Source: *Genetec – Modern User Experience*, GENETEC.

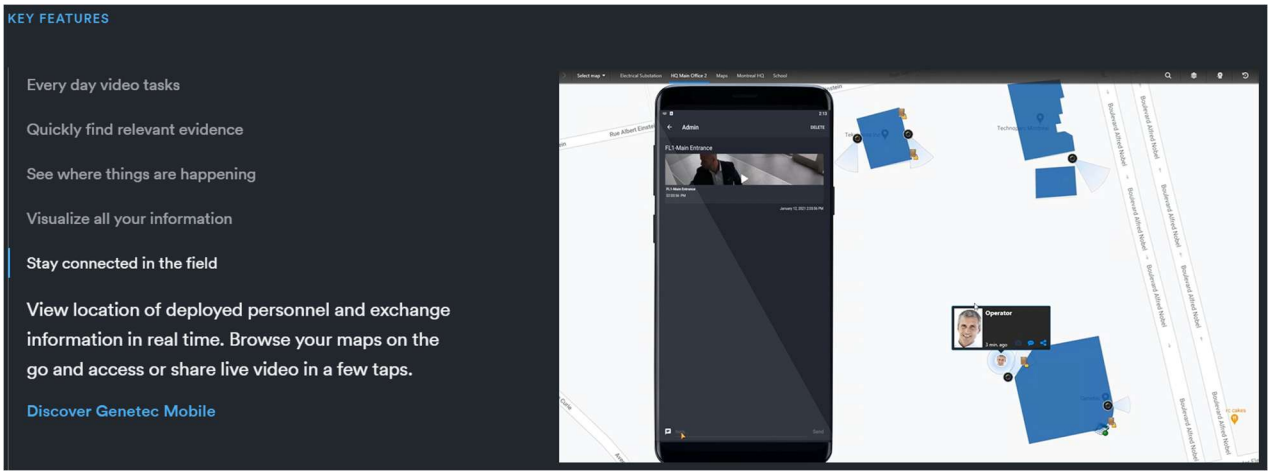
52. On information and belief, each Infringing Product is also configured to receive geographical locations from supervisor devices. For example, Genetec has partnered with Critical Response Group ("CRG") to integrate CRG's "Collaborative Response Graphics" and utilize "GeoRelevant integrated floor plans" and geospatial data (*i.e.*, geographical locations) to provide detailed maps and location information to users:

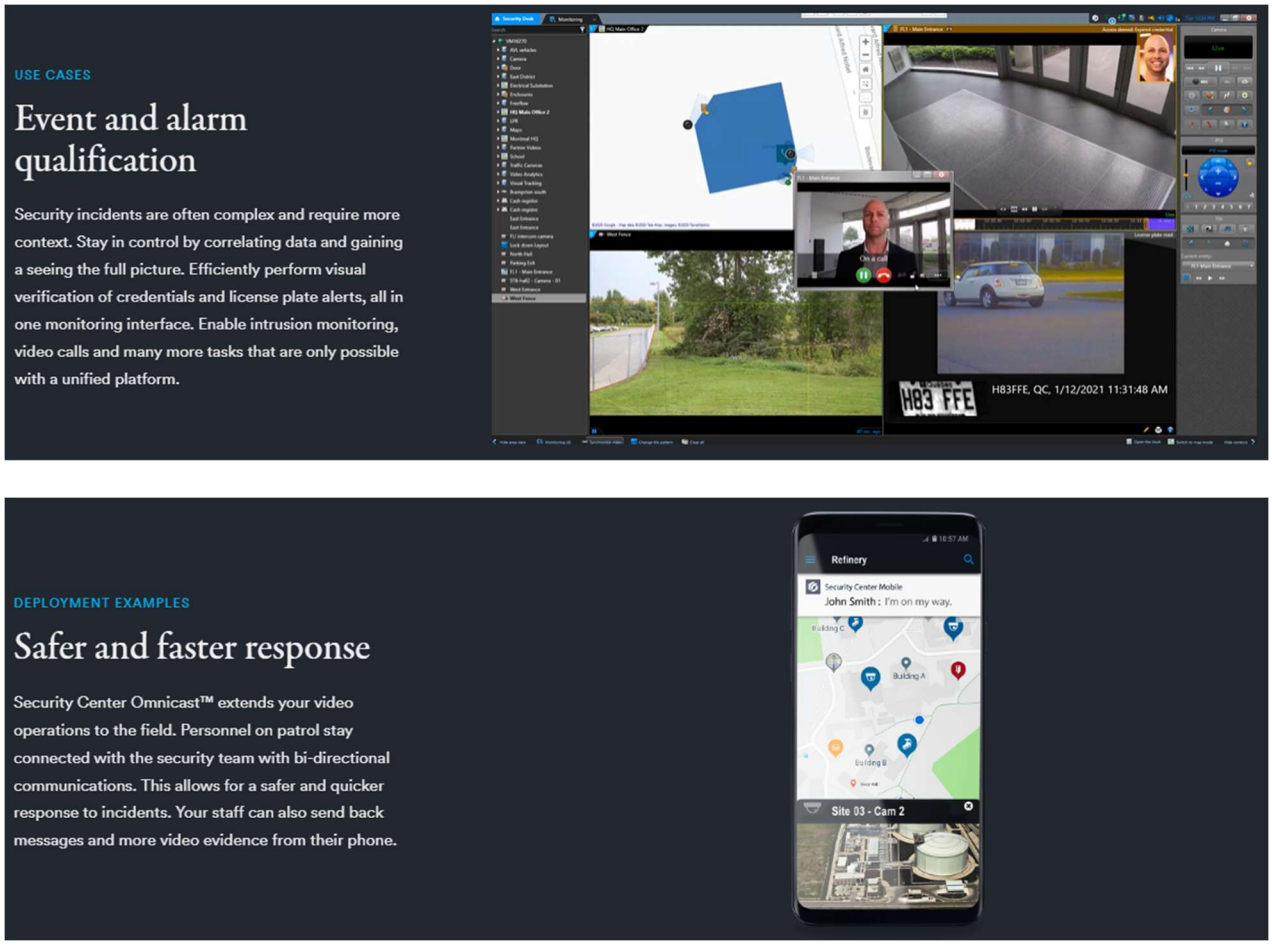


Source: *Genetec*, CRG, https://www.crgplans.com/integrations/genetec/ (last visited July 15, 2026).

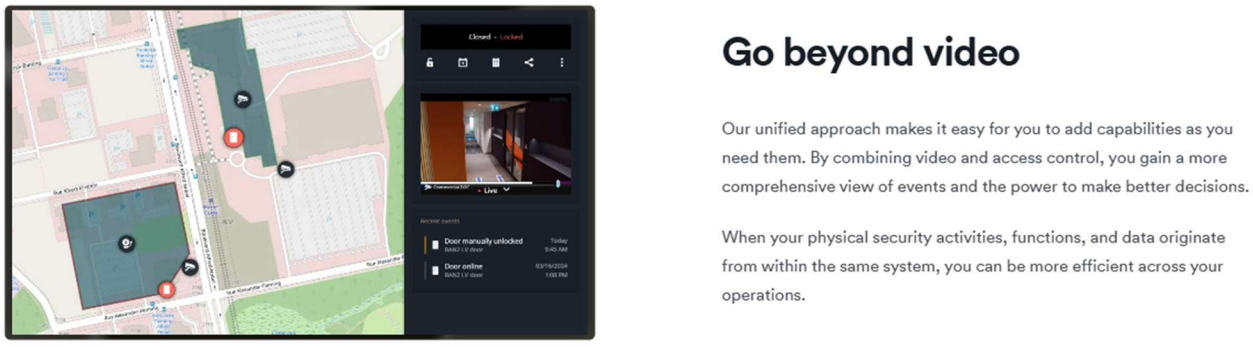
Source: *Collaborative Response Graphics* ®, CRG, https://www.crgplans.com/collaborative-response-graphics/ (last visited Mar. 6, 2026).

53. On information and belief, each Infringing Product is configured to analyze the geographical location based on the security parameters and generate a geofence corresponding to a geographical area based on the analyzing. For example, the Infringing Products enable viewing security-related information according to their geographical locations including, for example, personnel, cameras, doors, alarms, and building perimeters. The Infringing Products display this information on a map with virtual, geo-fenced boundaries:





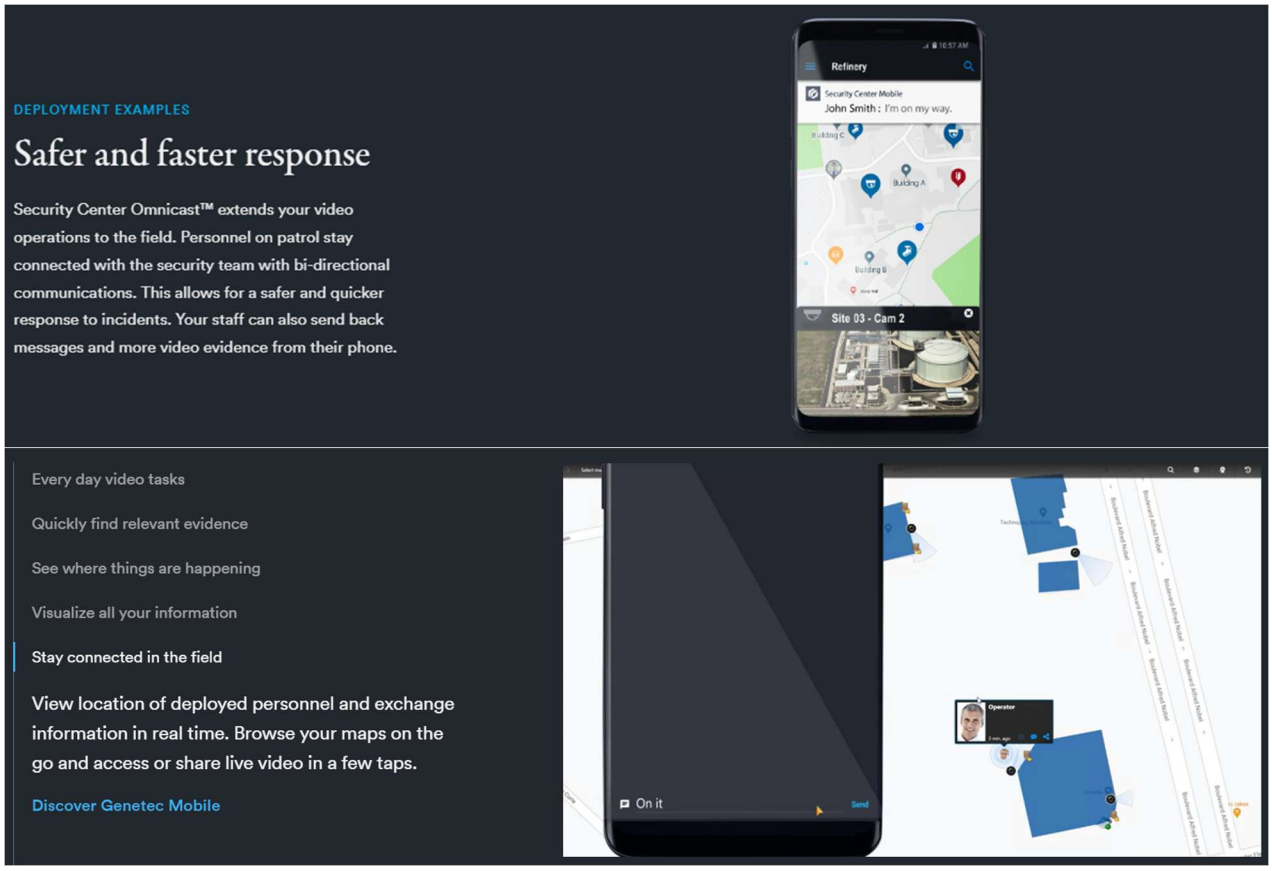
Source: *Genetec – Modern User Experience*, GENETEC.



Source: *Video Surveillance as a service*, GENETEC, https://www.genetec.com/products/unified-security/vsaas (last visited July 15, 2026).

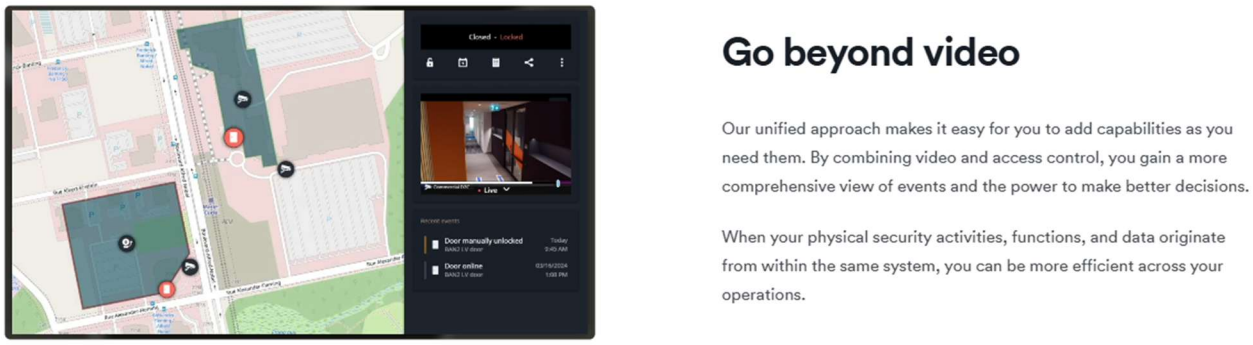
54. Each Infringing Product is configured to receive supervisee data and analyze it based on the geofence. For example, the Infringing Products enable "bi-directional communications" between security personnel and admins, transferring supervisee data (*e.g.*, data

associated with security personnel and/or individuals they are monitoring) to the servers and the admins, including exchanging messages "in real time" while supervisees are tracked within the geofenced geographical area:



Source: *Genetec – Modern User Experience*, GENETEC.

55. As another example, admins utilizing the Security Center Products can see locations, device activations, video feeds, and other supervisee data with respect to geographical location and within geofenced boundaries:



Source: *Video Surveillance as a service*, GENETEC.

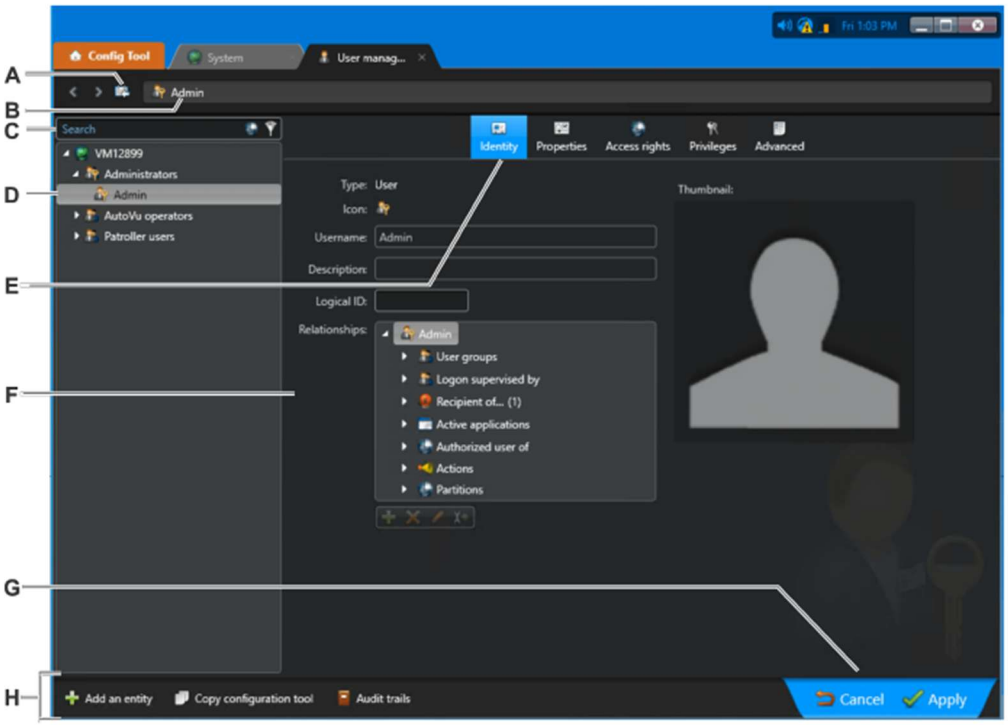
56. On information and belief, the Infringing Products generate supervision notifications based on the analysis and transmit notifications to supervisor devices. For example, as discussed above, these notifications can include, but are not limited to indications of personnel locations, event reports, alarm notifications, and bi-directional communications with deployed personnel.

57. As another example, the Infringing Products also transmit and store supervision notifications and supervisee data, including stored access and alarm history as well as recorded videos:

Administration task workspace overview

Administration tasks are where you create and configure the entities required to model your system.

This section describes the common elements of most administration tasks. The *User management* task is used in the following example. You can open the *User management* task by typing its name in the search box on the home page.



A	**Entity history**	Use these buttons to browse through recently used entities within this task.

Source: *Security Center Administrator Guide 5.10*, GENETEC, at 18 (June 12, 2023).

Managing video archives

You must work with your video archives to ensure that the recordings are always available to assist an investigation.

Security Center stores surveillance video as *video archives*. You control where the archives are stored and how long they are retained. To ensure your video is properly archived and available when you need it, you must perform the following tasks:

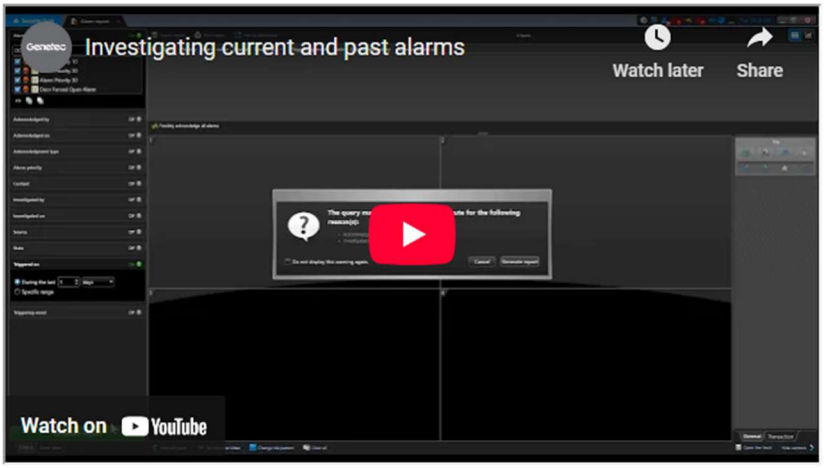
- Check the archive storage requirements to ensure you have enough room for your video recordings.
- If storage performance is an issue, consider distributing the archive storage over multiple disks.
- Regularly monitor how much disk space you have left to ensure there is always sufficient space for new recordings.
- When required, free up disk space by deleting older video files, shortening retention periods for cameras, and so on.
- Ensure the recordings are properly archived, easily accessible, and secure. You can:
  - Transfer video recordings from cameras or other edge devices to your video archives.
  - Copy video archives from one Archiver role to another.
  - Back up video archives to protect them from loss.
  - Restore video archives from a backup to an Archiver.
- Protect important video files from being automatically deleted.
- Protect important video files from tampering by adding digital signatures.
- Audit the archive storage by reviewing the video file properties.
- If required, manage the effects of Daylight Savings Time on your video archives.
- Import external video files to Security Center.

Id. at 636.

Investigating current and past alarms

You can search for and investigate current and past alarms, using the *Alarm report* task.

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

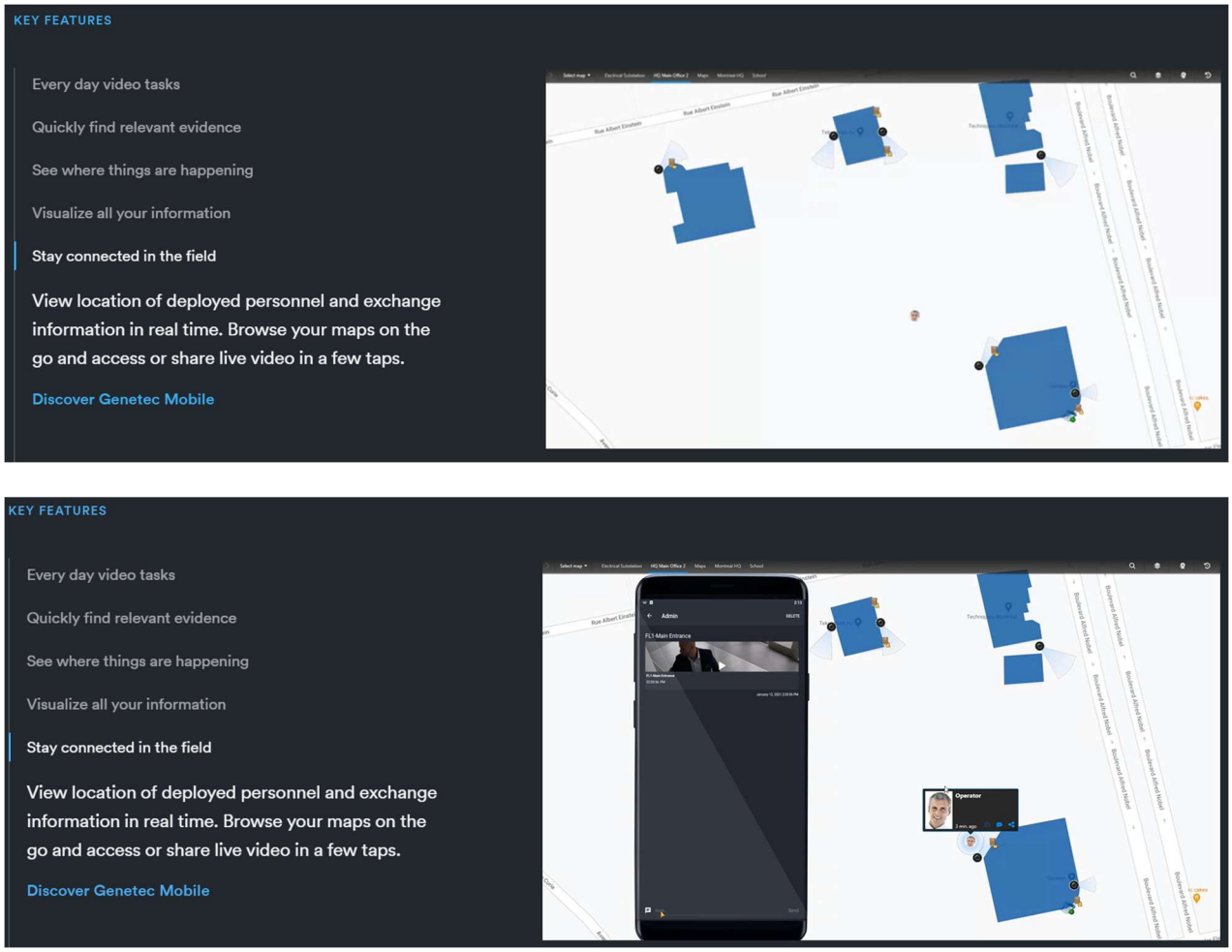


What you should know

In Security Desk, you can investigate the alarms that were triggered during the last week or since your last shift. You can also investigate major events that happened in your system (by only selecting critical alarms), who acknowledged a specific alarm, and why. You can also review the video associated to an alarm, which can then be exported and sent to law enforcement as evidence.

Source: *Security Center User Guide 5.12*, GENETEC TECHDOC HUB, https://techdocs.genetec.com/r/en-US/Security-Center-User-Guide-5.12/Investigating-current-and-past-alarms (last visited July 15, 2026).

58. On information and belief, each Infringing Product also generates a geofence that is characterized by a geofence area corresponding to the geographical area and comprises geofence grid boxes within the geofenced area. For example, as discussed above, the Infringing Products track supervisees on geofenced maps. Further, on Genetec's website, Genetec displays a clip showing a supervisee's icon moving in a stutter-step motion across a map, suggesting that the supervisee is moving from box to box within the gridded geofence:



Source: *Genetec – Modern User Experience*, GENETEC.

59. Additionally, on information and belief, Genetec enhances its grid-based geofencing via its partnership with CRG, using CRG's "Collaborative Response Graphics." CRG advertises the grid-based nature of its Collaborative Response Graphics as a key feature of the product, including a "gridded reference system" created by incorporating "key landmarks," "critical features," "site specific labels," "aerial imagery," and other parameters for determining how to establish the grid:

LAYER BREAKDOWN

Creating a Unified Map, Inside and Out

CRGs combine a gridded reference system, high-resolution imagery, floor plans, and critical features within a building and surrounding exterior areas to create a communication tool that is usable in a crisis and accessible by first responders through any smart device.

1. Grid & Template
2. Key Landmarks & Critical Features (AED, Gas, etc)
3. Site Specific Labels and Nomenclature
4. Highlighted Hallways, Stairwells, Doors, Exits
5. GeoRelevant Integrated Floorplans
6. Best Available Aerial Imagery

Source: *Collaborative Response Graphics* ®, CRG.

60. On information and belief, the Infringing Products are configured to receive at least one grid parameter. For example, as discussed above, Genetec's advertising shows maps comprising security personnel information as well as geographical location information. Further, the Infringing Products use grid-based geographical information gathered and created through the Collaborative Response Graphics technology obtained via Genetec's partnership with CRG:

Genetec

Genetec integrates with Critical Response Group mapping for Cloud-Based Security Solutions

Integrated VMS Security Solutions with Genetec and Critical Response Group

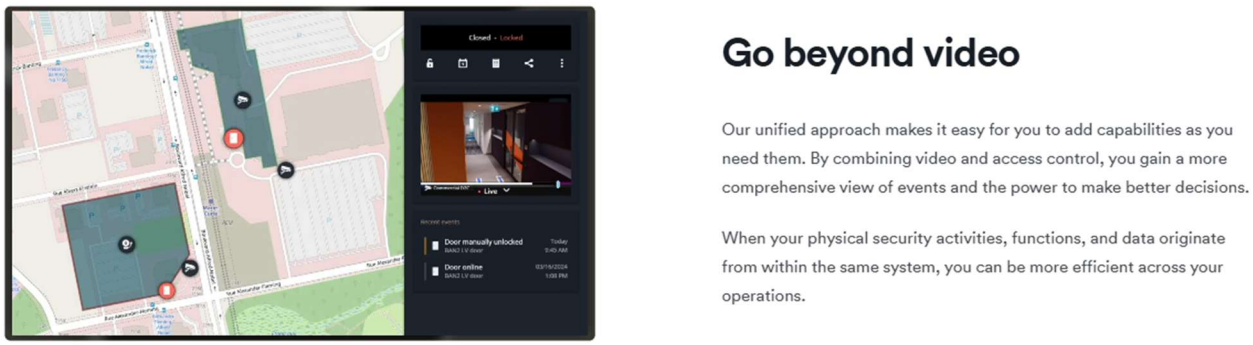
Genetec integrates Collaborative Response Graphics® into its Omnicast cloud-based VMS solutions, enhancing security and real-time emergency response coordination.

Omnicast™ is an IP-based VMS that lets you work smarter with video. With a clear picture of events, you respond quicker and make informed decisions. Its flexible architecture and efficient streaming reduces storage and lightens network load.

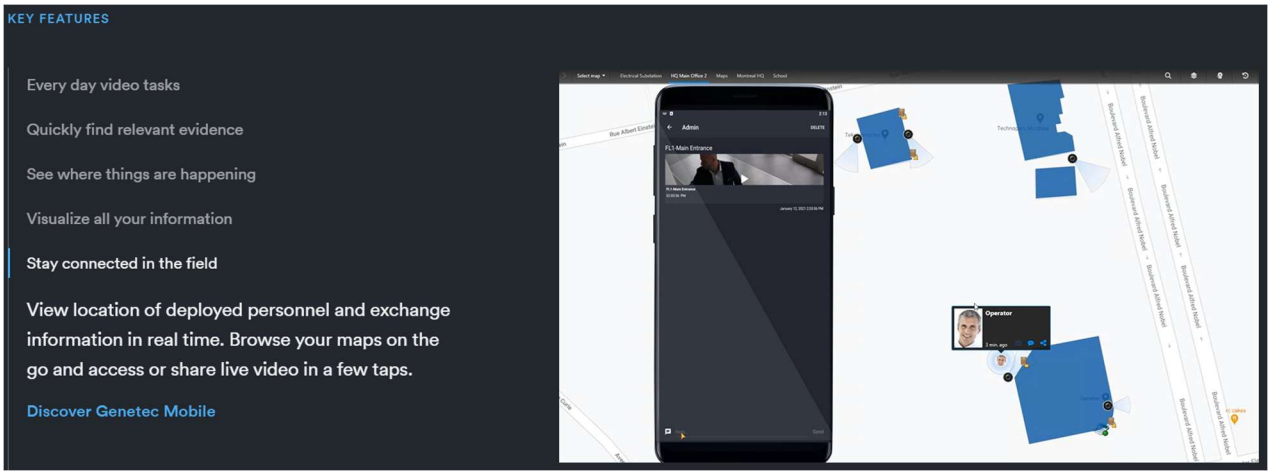
Source: *Genetec*, CRG.

61. On information and belief, this geographical and security information constitutes grid parameters used by the Infringing Products.

62. On information and belief, the Infringing Products are configured to analyze grid parameters, determine a grid box geofence area based on the grid parameters, and generate geofence grid boxes accordingly. For example, as discussed above, Genetec's advertising for the Infringing Products shows maps comprising geographical information and security personnel moving across grid boxes on those maps—indicating that the Infringing Products use the grid parameters to generate grid boxes:



Source: *Video Surveillance as a service*, GENETEC.



Source: *Genetec – Modern User Experience*, GENETEC.

63. On information and belief, the Infringing Products comprise sensors that are configured for detecting signals made by supervisees. For example, Genetec enables users to set alarms in response to situations detected by cameras, doors, and other security sensors in order to facilitate security responses. Those alarms can be triggered manually (*i.e.*, via signal made by a supervisee):

About alarms

Apr 16, 2025

An alarm entity informs users of a situation that requires immediate attention and provides details on how it can be handled in Security Center. For example, an alarm can indicate which entities (usually cameras and doors) best describe the situation, who must be notified, how it must be displayed to the user, and so on.

An alarm has the following basic properties:

- **Name:** Alarm name.
- **Priority:** Priority of the alarm (1-255), based on the urgency of the situation. Higher-priority alarms are displayed first in Security Desk.
- **Recipients:** Users, user groups, and analog monitor groups who are notified when the alarm occur. Recipients are responsible for responding to the alarm situation.
- **Broadcast mode:** How the alarm recipients are notified about the alarm.
  - **All at once:** All recipients are notified at the same time, immediately after the alarm is triggered.
  - **Sequential:** Each recipient is notified sequentially after a **Forward delay** that is calculated from the time the alarm is triggered. The maximum delay is 20 days, which is entered using seconds as the unit of measurement. If the recipient is a user group, all members of the group are notified at the same time.
- **Attached entities:** Entities that help describe the alarm situation, such as cameras, areas, doors, alarm procedures, and so on. When Security Desk receives an alarm, the attached entities can be displayed sequentially or all at once in the canvas.

  If a composite entity is attached to the alarm, the entities that compose it are also attached to the alarm. For example, if a door entity is attached to the alarm, the cameras associated to the door are also attached to the alarm.

Source: *Security Center Administrator Guide 5.12*, GENETEC TECHDOC HUB, https://techdocs.genetec.com/r/en-US/Security-Center-Administrator-Guide-5.12/About-alarms (Apr. 16, 2025).

Triggering alarms manually

To test an alarm that you just created, or if something critical occurs and you want to activate an alarm, you can trigger the alarm manually.

Before you begin

- The alarm must be configured in Config Tool.
- The alarm cannot be set to maintenance mode.
- If you want to trigger alarms from the *Monitoring* task, you must enable alarm monitoring.

Procedure

1 From the homepage, open the *Alarm monitoring* task or the *Monitoring* task.

2 Click **Trigger alarm** ( ).

3 From the list, select an alarm, and then click **Trigger alarm**.

All pre-configured alarm recipients receive the alarm if they are logged on to Security Desk.

Source: *Security Center User Guide 5.11*, GENETEC (July 5, 2024), at 512 (available for download at https://techdocs.genetec.com/r/en-US/Security-Center-5.11-guides/Security-Center-guides)

64. On information and belief, the Infringing Products' sensors are configured to generate supervisee data, based on the detection of the signal, that comprises audio and video recordings. For example, as discussed above, the Infringing Products generate and store video relating to triggered alarms or detected motion (*i.e.*, supervisee data) and the data collected by the Infringing Products comprises audio and video recordings:

Configuring recording settings for cameras

Mar 27, 2023

To set the recording mode (continuous, on motion, and so on) or enable encryption for your cameras, you can do so through the **Recording** tab of each individual camera.

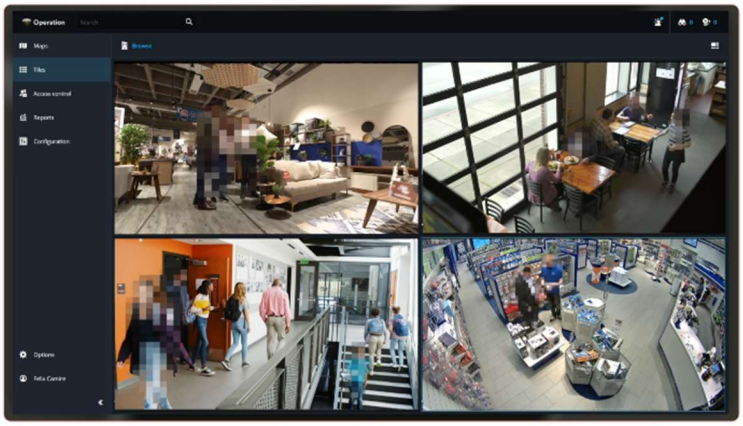
4. Click the **Recording modes** list and select a recording mode:

- **Continuous:** Records continuously. Recording cannot be stopped by the user ( ).
- **On motion/Manual:** Recording begins when triggered by the following:
  - A specific action, such as *Start recording*, *Add bookmark*, or *Trigger alarm*
  - Motion detection
  - User requests

  In this mode, the **Record** button in Security Desk indicates the recording status:

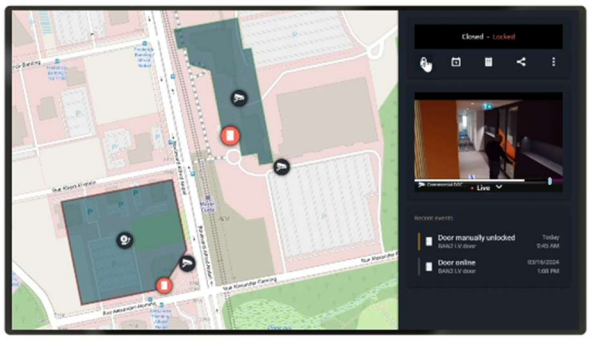
  - Grey ( ) when the system is not recording. Clicking the button starts the recording.
  - Red ( ) when the system is recording. Clicking the button stops the recording.
  - Red with a lock ( ) when the system is recording and cannot be stopped by the user, such as on motion or on alarm.
- **Manual:** Records only when a user or a system action, such as *Start recording*, *Add bookmark*, or *Trigger alarm*, requests it.
- **Custom:** Recording is specified by custom schedules.

Source: *Security Center User Guide 5.12*, GENETEC TECHDOC HUB, https://techdocs.genetec.com/r/en-US/Security-Center-Administrator-Guide-5.12/Configuring-recording-settings-for-cameras (Mar. 27, 2023).



Data protection and resiliency

Security Center SaaS offers VSaaS that's specially designed for mission critical applications and features uninterrupted streaming of live or recorded video, with redundancy. Built-in video anonymization capabilities make sure you can provide both privacy and security while you protect your everyday.



Go beyond video

Our unified approach makes it easy for you to add capabilities as you need them. By combining video and access control, you gain a more comprehensive view of events and the power to make better decisions.

When your physical security activities, functions, and data originate from within the same system, you can be more efficient across your operations.

Source: *Video Surveillance as a service*, GENETEC.

65. On information and belief, the Infringing Products' sensors that generate supervisee data are selected from one or more nearby sensors based on the most proximal nearby sensor by

geographical location in real-time. For example, as discussed above, audio and video can be automatically recorded based on triggered alarms. Cameras and other sensors can also be selected based on their geographical location:

Source: *Plan Manager Feature Note*, GENETEC, at 1-2 (2020) (available for download at https://resources.genetec.com/en-feature-notes/security-center-plan-manager).

66. On information and belief, the Infringing Products' sensors track supervisees as the supervisees move between one or more nearby sensors. For example, as shown above, the Infringing Products can track supervisees between cameras (*i.e.*, sensors), including between floors and facilities.

67. On information and belief, the steps described above are performed by Defendant's servers, which are installed locally on customer's computers and deployed on-premises at customers' campuses, through cloud-based servers to customers' remote locations, or a hybrid of both:

About servers

Feb 13, 2017

In Security Center, a server entity represents a computer on which the Genetec™ Server service is installed.

> IMPORTANT: Server names must be 15 characters or fewer. Security Center truncates all server names longer than 15 characters, causing errors when the system tries to access those servers.

Server entities are automatically created when the Security Center Server software is installed on a computer, and that computer is connected to the *main server* of your system.

Main server

The main server is the computer that hosts the *Directory* role. All other servers (expansion servers) on the system must connect to the main server in order to be part of the same system.

You can have only one main server on a Security Center system.

Expansion servers

An expansion server is a computer that you add to your system to increase its overall computing power. An expansion server must connect to the main server, and can host any role in Security Center, except the Directory role.

You can increase the computing power of your system at any time by adding more expansion servers to your pool of resources.

Genetec™ Server service

The Genetec™ Server service is a Windows service that is automatically installed when you install Security Center Server on a computer.

Security Center Server and the *Genetec™ Server* service must be installed on every computer that you want to include in the pool of servers available for Security Center. After the *Genetec™ Server* service is installed, you can change its password and other settings using the *Server Admin* web application.

Source: *Security Center Administrator Guide 5.12 | About Servers*, GENETEC TECHDOC HUB, https://techdocs.genetec.com/r/en-US/Security-Center-Administrator-Guide-5.12/About-servers (Feb. 13, 2017)

Truly unified security, the way you want it.

Deploy in the cloud, on-premises, or a mix of both

Security Center SaaS

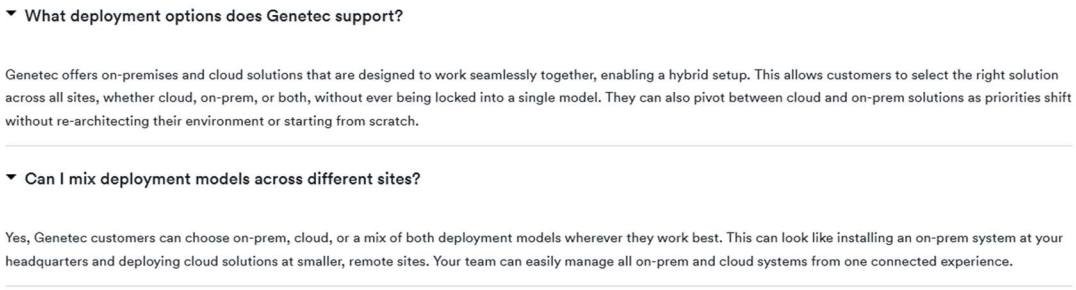
Designed for organizations that want cloud-managed security that can evolve and adapt over time.

Learn more

Security Center

Designed for organizations that require on-prem control, hybrid flexibility, or complex multi-site environments.

Learn more



Source: *Security built for choice*, GENETEC, https://www.genetec.com/choice (last visited July 19, 2026).

68. Defendant has been and is now directly infringing, literally and/or under the doctrine of equivalents because without authority it makes, uses, offers to sell, sells, and/or imports within the United States the patented invention of one or more claims, including at least claims 1 and 22 of the ’421 Patent. Defendant is therefore liable to Samscloud for patent infringement under 35 U.S.C. § 271(a).

69. Further, Defendant’s customers and end users who offer for sale, sell, and/or use the Infringing Products directly infringe at least claims 1 and 22 of the ’421 Patent.

70. Furthermore, Defendant has been and is now liable under 35 U.S.C. § 271(b) for actively inducing infringement of one or more claims including at least claims 1 and 22 of the ’421 Patent. Genetec has had actual notice of the ’421 Patent since at least its receipt of Samscloud’s complaint. Despite such knowledge, Genetec has intended that its customers and end users infringe the ’421 Patent by selling, offering for sale, importing, and/or using the Infringing Products in the United States, and has actively induced such infringement by instructing users in the United States to practice ’421 Patent claims in their user manuals, posted videos and/or other materials with knowledge of the ’421 Patent as set forth in this complaint and with knowledge of the ’421 Patent since at least the time Genetec became aware of the ’421 Patent.

71. As a result of Defendant’s infringement of the ’421 Patent, Samscloud has suffered and continues to suffer damages. Thus, Samscloud is entitled to recover from Defendant the

damages Samscloud sustained as a result of Defendant's wrongful and infringing acts in an amount no less than a reasonable royalty, together with interest and costs fixed by this Court under 35 U.S.C. § 284.

72. Defendant's infringement of the '421 Patent was, is, and continues to be deliberate and willful. Moreover, Genetec was and is on notice of the '421 Patent at least as early as the filing of the Complaint in this lawsuit, yet continued and continues to infringe the '421 Patent.

CONCLUSION

73. Defendant has directly and/or indirectly infringed on Plaintiff's rights as owner of the Asserted Patents. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of Defendant's wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court.

74. Plaintiff has incurred and will incur attorneys' fees, costs, and expenses in the prosecution of this action. The circumstances of this dispute may give rise to an exceptional case within the meaning of 35 U.S.C. § 285, and Plaintiff is entitled to recover its reasonable and necessary attorneys' fees, costs, and expenses.

JURY DEMAND

75. Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

76. Plaintiff requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

1. A judgment that Defendant has infringed the Asserted Patents as alleged herein;
2. A judgment that Defendant's infringement of the Asserted Patents was deliberate and willful;

3. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendant;
4. A judgment and order requiring Defendant to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;
5. A judgment and order requiring Defendant to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;
6. A judgment and order finding this to be an exceptional case and requiring Defendant to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and
7. Such other and further relief as the Court deems just and equitable.

OF COUNSEL:

Robert M. Harkins
CHERIAN HARKINS DUNHAM LLP
555 12th Street, Suite 2140
Oakland, CA 94607
(510) 944-0190

Thomas M. Dunham
J. Michael Woods
CHERIAN HARKINS DUNHAM LLP
1901 L St. NW, Suite 700
Washington, DC 20036
(202) 838-1560

Hunter S. Palmer
CHERIAN HARKINS DUNHAM LLP
12 Greenway Plaza, Suite 1133
Houston, TX 77046
(945) 205-0305

Dated: July 23, 2026
13065837

POTTER ANDERSON & CORROON LLP

By: */s/ Philip A. Rovner*

Philip A. Rovner (#3215)
Nicole K. Pedi (#6236)
Hercules Plaza, 6th Floor
1313 North Market Street
Wilmington, DE 19801
(302) 984-6000
provner@potteranderson.com
npedi@potteranderson.com

Attorneys for Plaintiff Samscloud, LLC