UNITED STATES DISTRICT COURT
DISTRICT OF COLORADO

Civil Action No.

SecureNet Solutions Group, LLC,

Plaintiff,

v.

Arrow Electronics, Inc.,

Defendant.

COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement arising under the Patent Laws of the United States of America, 35 U.S.C. § 1 *et seq*. Plaintiff SecureNet Solutions Group, LLC (the "Plaintiff" or "SecureNet") sues Defendant Arrow Electronics, Inc. (the "Defendant" or "Arrow") for patent infringement via the sale and offer for sale of various end-to-end IT and OT solutions in the internet of things space. Arrow offers and sells technologies for profit that are protected by, and infringe on Patents owned by SecureNet, including but not limited to, U.S. Patent Nos. 9,344,616, 10,862,744 and 11,323,314 (the "Asserted Patents"). Arrow's infringing products or technologies include, but are not limited to, sensors, hardware, software, and services such as Lumada (Hitachi Vantara), Gorilla Edge Technology in combination with Intel hardware, and Infineon hardware and software in combination with analytics and cloud storage (collectively, the "Products" or the "Accused Instrumentality").

I. Parties

1. Plaintiff SecureNet Solutions Group, LLC is a limited liability company organized and existing under the laws of the State of Florida, with its principal place of business at 2073 Summit Lake Drive, Suite 155, Tallahassee, Florida 32317.

2. On information and belief, Defendant Arrow Electronics, Inc. is a company incorporated under the laws of New York with its principal place of business at 9201 E. Dry Creek Road, Centennial, Colorado 80112.

II. Jurisdiction and Venue

3. This action arises under the Patent Laws of the United States, Title 35 of the United States Code. The Court has original subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over Arrow in this action pursuant to Colorado's long arm statute, C.R.S. § 13-1-124(a) & (b), which provides personal jurisdiction over any defendant who transacts business or commits tortious acts in this state. Arrow transacts business and commits tortious acts in this state, as it has its principal place of business in Colorado and markets and sells its products to Colorado consumers.

5. Venue is proper in this district under 28 U.S.C. § 1400(b) because Arrow has its principal place of business in Colorado and is subject to the Court's personal jurisdiction with respect to this action.

III. The Background of the Asserted Patents

6. The claims of the Asserted Patents address a need arising specifically within the field of computerized security systems. Inventors Daniar Hussain and Dr. John Donovan conceived of the inventions. Mr. Hussain was educated at MIT in electrical engineering, biomedical engineering, and computer science and studied theoretical geophysics at the University of Cambridge, and environmental engineering and civil engineering at Carnegie Mellon University. He won the Siemens Westinghouse National Science Award (2000), a national award given to one team in the United States for engineering excellence. According to Science Magazine, this is "a junior Nobel Prize." He worked for NASA on techniques for sending satellite image data to mobile devices, and for Siemens Corporate Research developing techniques for 3D image registration. He is a named inventor on more than a dozen U.S. patents and five foreign patents.

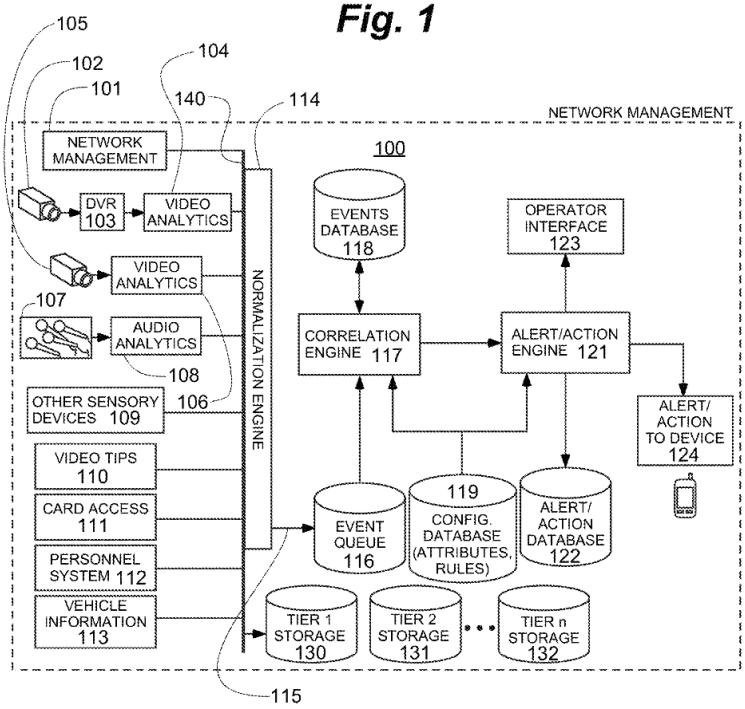
7. Hussain and Donovan conceived the inventions after a three-day workshop with CLEMIS, the IT Department for the Oakland County, Michigan confederation of police departments—the largest confederation of police departments in the country. During the workshop, the police described several major problems with known police IT systems. In 2007 (the priority date for the Asserted Patents), smart surveillance systems gained commercial adoption and started to replace traditional security systems, causing challenges for large-scale data analysis. *See e.g.,* Lisa Brown, Arun Hampapur, Jonathan Connell, Max Lu, Andrew Senior, Chiao-Fe Shu, Yingli Tian, IBM Smart Surveillance System (S3): *An open and extensible*

architecture for smart video surveillance, IBM T.J. Watson Research Center, Proceedings of the IEEE Conference on Advanced Video and Signal Based Surveillance, AVSS 2005, Sept. 15-16, 2005.

8. The claims of the Asserted Patents disclose technical solutions to some challenges, such as reducing errors and false positives via a particular computerized process. In particular, the inventors conceived of systems and methods for using integrated cameras, sensor networks, and other data sources with a correlation engine that correlates two or more events weighted by the attribute data of the data sources. Such correlations could effectively connect crime-related events to specific sensor data, other legacy system data, 911 calls, anonymous tips, and video records.

9. A high-level depiction of one embodiment of the invention is illustrated in Figure 1 of the U.S. Patent No. 10,862,744 (the "'744 Patent"):

Fig. 1



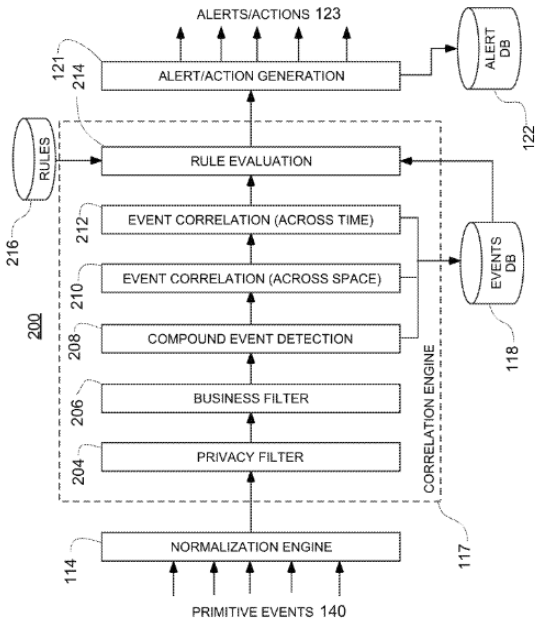
Declaration of Mukul Shirvaikar ("Shirvaikar Decl."), attached hereto as **Exhibit A**, ¶14 (citing 744 Patent, Fig. 1). In this embodiment, various types of security-related data are collected from various sources, such as video cameras and other sensory devices, a video tip system, a card access system, a personnel system, and a vehicle information module. *Id.* These data describe "primitive events," which are "atomic, indivisible event[s] from any subsystem," such as people entering a designated area, a vehicle driving the wrong way in a designated lane, a package left behind in an area, a person screaming, glass breaking, or a gunshot. *Id.* (citing 744' Patent[1] at 7:62-8:3).

10. The primitive events are then normalized by the normalization engine. *Id.* at ¶15 (citing 6:26-28). The normalization engine normalizes the primitive events into a "normalized event 115," which is in "a standardized format the system can recognize." *Id.* (citing 10:45-48). The specification points out that "each type of sensory device may have its own normalization engine." *Id.* (citing 10:45-51). Or, "one normalization engine as shown in FIG. 1 may have multiple modules for each type of sensory device." *Id.* (citing 10:56-58).

11. In the described embodiment, "[n]ormalized events 115 are placed in event queue 116 for processing by correlation engine 117." *Id.* at ¶16 (citing 10:63-65). The basic function of the correlation engine is to "correlate[] two or more primitive events, combinations of primitive events and compound events, and

[1] For ease of reference, all citations are to the '744 Patent, however all of the Asserted Patents contain the same elements cited herein.

combinations of compound events." *Id.* (citing 11:10-13). Carrying out this function is quite complex. Figure 2 shows how the correlation engine works in one embodiment of the invention:



Id. (citing Fig. 2 (rotated)).

12. As described by the specification, the correlation engine receives normalized events from the normalization engine. *Id.* at ¶17 (citing 11:50-55). These normalized events are then filtered by a privacy filter 204, which applies a set of privacy rules defined by a system administrator. *Id.* (citing 11:50-59). For example, a privacy rule may instruct the system to ignore all primitive events between certain time periods, or to disregard other categories of data. *Id.* (citing 11:59-12:12).

13. After applying the privacy filter, the correlation engine applies the business filter, which applies a set of business rules set by a system administrator. *Id.* at ¶18 (citing 12:12-16). The objective of the business filter is to "eliminate []

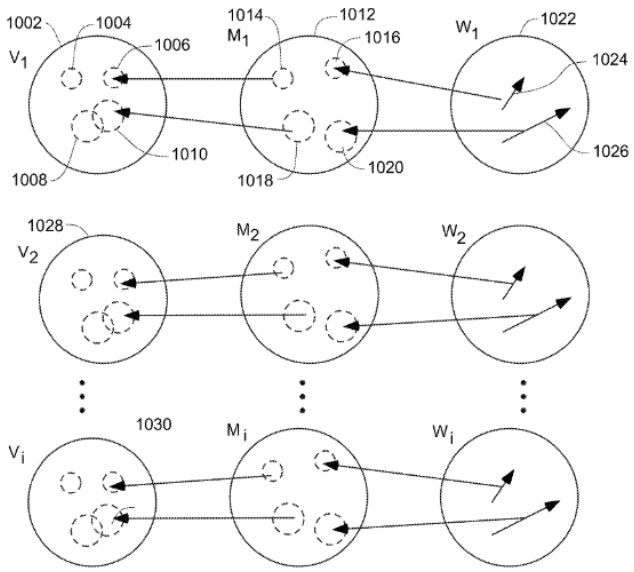
unnecessary false alarms by disregarding events when they are not significant based on normal business processes." *Id.* (citing 12:24-26). For example, in a security system designed to guard a data center, a business filter could be configured to ignore primitive events taking place during hours when the data center is scheduled to be serviced. *Id.* (citing 12:20-24).

14. After the correlation engine has filtered primitive events based on the privacy and business rules, it evaluates the remaining primitive events for the presence of "compound events"—events that are composed of one or more primitive events. *Id.* at ¶19 (citing 12:27-30). An example of a compound event is tailgating (i.e., where two or more persons enter a designated area as detected on the video data using a person-counting algorithm, when only one corresponding swipe/access card is detected by the legacy access control system). *Id.* (citing 12:30-40). Compound events "may include primitive events from one sensor, from two or more sensors, or even from two disparate types of sensors." *Id.* (citing 12:40-43).

15. Next, the correlation engine uses a "correlation module 210" to correlate both the primitive and compound events across geographical space. *Id.* at ¶20 (citing 12:44-46). For example, the correlation engine may identify multiple tailgating events in different parts of a facility, or the loitering of two different vehicles in different parts of a campus. *Id.* (citing 12:50-52). The correlation module also correlates events across time, by comparing events detected presently with events detected in the past. *Id.* (citing 12:52-56). Examples include detection of the presence of the same

individual allowing another to tailgate at different times, or the same person loitering or being stopped multiple times by security. *Id.* (citing 12:56-61).

16. The correlation engine's forensic analysis of events is depicted in even greater detail in Figure 10 of the specification:



Id. at ¶21 (citing Fig. 10). Figure 10 depicts various sets of video data (i.e., V_1 through V_i; the large circles in the first column), with each subset corresponding to data obtained from a particular video camera. *Id.* (citing 35:39-49). The dashed circles inside V_1 through V_i each represent a subset of video data. *Id.*

17. Figure 10 also depicts various sets of meta-data (i.e., M1 through Mi; the large circles in the second column). *Id.* at ¶22 (citing 35:50-56). Each set of meta-data is indexed and points to at least one set of video data. *Id.* (citing 35:56-57). In Figure 10, each set of meta-data corresponds to one and only one set of video data, but the specification is clear that the relationship between meta-data and video data may be one-to-many, many-to-one, as well as many-to-many. *Id.* (citing 35:57-64).

18. Finally, Figure 10 depicts various sets of attribute weight data (i.e., W1 through Wi; the large circles in the third column). *Id.* at ¶23 (citing 35:65-67). The sets of attribute weight data "are sets of vectors … which represent weights associated with subsets of the meta-data M1." *Id.* (citing 35:67-36:2). These weights may be multi-dimensional. *Id.* (citing 36:4-7). For example, a two-dimensional weight may represent the attribute weights associated with (i) the reliability of a particular video camera for motion detection reliability; and (ii) the reliability of that camera for gunshot detection reliability. *Id.* (citing 36:7-11). This would enable the system to account for the fact that a camera might have high motion detection reliability and low gunshot detection reliability, or vice-versa. *Id.* (citing 36:11-14). The specification provides an equation that can be used for determining weights for attribute data:

$$w_i = \sum_{k=1}^{N} \omega_k a_k$$

Id. (citing 39:27-34). In this equation, "[t]he weights "ω_i" may be a weighted average of attribute data (a_i)." *Id.* (citing 39:14-22). The symbol "ω_k" refers to relative weights of the attributes (a_k), "which are themselves weights associated with the data sources." *Id.* (citing 39:34-36).

19. The specification further discusses how attribute weights may be recalculated to yield the weighted attribute data of (i) two or more events occurring substantially simultaneously, or (ii) any of two or more events occurring substantially simultaneously. *Id.* at ¶24 (citing 39:9-33). Respectively, the formulae are as follows:

(i) $W(M_1 \cap M_2) = W(M_1) \cdot W(M_2)$

(ii) $W(M_1 \cup M_2) = W(M_1) + W(M_2) - W(M_1) \cdot W(M_2)$

Id.

20. As the compound events and correlated events are detected, the correlation module stores them in the events database 118. *Id.* at ¶25 (citing 12:62-66). The data may be stored in an events table such as the following:

TABLE 3

Events table

MDEntryID	MDParameterID	MD_Event_DateTime	MD_Event_Duration	SrcID	Src_Description	Src_Location
. . .	. . .	. . .	. . .	. . .	. . .	. . .
432	6	Sep. 27, 2007 7:05:24PM	1:05	1	Camera 1	Lobby
433	16	Sep. 27, 2007 7:10:18PM	0:01	1	Camera 1	Lobby
434	11	Sep. 27, 2007 8:13:08PM	0:01	9	Card Reader in Server Room	Server Room
435	10	Sep. 27, 2007 8:13:10PM	0:02	4	Camera 34	Server Room
436	10	Sep. 27, 2007 8:13:14PM	0:02	4	Camera 34	Server Room
437	12	Sep. 27, 2007 8:13:24PM	0:06	4	Camera 34	Server Room
438	14	Sep. 27, 2007 9:05:00PM	0:26	23	Registered Student	Off-campus (River St.)
439	15	Sep. 27, 2007 9:14:04PM	0:10	2	Camera 2	Parking Lot

Id. (citing Table 3). Here, the column "MDEntryID" contains the unique identifiers of the events. *Id.* (citing 26:64-68). "MDParameterID" refers to the types of events that were detected, which are fully described in a separate Meta-data parameters table. *Id.* (citing *Id.*) An example of a Meta-data parameters table is as follows:

TABLE 1

Meta-data parameters table

MDParametersID	Nickname	MDTypeID	SrcID	MD_TimeStart	MD_TimeEnd
6	Motion in Camera 1	1	1	17:00	8:00
. . .	. . .	. . .	. . .	. . .	. . .
10	Person Enters Server Room	23	4	0:00	23:59
11	Swipe Card Detected to Server Room	22	9	0:00	23:59
12	Tailgating	24	4	0:00	23:59
13	Anonymous Video Tip	98	22	0:00	23:59
14	Registered Student Video Tip	98	23	0:00	23:59
15	Stolen Plate	99	2	17:00	8:00
16	Camera 1 loses connection	105	1	0:00	23:59

Id. (citing Table 1). Here, the "MDParametersID" column contains the unique identifiers of the meta-data parameter, (*id.* (citing 23:63-64)) and "MDTypeID" refers to the Meta-data types, which are fully described in a separate Meta-data types table. *Id.* (citing 23:67-68 and Table 2). The "SrcID" column refers to the Sources table, which describes the devices (such as video cameras and card readers) used by the correlation engine. *Id.* (citing 23:68-24:2 and Table 4). The specification provides a number of examples to illustrate the functionality of the Meta-data parameters table and its relationship among the other tables. One example is as follows:

> For example, the row "MDParametersID=6" corresponds to an event with a nickname "Motion in Camera 1." This event has "MDTypeID=1", which by examining Table 2 corresponds to a motion event. It has "SrcID=1", which by examining Table 4 corresponds to Camera 1 located in a lobby. Based on "MD_TimeStart" and "MD_TimeEnd", this event is only being monitored and recorded between the hours of 5:00 PM (17:00) and 8:00 AM (8:00) to protect privacy or to follow a business rule.

Id. (citing 24:6-14).

21. When the rule evaluation module 214 retrieves the events in the events database, it does so in accordance with a set of rules from a rules database 216. *Id.* at

¶26 (citing 12:66-13:1) An exemplar Rules table from the rules database is depicted as follows:

TABLE 5

Rules table

RuleID	Nickname	MDParamterID	ThresholdValue	ContactID	MsgTxt
1	Alert 1	6	null	4	Motion in lobby during forbidden hours
2	Tailgating SR	12	null	1	Tailgating in server room
3	Global Alert	null	61	7	Null
4	Stolen Plate	15	null	2	Stolen plate detected in parking lot
5	Camera 1 goes down	16	null	null	Camera 1 has lost connection!

Id. (citing Table 5). An exemplar description of an alert defined in Table 5 is provided by the specification:

> In the sample Rules table shown in Table 5, "AlertID" is a primary key uniquely identifying each rule, "Nickname" provides a nickname for each rule, "MDParameterID" specifies which event (including primitive or compound events) that triggers the alert (or null if a system-wide alert), "ThresholdValue" specifies a threshold value which triggers an alert (for correlated system-wide alerts, or null if an event-based alert), "ContactID" specifies the group, or individual, that will receive the alert, or the set of actions that will be triggered by the alert, and "MsgTxt" specifies the text of the message sent on an alert. "ContactID" is a foreign key into another table (not shown) that specifies the list of recipients or the list of actions to be performed when the alert corresponding to "ContactID" is triggered.

Id. (citing 31:34-37).

22. The above description of the database tables is only a summary. The specification's "Database Design" section describes in great detail these and various other database tables, as well as the relationships among them. *Id.* at ¶27 (citing Tables 1-7).

23. Based on the evaluation of rules by the rule evaluation module 214, the correlation engine issues alerts or performs other appropriate actions. *Id.* at ¶28 (citing 13:4-6). These alerts may be issued in real-time in response to the correlation exceeding a particular threshold. *Id.* (citing 38:35-52). Sets of specific conditions may also be specified, and alerts and other actions can be configured to be triggered only when a certain set of conditions are met. *Id.*

24. Further, actions can be configured to be triggered based on "accumulated value of multiple events across space and time." *Id.* at ¶29 (citing 38:53-56). Although the specification provides that various equations may be used, it provides three examples of such equations:

$$a_1: \sum_{i=1}^{i=N} w_i \cdot x_i + \sum_{i=1}^{m} w_i \cdot v_i \geq \tau_1$$

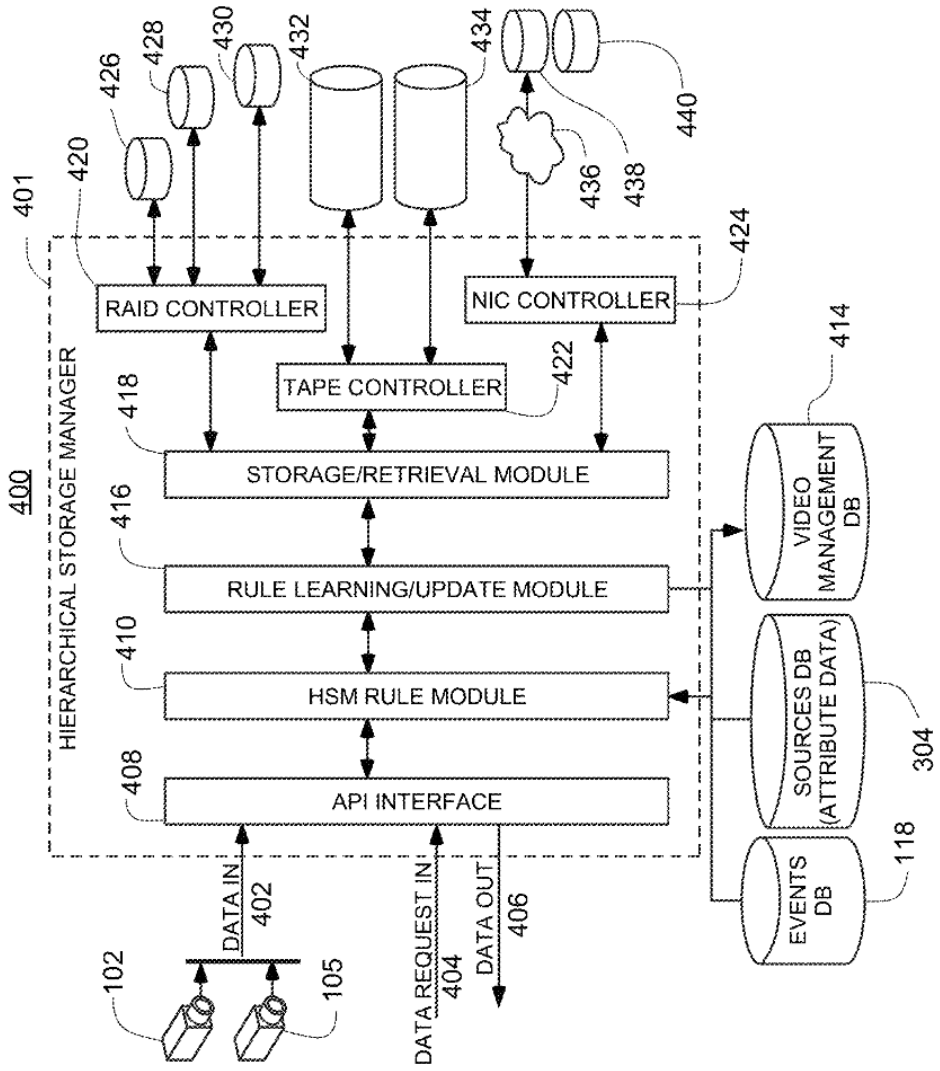
$$a_2: \sum_{i=1}^{i=N} w_i \cdot x_i + \sum_{i=1}^{m} w_i \cdot v_i \geq \tau_2$$

$$\cdots$$

$$a_n: \sum_{i=1}^{i=N} w_i \cdot x_i + \sum_{i=1}^{m} w_i \cdot v_i \geq \tau_n$$

Id. (citing 39:1-13). In these equations, "a" indicates an action, "w" indicates attribute weights, "x" indicates non-video events, and "v" indicates video events. (28:60-62). These equations "could represent a hierarchy of actions that would be activated for different threshold scenarios." *Id.* (citing 28:62-64).

25. The Asserted Patents also describe a Hierarchical Storage Manager (HSM) for intelligent storage of large volumes of data created by security and surveillance applications. *Id.* at ¶30 (citing Fig. 4).



Id. citing Fig. 4; (rotated)). The HSM resolves a problem that arises from the sheer volume of sensor data in smart surveillance systems. Routine operation of the sensors in the claimed invention generate large amounts of data. *Id.* (citing 14:63-15:22). "For example, a typical 3-Mega-pixel digital surveillance camera generates images of

approximately 280 Kbytes per second per frame. If the camera were running at 5 frames per second, it would generate approximately 60 GB per day. . . In a typical application having 100 surveillance cameras around a particular facility, this translates to 6 TB per day… or approximately 2,000 TB per year." *Id*. "Ideally, requested data should be retrieved at the fastest rate and this is possible only if all of the data is available on high-speed devices at all the time, but this is beyond the ability of most organizations." *Id*. HSM enables data to be moved from a faster storage medium (like cache) to a slower storage medium (such as tape). *Id.* (citing 15:23-44). One of the benefits of Hierarchical Storage is that "performance is improved as unused data is moved to lower level storage devices and frees up higher level (faster) storage devices, thus increasing overall system performance." *Id*. The Patent discloses particular ways of "cascading" storage.

26. One embodiment is illustrated by video data. *Id*. at ¶31 (citing 15:48-61). A video data segment is stored by its importance ("Y"), which may be calculated as weighted attributes of the data (including attributes of the camera). *Id.* (citing 15:62-66). Such attributes include resolution of the data ("R"); reliability of the source (such as whether derived from a "video tip", "RS"); age of camera ("A"); location of camera ("L"); time since video was last accessed ("TS"); time of collection ("TM") and whether the data includes a "primitive event," along with attributes of the data. *Id.* (citing 15:66-16:17). A "primitive event" is an "atomic, indivisible event[s] from any subsystem," such as people entering a designated area, a package left behind in an

area, a gunshot detected, a count of the number of cleaning people entering a building at a certain time, locks on gates not engaged, and so on. *Id.* (citing 7:62-8:13).

27. The importance of the video data segment may be calculated as a weighted average, as shown in the equation (a_i is the attribute of the data and w_i is the relative weight):

$$Y = \sum_{i=1}^{i=N} w_i a_i$$

Id. (citing 16:25-29).

28. For example, in a case of six attributes to a particular video data segment, each weighted equally, the importance is calculated as "Y=(L+R+A+RS+TM+TS)/6." (16:45-49). Depending on the value of Y, the video data may be stored in the highest or other lower storage hierarchy. *Id.* at ¶32 (citing 16:61-17:18; 19:11-18). When a given hierarchical level becomes nearly full, the video segments of lowest importance are automatically cascaded to free space to accommodate new data. *Id.* A hierarchical storage manager (HSM) 401 manages the storage of the video data segments and their corresponding locations. *Id.* (citing 17:55-59). The stored events may be later queried and retrieved from the appropriate hierarchy and migrated to a faster location for processing. *Id.*

29. The HSM system is complex and implements the following functions and sub-systems or a sub-set thereof, as described in detail in the patent: (a) storage hierarchy including on-site and off-site (network or cloud based) storage of various speeds and cost; (b) HSM Migration: data migration policy between different levels

codified by preset mathematical rules or operator override; (c) HSM Archiving: archival of data to slower or remote storage based on importance or frequency of use; (d) HSM Rules Engine: automated control or change of data storage location based on predefined policy rules being triggered; and (e) HSM Audit Trails: storage of an audit record including information about each data access event to enhance data privacy. *Id.* at ¶33. In summary, the HSM provides a detailed formal design and framework of operation to handle the large amounts of data produced by security and surveillance systems. *Id.*

IV. The Asserted Patents are Inventive Concepts Under *Alice*

30. The Asserted Patents are in the same family of patents. SecureNet, the applicant, filed a patent application that issued as U.S. Patent No. 9,934,616 (the "'616 Patent") after June 2014 when the U.S. Supreme Court decided *Alice Corp. Party Ltd. v. CLS Bank, Int'l*, 573 U.S. 208, 216 (2014) ("*Alice*"). The '616 Patent issued on May 17, 2016.

31. In *Alice*, the Supreme Court outlined three narrow exceptions to patent eligibility ("laws of nature, natural phenomena and abstract ideas") and established a test for determining patent eligibility. *Id.* Under *Alice*, 'inventive concepts' sufficient to 'transform' the claimed abstract idea are eligible for patentability. *Id.* Whether a patent contains an 'inventive concept' entails consideration of the elements of each claim "both individually and as an ordered combination to determine whether they involve more than the performance of well-understood, routine, and conventional activities" to those skilled in the art at the relevant time. *Id.*

32. During prosecution of the '616 Patent in a November 4, 2015 interview, the applicant discussed with the Patent Examiner whether this patent would be eligible as a "inventive concept" under the test set forth in *Alice* and under 35 U.S.C. §101.

33. The applicant also addressed *Alice* during the prosecution of each of U.S. Patent Nos. 10,862,744 and 11,323,314, confirming the patentability to the issued claims under 35 U.S.C. §101.

34. The prosecution histories for the Asserted Patents are useful to show that certain limitations—either alone or in combination—constitute "inventive concepts" over the then-existing prior art. Specifically, in Step 2 of the *Alice* assessment of the Asserted Patents, the Applicant identified the following ideas as "inventive concepts," *either as alone or in combination*:

> evaluating one more historical correlations by automatically analyzing said stored sensory events, ***across at least one of time and space*****,** for one or more historical correlations stored among the sensory events; monitoring continuously and in-real time the primitive sensory events from one or more sensors based on the one or more historical correlations to identify one or more critical events . . . sending one or more alerts based on at least one of said critical events and said network failures events," which is an unconventional improvement of the state of the art at the time the applicant by filed as evidence by the prior art cited in the IDS.

'616 Prosecution History (emphasis in original).

35. During the prosecution of the applications that issued as the Asserted Patents, the applicant confirmed the patentability of the inventions under each of Sections 101, 102, 103, and 112 of Title 35.

36. Attached hereto as **Exhibit B** is the declaration of Richard C. Helfers, Ph. D. ("Helfers Dec.") Dr. Helfers is a professor of criminal justice with decades of experience in policing and security-related work.

37. Dr. Helfers explains that the Asserted Patents are not directed at the kinds of duties that security guards perform. Rather, the patents aree directed at problems that exist within the realm of computers-problems that security guards have never been tasked with performing. Helfers Dec. at ¶8. He furthers that, the Asserted Patents account for disparate qualities of data obtained from different sensors, by weighting the "attribute data" of the sensors. *Id.* at ¶9. Security guards, on the other hand, do not typically interact with "attribute data of the sensors," or use attribute data to "weight" primitive events as required by the '744 Patent. *Id.* These issues exist within the realm of computerized security systems. *Id.* at ¶10.

38. He further explains that, "[w]hile it is true that security guards utilize computerized security systems and information from security systems, they have not done so in the manner described and claimed in the patents." *Id.* "For example, security guards typically have no information on the attribute data of a given sensor. A security guard typically has no information on when a given sensor was last maintained, for example, which is one type of attribute data described in the patent specification." *Id.* "This type of attribute data is usually stored in databases accessible by IT personnel only, and is not the kind of data that security guards have access to, much less take into account during their day-to-day functions of monitoring security systems." *Id.* "Similarly, security guards typically have no access to other technical

attribute data of sensors, such as a reliability of a bandwidth or power going to a given sensor, which again is a type of attribute data described and claimed in the patents, which only IT personnel typically have access to, not security guards." *Id.*

39. Dr. Helfers also clarifies that "security guards could not reasonably take into account attribute data such as sensor age, reliability, and power level for each sensor in a complex security system that contains hundreds, or even thousands of different sensors of different types in multiple locations (e.g., cameras, motion detectors, noise detectors, card swipes, door openings, smoke alarms, photobeam alarms, and much more), with different methods of communication and types of networking to the control center (e.g., radio frequency, microwave, optical cable)." *Id.*

40. He states further that, the Asserted Patents are directed at solving "correlating data obtained from different types of sensors located in different geographical locations." *Id.* at ¶11. "Although security guards certainly do observe video monitors that display scenes from video cameras in different locations, they do not perform the type of 'correlation' at which the patents are directed." *Id.* "Rather, the correlation described in the patents can only be performed by computers capable of processing digital data, such as the 'attribute data' of sensors that is used in correlating the events." *Id.* "For example, claims of the '744 Patent discuss generating new rules based on the correlated primitive events and the actions taken, so that future events can be more accurately correlated, with the appropriate actions being undertaken automatically." *Id.*

41. Dr. Helfers concludes that the type of correlation disclosed by the patents exists solely within the realm of computerized security systems whereas security guards simply observe their surroundings and video monitors in order to respond to threats; they do not "correlate" events "weighted by attribute data," and do not "generate" new "rules" that are followed automatically. *Id.*

42. Dr. Helfers illustrates that, for example, "security guards are stationed at different physical locations on a sprawling university or corporate campus, change shifts, and are laid off or fired. There is no proper sense in which any security guard can—or in practice does—correlate data across disparate geographical locations or points in time—as claimed in the patents." *Id.* at ¶12. He explains, that his "understanding of the invention is that it provides a novel way of correlating across space and time what has heretofore not been possible nor performed by any security guards." *Id.*

43. Dr. Helfers further explains that, "[y]et another problem that the patents are directed at solving is comparing data originating from different types of sensors and security systems, which may use disparate protocols, each with its own proprietary data format. The patents address this problem by 'normalizing' this data so that it can be effectively compared. Security guards do not perform this function. Security guards are generally not familiar with, much less involved in, accounting for discrepancies among various digital protocols and data formats used by sensors and security systems, which is what the 'normalization' limitation of the Asserted Patents address." *Id.* at ¶13.

44. For example, "security guards are used to using a disparate array of 'siloed' computerized security systems that do not 'talk' to each other. This leaves the security guards with a disorganized array of incompatible and confusing data. The disparate computerized security systems historically available to security guards may often cause more confusion, and obfuscate the real threat, rather than illuminate it. In contrast, the claimed invention utilizes a computerized correlation engine that takes data from multiple sources that have been normalized by a normalization engine, which transforms the data from various unrelated security systems into a coherent picture for the security guards to then take action on. This is not something that was available to security guards previously." *Id.*

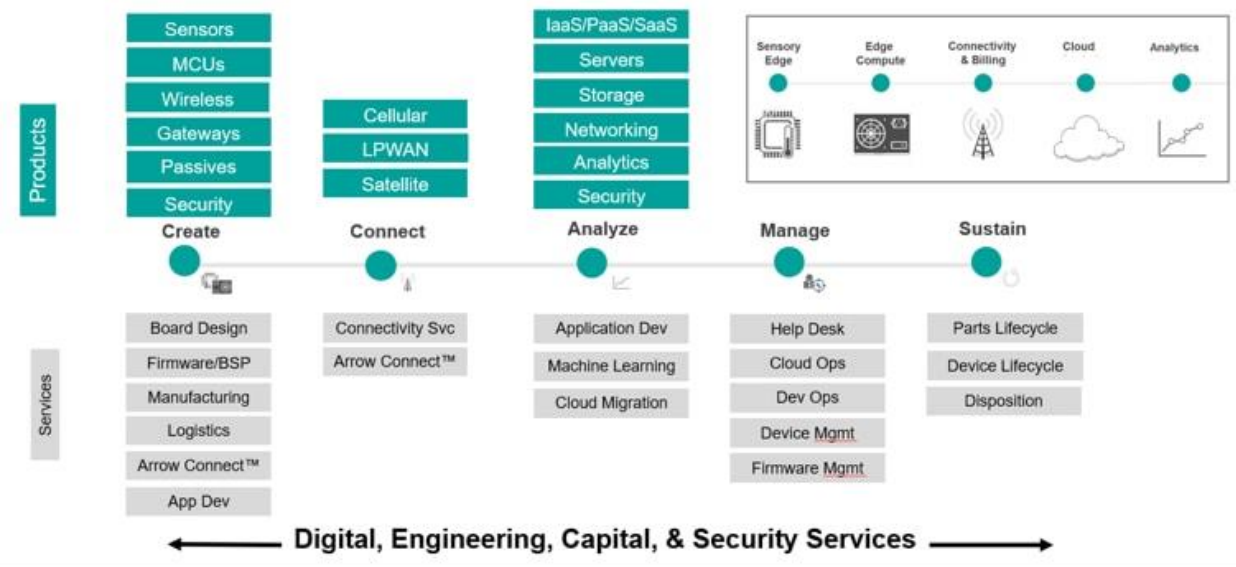
45. Dr. Helfers summarizes that an "individual could not perform the patents' functions mentally or with pen and paper. The patents describe problems and solutions existing within the realm of computerized security systems; it would not be possible to reduce the patents' claimed functionality to paper or to mental processes. It is not part of the job of a security guard, much less routine, to perform the kinds of complex and computerized correlations of normalized sensory data as described and claimed in these patents." *Id.* at ¶14.

V. Arrow's Product Offerings

46. Defendant Arrow offers sensors, servers, cloud storage, analytics, and services to enable its customers to deploy systems and methods that practice SecureNet's claimed inventions. For example, Arrow explains that the industrial internet-of-things ("IIoT"), "enables a new generation of data-driven decision making

to get the most out of [a company's] high value assets." *See* https://www.arrow.com/en/family/arrow-iot-industrial.

47. Through IIoT, an organization can "optimize operations, increase effectiveness of equipment, improve quality, improve worker safety and develop new products faster." *Id.* "IIoT enables you to converge data from silos across your environment, get brand new data about how your assets are operating via sensors and cameras, and use this data to create a centralized and insightful view of your operations." *Id.* Arrow boasts that it helps companies implement IIoT projects by integrated offerings of hardware, software, and service suppliers. *See id.*



Id.

48. Each of the Accused Instrumentalities incorporates Arrows' products and services as detailed herein.

VI. The Asserted Claims

COUNT 1

Infringement of U.S. Patent No. 9,344,616

49. Plaintiff realleges and incorporates by reference the foregoing paragraphs, as if fully set forth herein.

50. SecureNet is the owner by assignment of United States Patent No. 9,344,616 (the "'616 Patent"), entitled "Correlation engine for security, safety, and business productivity." On May 17, 2016 the United States Patent & Trademark Office duly and legally issued the '616 Patent to SecureNet as the owner and inventor. A true and correct copy of the '616 Patent is included as **Exhibit 1**.

51. Defendant has offered for sale, sold and/or imported in the United States the Accused Instrumentality that directly or indirectly infringes the '616 Patent since the issuance of the '616 Patent.

52. Defendant has directly and indirectly infringed and continues to infringe the '616 Patent by making, selling, offering for sale, and/or importing the Accused Instrumentality through its own use and testing of the Accused Instrumentality in the United States and here in Colorado. In addition, on information and belief, Defendant uses the Accused Instrumentality while providing technical support and repair services of the Accused Instrumentality to Defendant's customers.

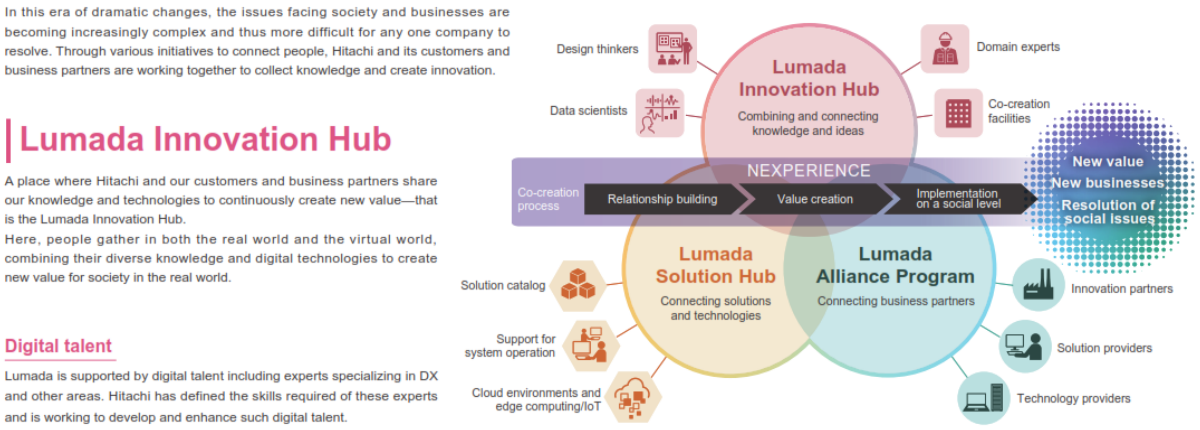
53. One non-limiting example of the Accused Instrumentality's infringement of Claim 46 of the '616 Patent is outlined below. The Accused Hitachi-

Arrow Instrumentality includes systems that use the Lumada platform and Hitachi Visualization Video Analytics and other Hitachi products, consisting of end-to-end, integrated solutions designed for monitoring and analyzing people, assets, and property each of which directly or indirectly infringe the '616, either literally and/or under the doctrine of equivalents.

54. Moreover, Arrow offers the Arrow Transcend Program for Hitachi Vantara Partners ("Trancend"). Transcend offers a wide array of tools and resources to help partners develop their Hitachi business. Arrow provides Partner Onboarding & Readiness; Certification, Marketing Support, and Financial Assistance.

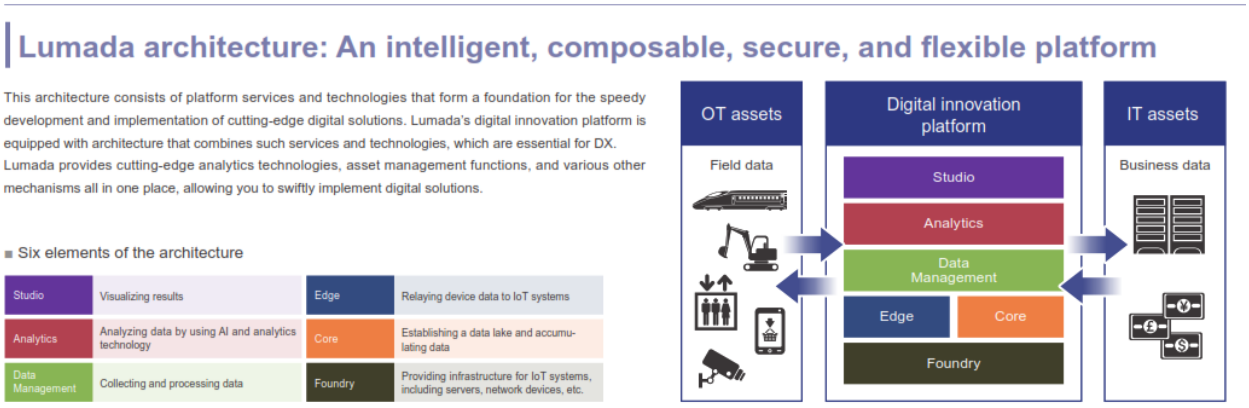
55. The preamble of Claim 46 of the "616 Patent discloses: "A non-transitory, physical storage medium storing computer-readable program code, the program code executable by a hardware processor, the program code when executed by the hardware processor causing the hardware processor to execute steps comprising:"

56. The Accused Hitachi-Arrow Instrumentality includes Lumada and Hitachi Video Analytics stored on a non-transitory, physical storage medium, executable by hardware processor and is provided to consumers via partnership with Arrow, as noted in the Lumada Innovation Hub.



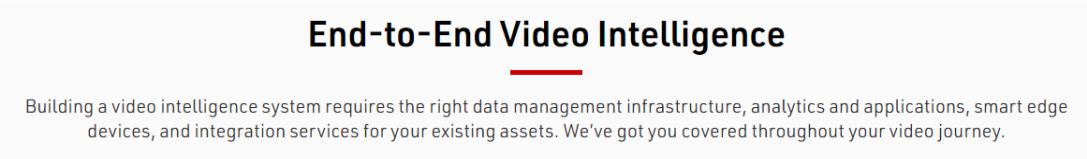
See The Lumada catalog, available at https://www.hitachi.com/products/it/lumada/global/en/download/data/lumada_catalog.pdf.

57. The Lumada architecture includes operational technology ("OT") assets such as sensors, edge servers, and analytics, and IT assets, which include storage.



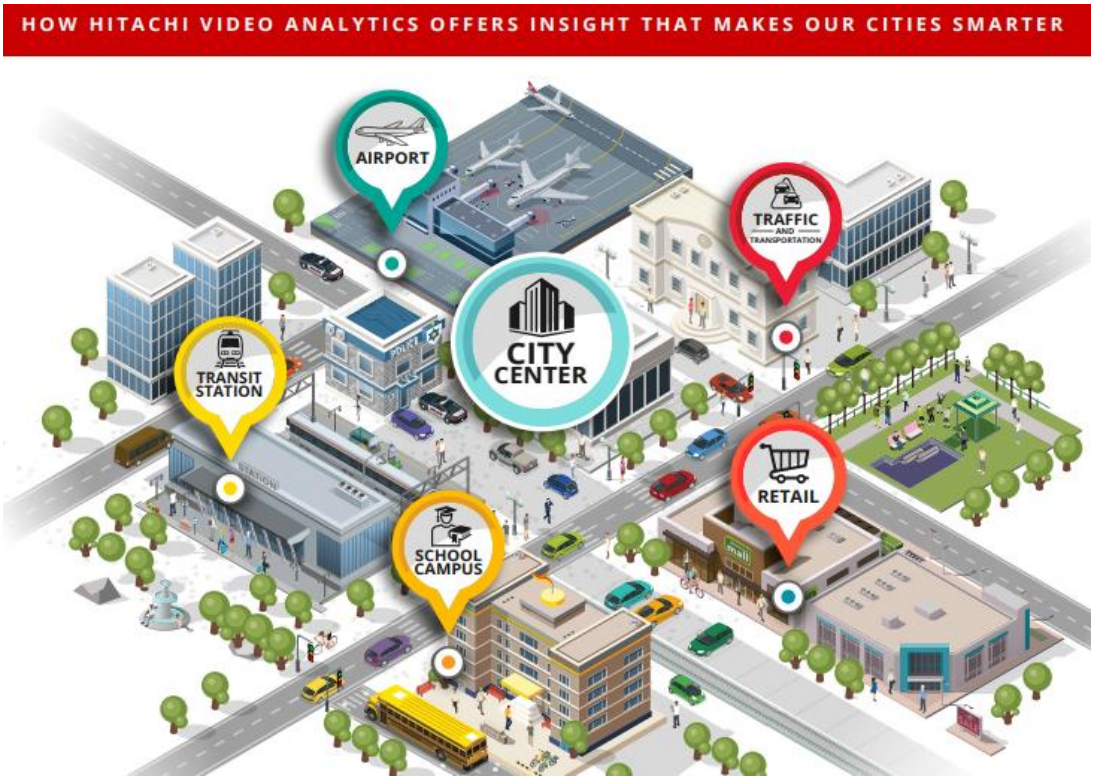
Id.

58. The Hitachi platform and systems provide end-to-end video intelligence which permits video sensors to capture video data for event analysis and provision of actionable triggers.



See https://www.hitachivantara.com/en-us/products/video-intelligence.html.

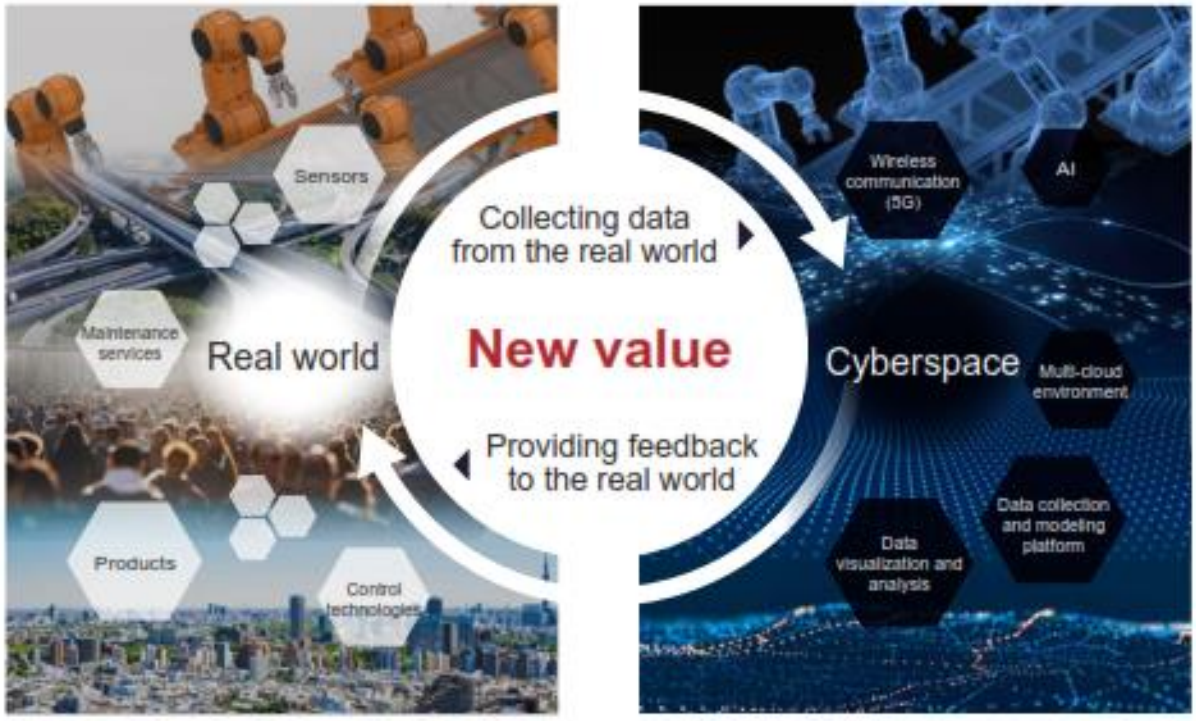
59. Hitachi Video Analytics provides an integrated solution that provides video monitoring and real-time data analysis through data aggregation.



See https://www.hitachivantara.com/en-us/pdfd/infographic/video-analytics-infographic.pdf; https://www.hitachivantara.com/en-us/products/video-intelligence/lumada-video-insights/video-analytics.htm; and https://www.hitachivantara.com/en-us/pdf/brochure/video-analytics-overview.pdf.

60. Claim 46 further recites that a hardware processor is capable of "receiving sensory data about a physical environment from one or more sensors." Cl.

46. The Lumada platform is capable of receiving sensory data about a physical environment from one or more sensors.



See The Lumada catalog, available at https://www.hitachi.com/products/it/lumada/global/en/download/data/lumada_catalog.pdf.

61. Lumada's website explains how this technology works and why its valuable:

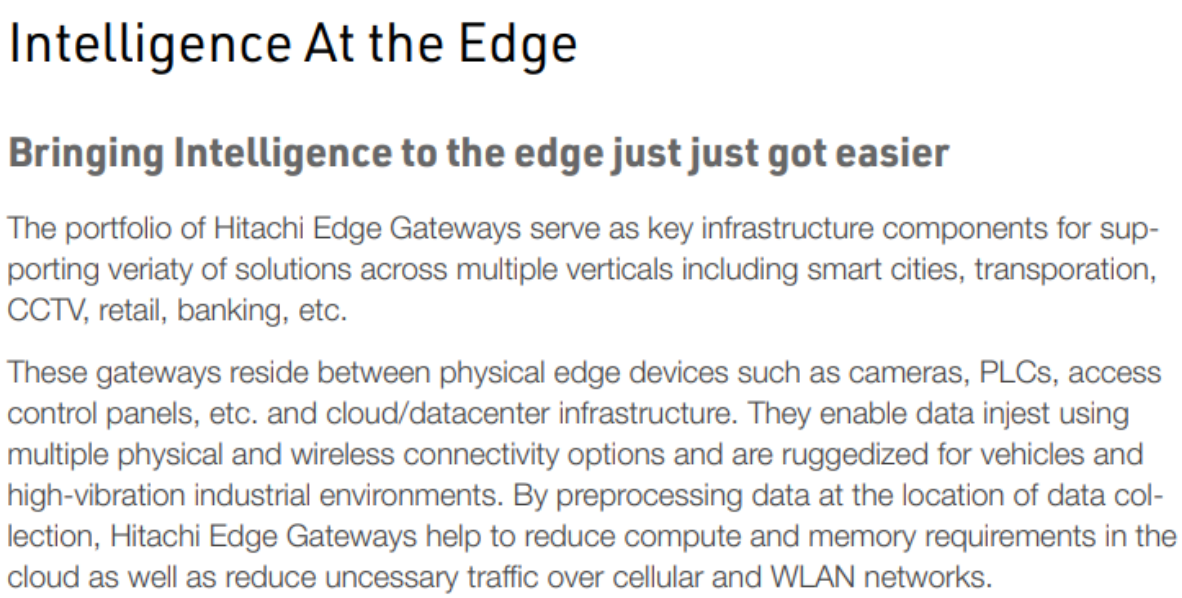
> To create a better society through DX, the concept of cyber-physical systems that use IoT is important. **In such a system, data obtained from the real world (physical spaces) is visualized and analyzed by AI or other technology running in a cloud in cyberspace**. Based on the analysis, solutions to issues are fed back to the real world.
>
> Through the use of digital twins (technology that simulates the real world in cyberspace), we can now find ways to address changes in the real world with greater speed and a broader perspective than in the past. By feeding this back to the real world, business sites are reborn as places

> where new value is continuously created even in the midst of great change.
>
> Lumada's digital innovation platform achieves continuous innovation by accelerating this value creation chain.

See The Lumada catalog, available at

https://www.hitachi.com/products/it/lumada/global/en/download/data/lumada_catalog.pdf (emphasis added).

62. Hitachi's Edge Gateway system collects data from multiple sensors. On its website, it claims:



Intelligence At the Edge

Bringing Intelligence to the edge just just got easier

The portfolio of Hitachi Edge Gateways serve as key infrastructure components for supporting veriaty of solutions across multiple verticals including smart cities, transporation, CCTV, retail, banking, etc.

These gateways reside between physical edge devices such as cameras, PLCs, access control panels, etc. and cloud/datacenter infrastructure. They enable data injest using multiple physical and wireless connectivity options and are ruggedized for vehicles and high-vibration industrial environments. By preprocessing data at the location of data collection, Hitachi Edge Gateways help to reduce compute and memory requirements in the cloud as well as reduce uncessary traffic over cellular and WLAN networks.

Completely Customizable to Support Any Requirement

- Advanced CPU/GPU options support intensive workloads including video analytics and machine vision or machine learning (ML) applications.
- Multiple PoE+ ports serve as an integrated switch for lidar and camera connections, while serial, DIO and CAN bus ports support operational technology integrations.
- WiFi or cellular communications allow wireless connectivity options to and from the gate-ways. All units are PTCRB certified and have gone through rigorous carrier certification testing.
- Multiple storage options including mPCIe, M.2, SSD, and HDD drives allow large data capture capabilities at the edge.
- Multiple operating system options

See https://www.hitachivantara.com/en-us/pdfd/datasheet/empower-your-iot-edge-with-connected-intelligence-datasheet.pdf.

63. Claim 46 further recites that a hardware processor is capable of "receiving IP data of the one or more sensors, wherein the IP data comprises at least an Internet Protocol (IP) address and a network status of at least one of the sensors." Cl. 46. The Accused Hitachi-Arrow Instrumentality also receives IP data of the one or more sensors, wherein the IP data comprises at least an Internet Protocol (IP) address and a network status of at least one of the sensors.

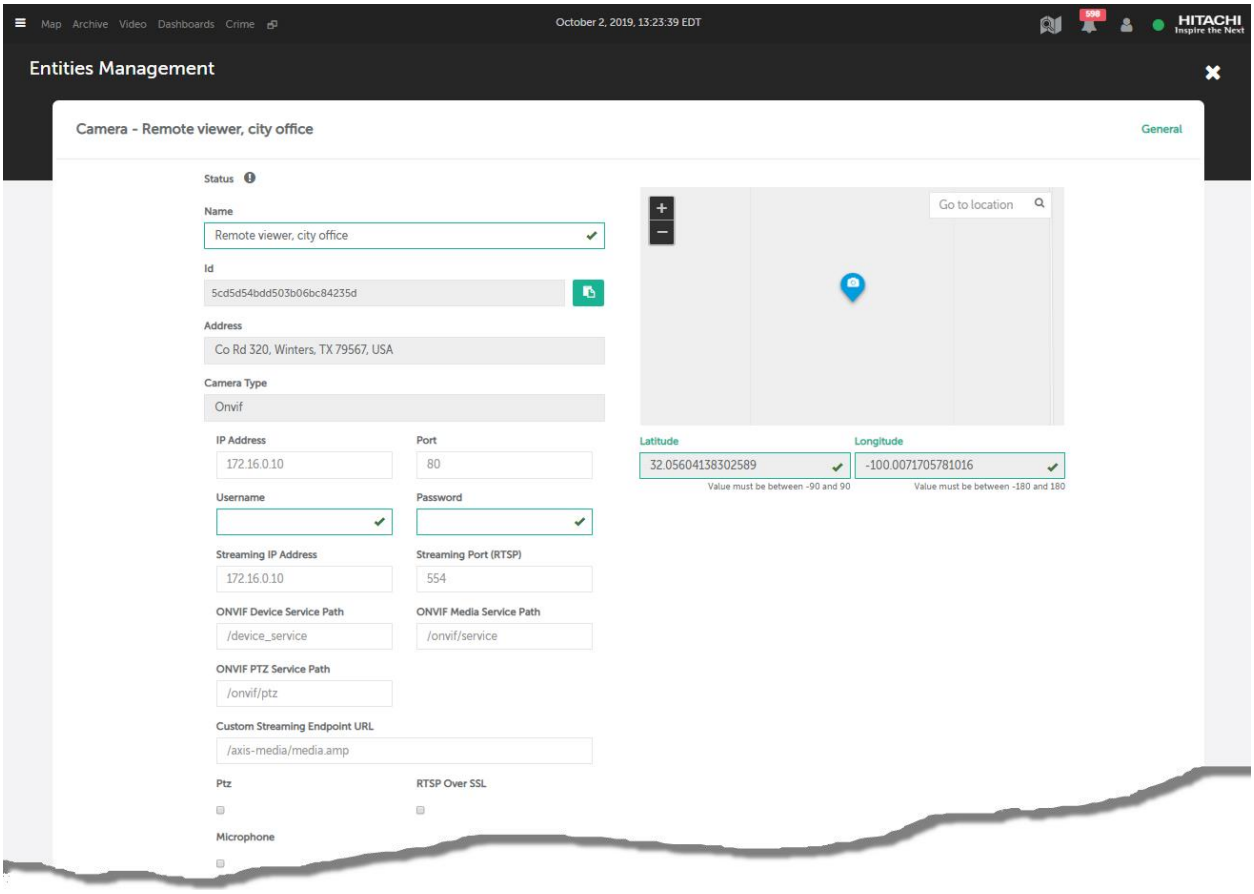
64. The Hitachi Video Intelligence System, including as part of Lumada, can be configured to receive the IP data of a sensor and its network status. For example, the HVS Management Interface for Smart Cameras includes the IP address and network status of a sensor. Hitachi claims:

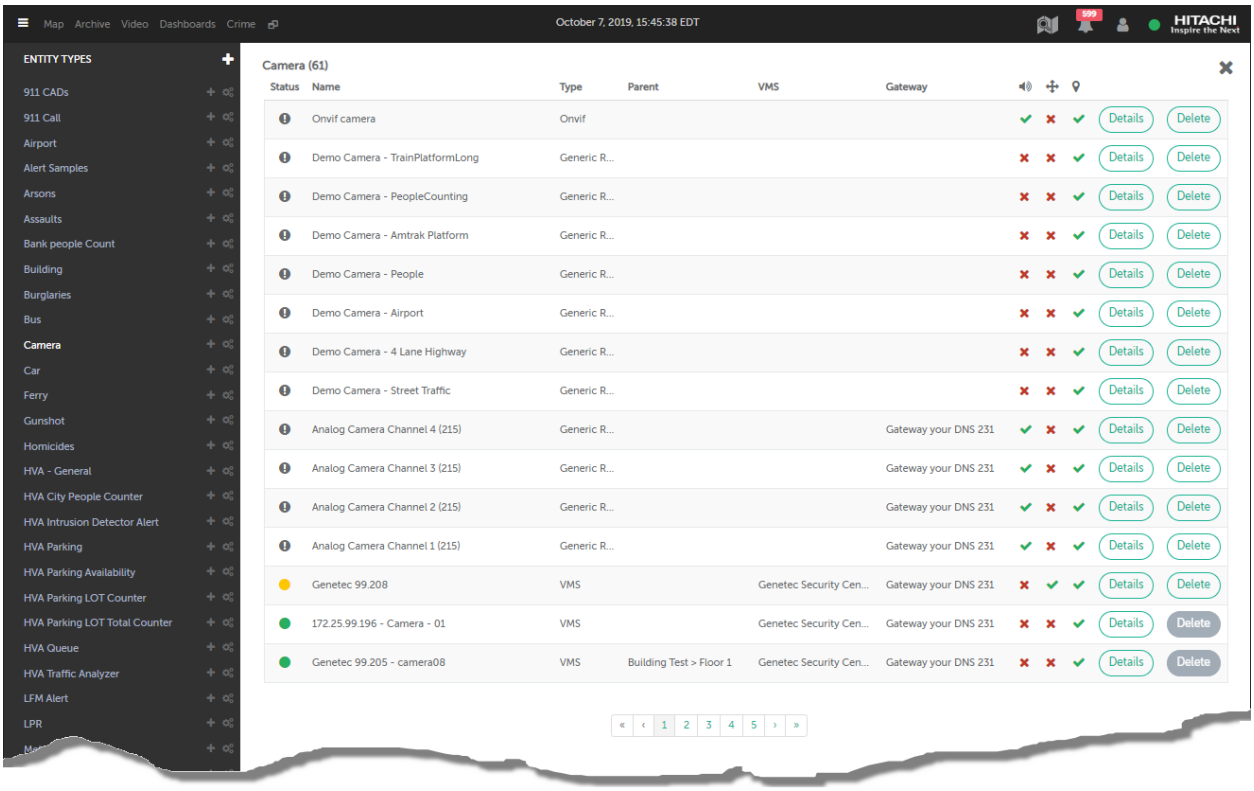
> All of the edge devices can be managed centrally using Hitachi Visualization Suite (HVS) software (see Figure 2). With HVS, an administrator can view bandwidth usage, cellular signal, monitor temperature, power input and draw, and reboot ports on the embedded

switch. In addition, all of the edge router configurations can be viewed and modified from a single management interface.

See https://www.hitachivantara.com/en-us/pdfd/datasheet/smart-edge-devices-for-video-datasheet.pdf (identify streaming IP address).

https://knowledge.hitachivantara.com/Documents/IoT/Smart_Spaces_and_Video_Intelligence/Visualization_Suite/6.2.0/Administration_Guide/Administering_Cameras (showing online status of camera).



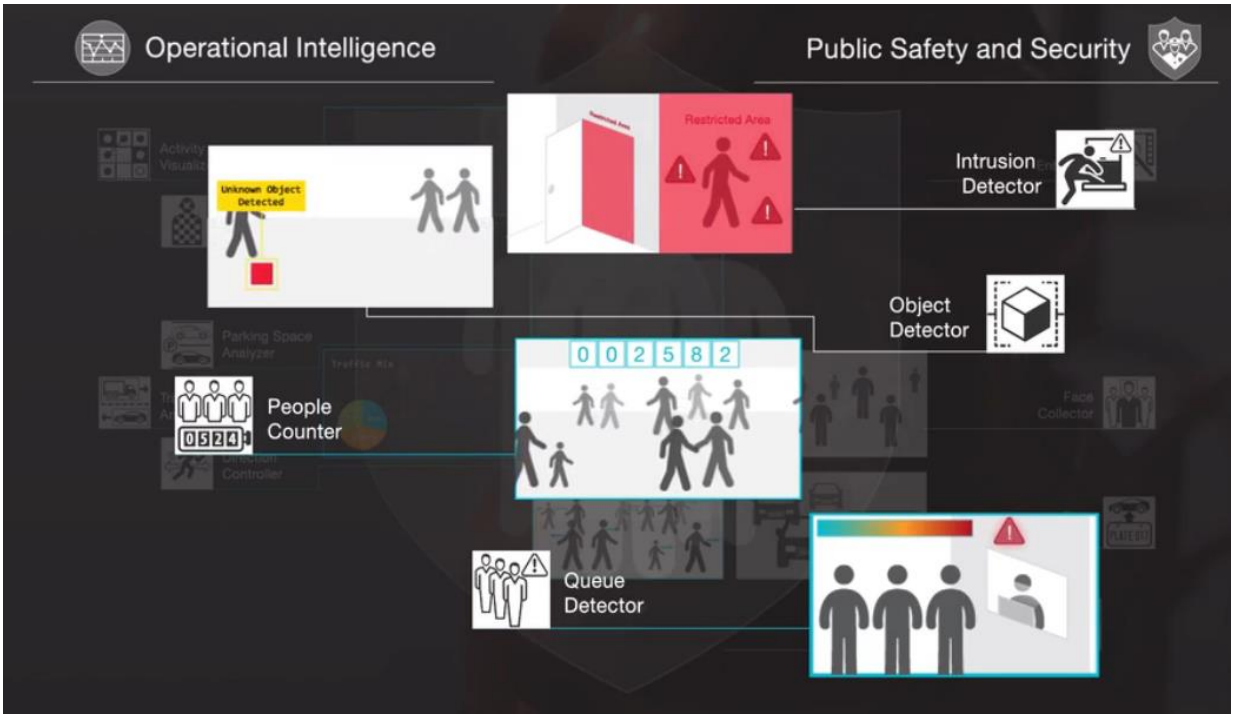


See id; see also, Hitachi Cameral Health Monitor which can inform user if the signal for camera is down.

See Hitachi Video Analytics Overview available at https://www.hitachivantara.com/en-us/products/video-intelligence/lumada-video-insights/video-analytics.html.

65. Claim 46 further recites "processing the sensory data from the one or more sensors to detect one or more primitive sensory events." Cl. 46. The Accused Hitachi-Arrow Instrumentality is capable of processing the sensory data from the one or more sensors to detect one or more primitive sensory events. Hitachi Video Analytics can process sensory data from sensors to detect one or more primitive sensory events, such as events identified in Hitachi infographic below. *See* Infographic Hitachi Video Analytics for Insights and Alerts available at https://www.hitachivantara.com/en-us/pdf/infographic/video-analytics-infographic.pdf.

66. The Accused Hitachi-Arrow Instrumentality detects primitive sensory events by, including reducing false positives.

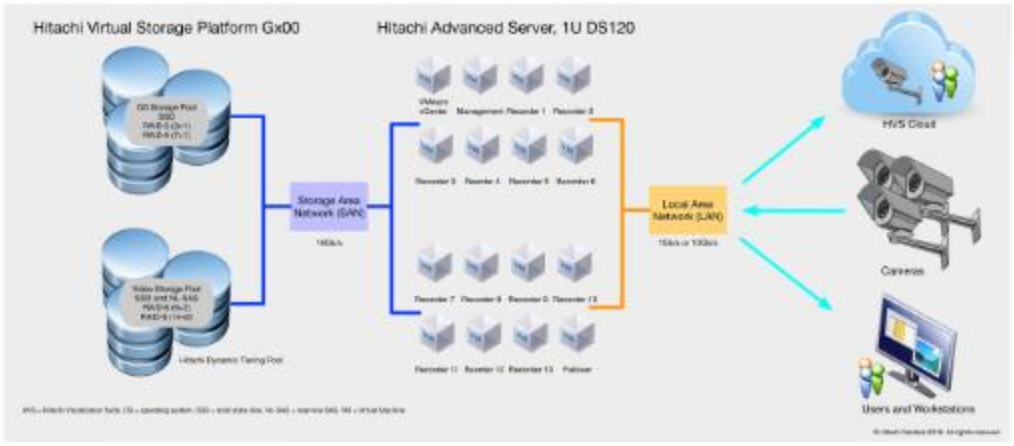


See https://www.hitachivantara.com/en-us/products/video-intelligence/lumada-video-insights/video-analytics.html .

67. Claim 46 further recites "normalizing the primitive sensory events into a standardized data format." Cl. 46. The Accused Hitachi-Arrow Instrumentality is capable of normalizing the primitive sensory events into a standardized data format. For example, the Lumada streaming platform takes data from disparate sources and performs transformations. For illustrative purposes only, in 2018, using the part of the Hitachi Accused Instrumentality, University College London Hospitals NHS Foundation Trust (UCLH) transformed legacy data into the Health Level Seven International (HL7) standard for data interoperability. "We needed to transform our patient data to the HL7 format before we could migrate it to" an electronic health record system. https://www.hitachivantara.com/en-us/company/customer-stories/uclh-case-study.html. Transformations are a type of normalization of data that permits analysis of disparate data types. The Lumada Data Integration manages fast-growing volumes and increased variety of data with a data orchestration tool. https://www.hitachivantara.com/en-us/products/data-management-analytics/lumada-dataops/data-integration-analytics.html.

68. Claim 46 recites "storing the normalized sensory events in an event database for later retrieval." Cl. 46. The Accused Hitachi-Arrow Instrumentality is capable of storing the normalized sensory events in an event database for later retrieval. In particular, Hitachi offers Video Management Platform that includes a Hitachi Virtual Storage Platform. The architecture of the Video Management Storage Platform can be as follows:

Figure 1. Video Management Platform Architecture



https://www.hitachivantara.com/en-us/pdfd/white-paper/video-management-platform-whitepaper.pdf *See also* https://www.hitachivantara.com/en-us/pdf/datasheet/video-management-platform-datasheet.pdf. On information and belief, the Accused Hitachi Instrumentality stores normalized sensory events in an event database, such as in the storage options shown above, for later retrieval. *See infra* additional elements for Claim 46.

69. Claim 46 recites "retrieving one or more historical normalized sensory events from the event database." Cl. 46. On information and belief, the Accused Hitachi Accused Instrumentality retrieves one or more normalized sensory events from the event database. *See infra* additional elements for Claim 46.

70. Claim 46 recites "evaluating one or more historical correlations by automatically analyzing said primitive sensory events, across at least one of time and space, for one or more historical correlations among the historical normalized sensory events." The Accused Hitachi Instrumentality is capable of evaluating one or more

historical correlations by automatically analyzing said primitive sensory events, across at least one of time and space, for one or more historical correlations among the historical normalized sensory events. For example, it:

- Easily ingests multiple datasets with potential correlations to crime e.g., police station locations, roads, street light locations, parole records, license plate captures, gunshot events, social media, etc. ± more data equals greater accuracy
- Keeps data fresh and runs autonomously ± solves the decay problem
- Leverages any number of variables to improve accuracy of the crime prediction i.e., reduce variance
- Offers a robust geospatial display showing probability assigned by crime type for all city blocks for future crime.

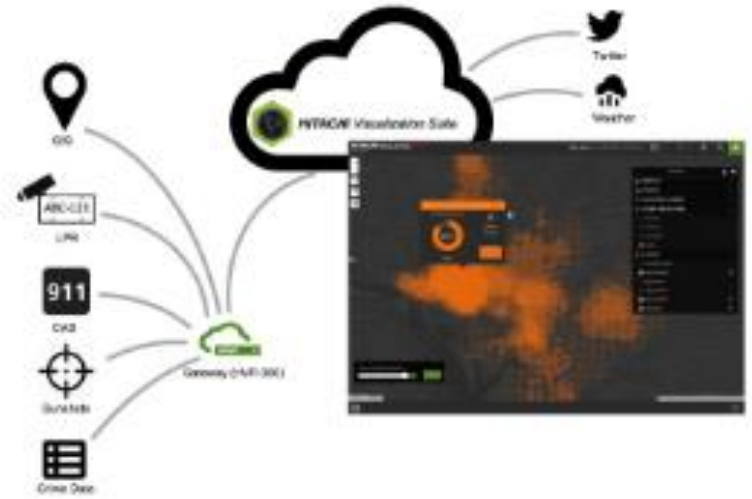
See HV_PCA_VMP Briefing Deck, 9/9/2016.

71. The methodology deployed is as follows:

- Multi-variable spatiotemporal model which uses spatial proximity, density, and temporal periodicity
- Utilizes weather and social media (Tweets) to improve accuracy by as much as 15%
- Provides insights into underlying risk factors e.g., proximity to schools
- Schedule data ingest and prediction runs hourly, daily, weekly
- More powerful than the self-executing point processes that competitors use.

Id.

72. The architecture for deploying the methodology is as follows:



Id.

73. Claim 46 recites "monitoring continuously and in real-time the primitive sensory events from the one or more sensors based on the one or more historical correlations to identify one or more critical events." Cl. 46. The Accused Hitachi Instrumentality is capable of monitoring continuously and in real-time the primitive sensory events from the one or more sensors based on the one or more historical correlations to identify one or more critical events. For example, the Lumada Edge Intelligence permits real-time analytics on streaming data. *See* e.g. Youtube video "What's Your Streaming-Data Strategy?" available at https://youtu.be/VpdH2XhTjKc at time 44:00. One use case is at time 17:46, in which one sensor detects temperature, another detects torque. Based on a previous correlation of these sensor events, which previously resulted in equipment failure, the Accused Hitachi Instrumentality can predict a critical event, such as equipment failure.

74. Claim 46 recites "monitoring continuously and in real-time the network status of one or more of the sensors based on the IP data to identify one or more network failure events." The Accused Hitachi Instrumentality is capable of monitoring continuously and in real-time the network status of one or more of the sensors based on the IP data to identify one or more network failure events. *See supra.*

75. Claim 46 recites "sending one or more alerts based on at least one of said critical events and said network failure events."

76. The Accused Hitachi Instrumentality is capable sending one or more alerts based on at least one of said critical events and said network failure events. For example, the Accused Hitachi Instrumentality in the above example could suggest maintenance to an operator before system failure occurs. *See,* What's Your Streaming-Data Strategy?" available at https://youtu.be/VpdH2XhTjKc at 18:19.

77. Claim 46 recites "generating one or more new rules based on primitive events correlated and alerts generated." The Accused Hitachi Instrumentality uses machine learning algorithms in real time which modifies the rules in real-time. *See generally,* What's Your Streaming-Data Strategy?" available at https://youtu.be/VpdH2XhTjKc.

COUNT 2
Infringement of U.S. Patent No. 10,862,744

78. Plaintiff realleges and incorporates by reference the foregoing paragraphs, as if fully set forth herein.

79. SecureNet is the owner by assignment of United States Patent No. 10,862,744 (the "'744 Patent"), entitled "Correlation system for correlating sensory events and legacy system events." The '744 Patent was duly and legally issued by the United States Patent & Trademark Office on December 8, 2020. A true and correct copy of the '744 Patent is included as **Exhibit 2**.

80. Defendant has offered for sale, sold and/or imported in the United States the Accused Instrumentality that directly or indirectly infringes the '744 Patent since the issuance of the '744 Patent.

81. Defendant has directly and indirectly infringed and continues to infringe the '744 Patent, for example, by making, selling, offering for sale, and/or importing the Accused Instrumentality; and through its own use and testing of the Accused Instrumentality in the United States and here in Colorado. In addition, on information and belief, Defendant uses the Accused Instrumentality while providing technical support and repair services of the Accused Instrumentality to Defendant's customers.

82. One non-limiting example of the Accused Instrumentality's infringement of Claim 1 of the '744 Patent is outlined below. The Accused Gorilla-Intel-Arrow Systems that use the Gorilla Edge AI Video Analytics product including

the Intelligent Video Analytics Recorder ("IVAR") in combination with Intel products such as Intel OpenVINO and Arrow Intelligent Solutions products and systems offered for sale and sold by Arrow Electronics, Inc. consisting of end-to-end, integrated solutions designed for monitoring and analyzing people, assets, and property each of which directly or indirectly infringe the '744 Patent, either literally and/or under the doctrine of equivalents.

83. The preamble of Claim 1 of the '744 Patent discloses: "A monitoring system comprising a non-transitory, physical storage medium storing computer-readable program code. The program code executable by a hardware processor. When the program code is executed by the hardware processor, the program code causes the hardware processor to implement" the elements detailed below. Cl. 1.

84. Arrow offers the Gorilla Edge AI Video Analytics product including the Intelligent Video analytics Recorder (IVAR), in combination with Intel products and hardware and service solutions to intelligently analyze video that monitors individuals and vehicles in retail, industry, security, and healthcare as specified in the product brief and product webpages. The Intel-Gorilla-Arrow Accused Products includes the following:

Solution Stack Components:

Gorilla
– Gorilla IVAR (Intelligent Video Analytics Recorder)
Intel®
– Intel® Core™ i7 processors
– Intel® Movidius™ Vision
– Processing Units (VPUs)
– Movidius™ PCIe Accelerator

Card (optional)
– Intel OpenVINO™
Arrow Intelligent Solutions
– Hardware: Seneca Balto C3 appliance
– Product services: Design, support, or professional services
– Manufacturing services: Supply chain, integration, and logistics

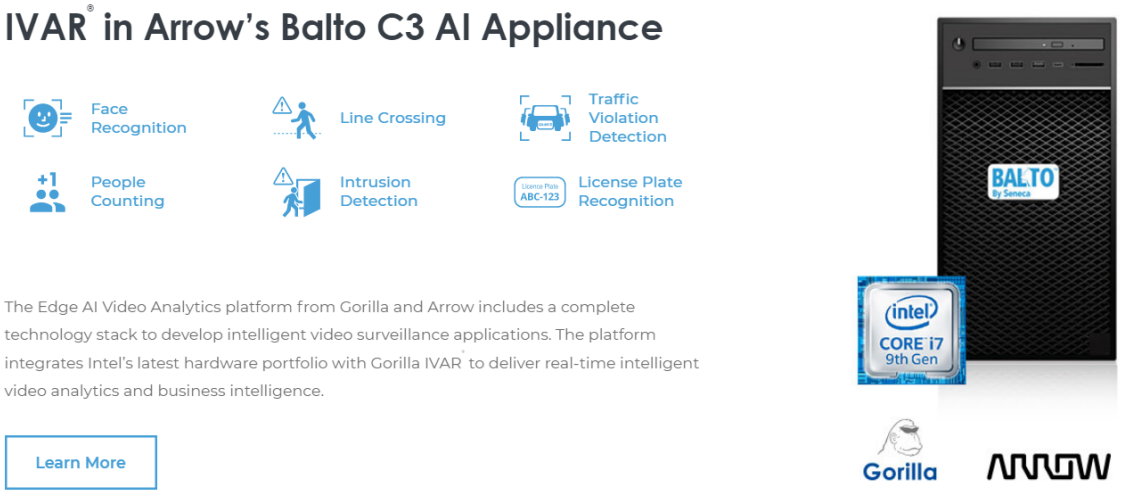
See https://www.arrow.com/ais/intel/wp-content/uploads/sites/6/2022/04/Gorilla-Product-Brief_Nov-02.pdf;

https://www.arrow.com/ais/intel/wp-content/uploads/sites/6/2021/04/Gorilla-Product-Brief_Feb-26.pdf;

https://www.gorilla-technology.com/Products/AI-Appliances/Vision-AI;

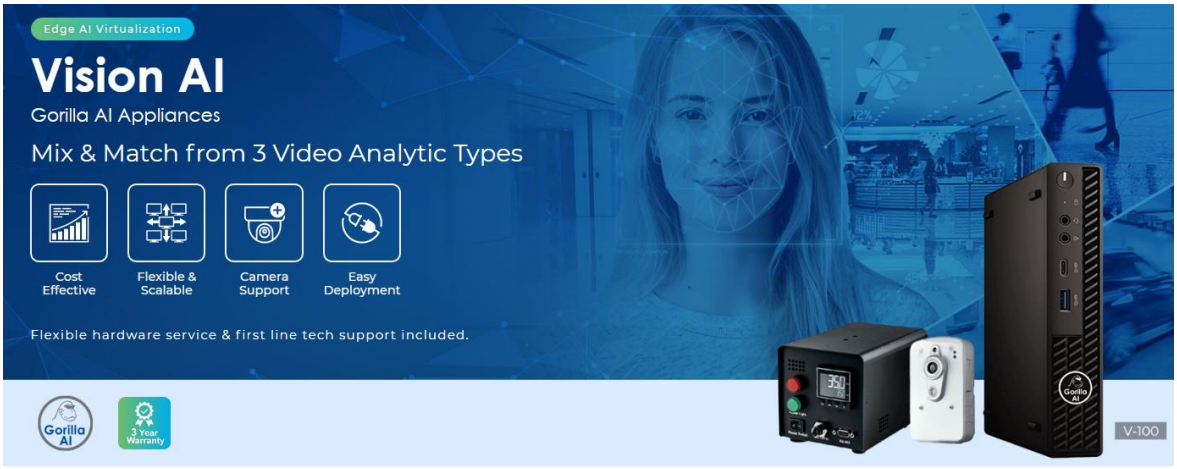
https://www.gorilla-technology.com/Technologies/IVAR.

85. Gorilla Edge AI Video in combination with Intel and Arrow hardware is a non-transitory, physical storage medium storing computer-readable program code, the program executable by hardware processor. Gorilla's AI video platform offers end-to-end monitoring solutions, including the necessary hardware, provided in part by Intel and Arrow's Seneca Balto C3 AI appliance.



86. Claim 1 further recites "a sensory event analytics module to receive sensory data about a physical environment from one or more sensors and to process the sensory data from the one or more sensors to detect one or more sensory events, wherein the one or more sensors comprises at least an Internet Protocol (IP) video camera, and wherein the one or more sensory events is selected from the group consisting of a person detected, a face detected, a vehicle detected, and a license plate detected." Cl. 1.

87. The Accused Gorilla-Intel-Arrow Systems includes a sensory event analytics module to receive sensory data about a physical environment from one or more sensors and to process the sensory data from the one or more sensors comprises at least an Internet Protocol (IP) video camera, and wherein the one or more sensors to detect one or more sensory events is selected from the group consisting of a face detected, a vehicle detected, a license plate detected, a size of an object, and a speed of an object. Arrow's AI Video Analytics, sourced from Gorilla, and in combination with Intel products, is comprised of (inter alia) software capable of receiving sensory data consisting of facial, vehicle, and license plate detection.

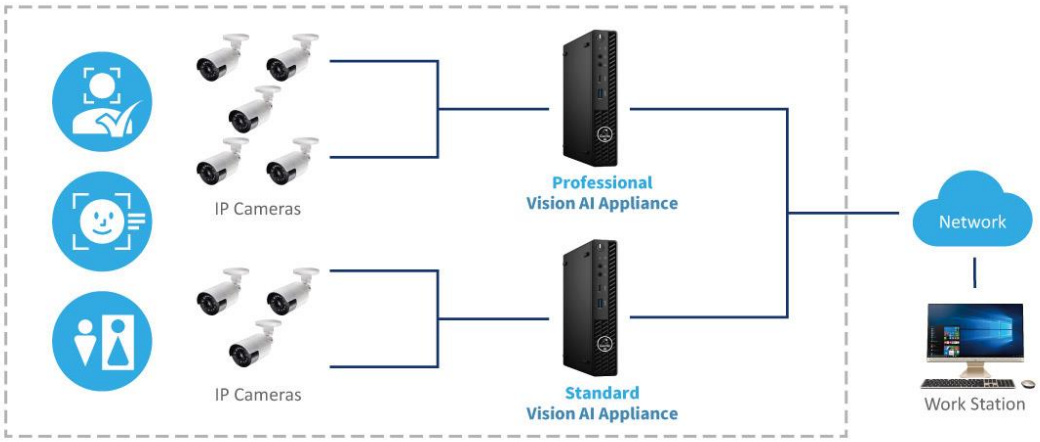


https://www.gorilla-technology.com/Products/AI-Appliances/Vision-AI. *See also,* https://www.arrow.com/ais/intel/wp-content/uploads/sites/6/2021/04/Gorilla-Product-Brief_Feb-26.pdf.

See id.

88. Gorilla's system can be configured to work with IP cameras. It claims, "ONVIF Profile S, is designed for IP-based video systems. An ONVIF Profile S device (e.g., an IP network camera or video encoder) is one that can send video data over an IP network to a Profile S client like IVAR. A Profile S client (e.g., IVAR) is one that

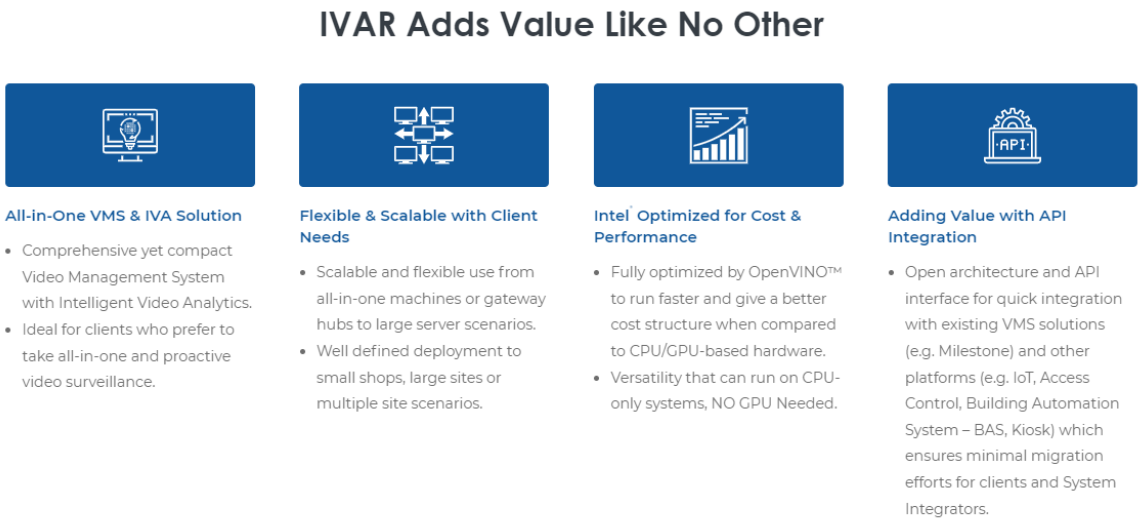
can configure, request, and control video streaming over an IP network from a Profile S device. Profile S also covers ONVIF specifications for PTZ (Pivot Tilt Zoom) control." *See Gorilla White Paper – the Future of Intelligent Video Analytics Recorder* (May 2019).



89. Claim 1 further recites "a legacy event analytics module to receive legacy system data from one or more legacy systems and to process the legacy system data from the one or more legacy systems to detect one or more legacy events, wherein the one or more legacy systems is selected from the group consisting of an access control system, a personnel system, a license plate system, an inventory system, a law enforcement system, and a lighting system." Cl. 1

90. The Accused Gorilla-Intel-Arrow Systems includes a legacy event analytics module to receive legacy system data from one or more legacy systems and to process the legacy system data from the one or more legacy systems to detect one or more legacy events, wherein the one or more legacy systems is selected from the group consisting of an access control system, an inventory system, a financial system,

a law enforcement system, and a lighting system. Gorilla's IVAR allows for legacy system data and analysis. *See* https://www.gorilla-technology.com/Technologies/IVAR. "In addition, IVAR was also developed with full integration capabilities for existing camera/surveillance systems. For example, IVAR has integration capabilities with Video Management Systems (VMS), Network Video Recorders (NVR) and System Access Control. This is particularly integral as the focus on smart video surveillance and asset protection grows in importance and companies seek out advanced video analytics capabilities." *See Gorilla White Paper – the Future of IVAR*.



91. Gorilla can "[s]eamlessly integrate with existing systems, including clock-in machines, tablets or PCs with webcams. Place clock-in/out devices anywhere within a facility and attendance records will be synchronized over the network." https://www.gorilla-technology.com/Technologies/Smart-Attendance.

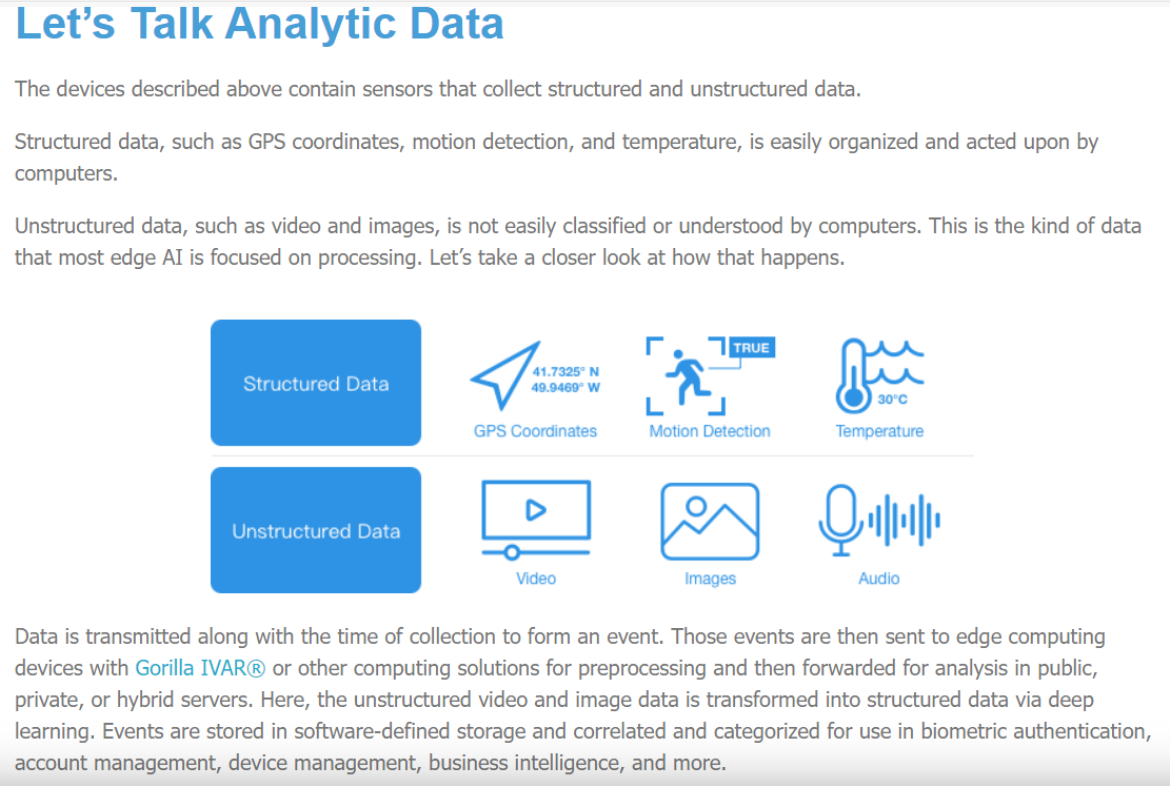
92. The Accused Gorilla-Intel-Arrow System is configured to receive data from one or more legacy systems, such as those used in retail: "Gorilla Smart Retail's metrics dashboard allows management team to make decisions and take action immediately to capture market momentum, and prevent potential losses. Customized widget setting allows store managers to review higher priority, relevant individual store information, and product/behavior correlation analysis to accurately target marketing campaigns. The metrics dashboard live platform can be integrated with external databases, e.g. POS, CRM, to generate in-depth comparison analysis insights across different datasets." *See* https://www.intel.com/content/www/us/en/internet-of-things/ai-in-production/partners/gorilla-technology.html.

93. Gorilla offers the EVMS product which integrates the various Gorillas subsystems and offers server and big data platform. A similar server and big data platform is offered by Arrow to work in conjunction with the Gorilla AI Edge. Gorilla uses an open API to permit integration with legacy systems: "Integrating this solution to create AI appliances and then deploy in the market is easily achieved through the IVAR open API: Retail & Hospitality Machines – Kiosk, POS, ATM, and Signage; Enterprise Machines – Access Control, Attendance Systems, Auto Gates; Public Service Machines – Access Control, Auto Gates. IVAR is flexible to meet camera and hardware standards & protocols for deployment on new or existing systems." *Id.*

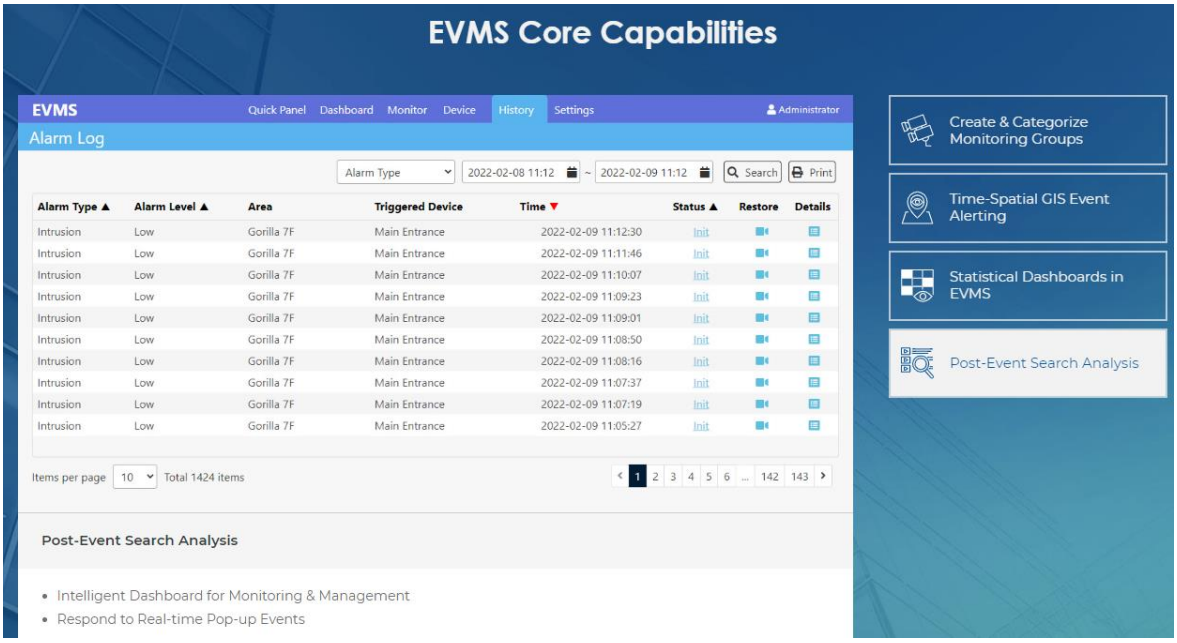
94. Claim 1 further recites "an event queue having access to an event database to store the sensory events and the legacy events for later retrieval as stored sensory events and stored legacy events." Cl. 1

95. The Accused Gorilla-Intel-Arrow System includes an event queue having access to an event database to store the sensory events and the legacy events for later retrieval as stored sensory events and stored legacy events. Gorilla IVAR employs dashboards that permit, for example, a retail environment to capture data from multiple points, stored in separate datasets that include sensory events, from cameras for example, and legacy events. https://www.gorilla-technology.com/Products/AI-SaaS/Smart-Retail.

96. According to its website, "Gorilla Smart Retail's metrics dashboard allows management team to make decisions and take action immediately to capture market momentum, and prevent potential losses. Customized widget setting allows store managers to review higher priority, relevant individual store information, and product/behavior correlation analysis to accurately target marketing campaigns. The metrics dashboard live platform can be integrated with external databases, e.g. POS, CRM, to generate in-depth comparison analysis insights across different datasets." *Id.*



97. Gorilla's EVMS system collects and logs sensory events that can be displayed as lists or retrieved at a later date for post-event analysis. *See* https://www.gorilla-technology.com/Technologies/EVMS#section-value.



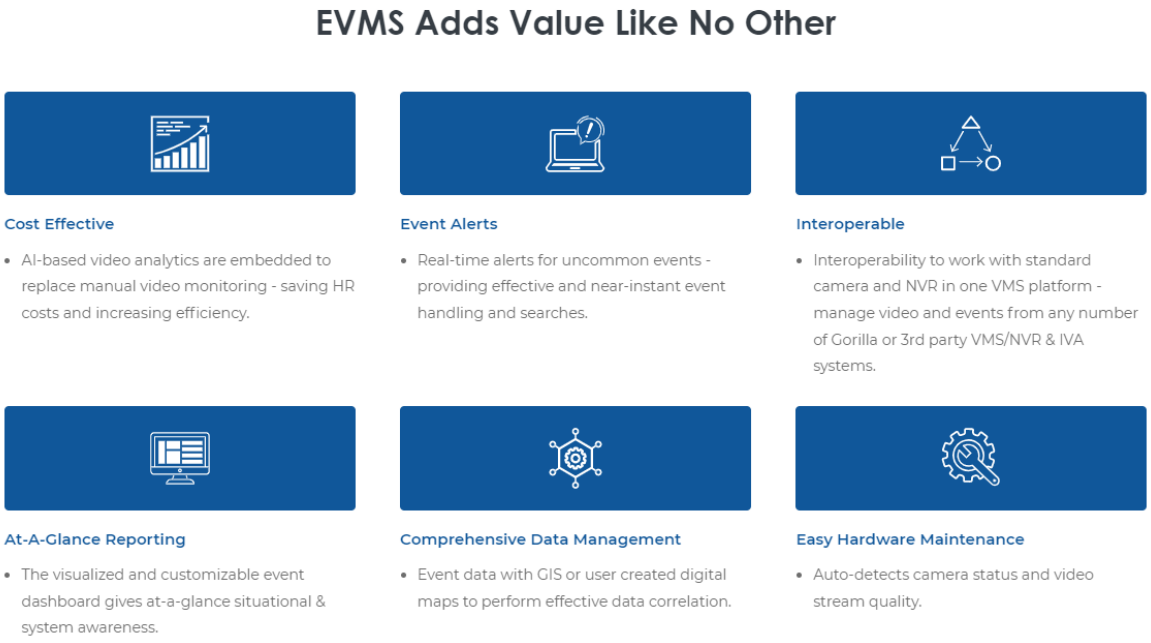
See id.

98. Claim 1 further recites "a correlation module to calculate one or more historical correlations by automatically analyzing the stored sensory events and the stored legacy events across at least one of time and space, wherein the correlation module is adapted to monitor continuously and in real-time the sensory events and the legacy events to identify one or more critical events, and wherein the one or more critical events are based at least on the one or more historical correlations among the stored sensory events and the stored legacy events." *Id.*

99. The Accused Gorilla-Intel-Arrow System includes "a correlation module to evaluate one or more historical correlations by automatically analyzing the stored sensory events and the stored legacy events across at least one of time and space, for one or more historical correlations among the stored sensory events and the stored legacy events, wherein the correlation module is adapted to monitor continuously and

in real-time the sensory events and the legacy events to identify one or more critical events, and wherein the one or more critical events are based at least on the one or more historical correlations among the stored sensory events and the stored legacy events." *Id.*

100. Gorilla IVAR implements a correlation module to evaluate one or more historical correlations by analyzing stored sensory events and legacy event across at least time or space to identify a critical event based on a historical correlation using real-time and continuous monitoring. *See e.g.*, https://www.gorilla-technology.com/Technologies/EVMS. It boasts, "Powered by Gorilla's IVAR technology, EVMS [Gorilla's AI-based operational management and business insight] merges an AI-based video analytics event search & management system with an advanced VMS to create a comprehensive reporting platform. EVMS stores event/object attributes in a temporal-spatial big data database to deliver comprehensive operational management with up-to-the-minute business insights." *Id.*



See also https://www.intel.com/content/www/us/en/internet-of-things/ai-in-production/partners/gorilla-technology.html.

101. The Accused Gorilla-Intel-Arrow System correlates data from multiple sensors to optimize inventory control and promotion strategy, energy use, and connects demographics to public information:

AI Toolkit	Deliverd Solutions	Scenarios and Applications	Machines
Retail and Hospitality	• Customer demographics • Targeted marketing based on gender and age	Correlation analysis of shopper demographic & people counting with sold merchandise optimizes inventory control and promotion strategy.	• Signage • POS • Kiosk • IPC
Enterprise	• Visitor Traffic Statistics • Information Kiosk	Integration of visitor statistics with building automation system effectively controls energy.	• Kiosk
Public Services	• Traveler D emographics • Information Kiosk	Better service delivery based on demographics. Correlation analysis between kiosk inquiries and demographics to improve information data center.	• Signage • Kiosk • IPC

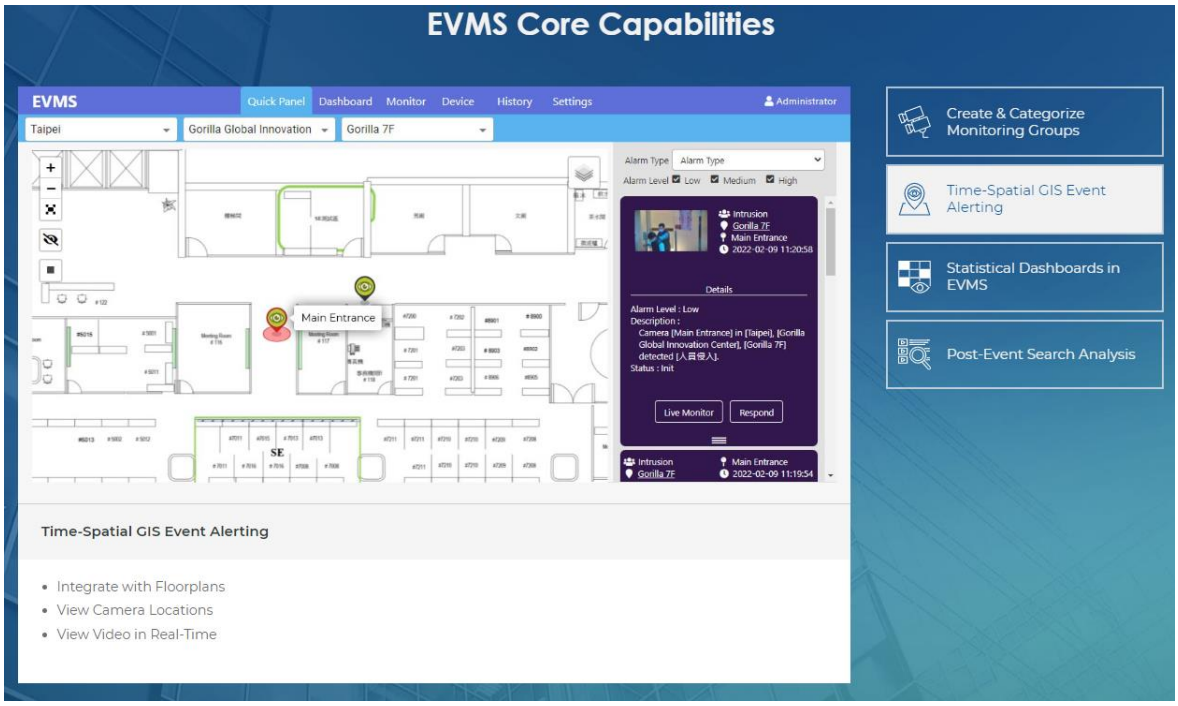
102. Claim 1 further recites "an alerting module to send one or more alerts based on the one or more critical events." Cl. 1.

103. The Accused Gorilla-Intel-Arrow System includes an alerting module to send on or more alerts based on the one or more critical events:

> The Edge AI Video Analytics platform from Arrow and Gorilla includes a complete technology stack to develop intelligent video surveillance applications. The platform integrates Intel's latest hardware portfolio with Gorilla IVAR™ (Intelligent Video Analytics Recorder) to deliver real-time intelligent video analytics and business intelligence. Core video analytics capabilities of the solution include people/face recognition, behavior analysis, vehicle detection/recognition, and realtime insights. Exception alerts based on key business or security parameters make the platform well suited for video surveillance applications in public safety, smart cities, and enterprise security and for enhancing customer experiences in retail. Together these features provide a complete security convergence platform that safeguards both physical and network security.

See https://www.arrow.com/ais/intel/wp-content/uploads/sites/6/2022/04/Gorilla-Product-Brief_Nov-02.pdf.

104. Gorilla EVMS provides capabilities for critical event alerts including "Time-Spatial GIS Event Alerting." Hence, it can perform historical correlations across time and space and send an alert for a critical event.



https://www.gorilla-technology.com/Technologies/EVMS.

COUNT 3

Infringement of U.S. Patent No. 11,323,314

105. Plaintiff realleges and incorporates by reference the foregoing paragraphs, as if fully set forth herein.

106. SecureNet is the owner by assignment of United States Patent No. 11,323,314 (the "'314 Patent"), entitled "Heirarchical data storage and correlation system for correlating and storing sensory events in a security and safety system." The '314 Patent was duly and legally issued by the United States Patent & Trademark Office on May 3, 2022. A true and correct copy of the '987 Patent is included as **Exhibit 3**.

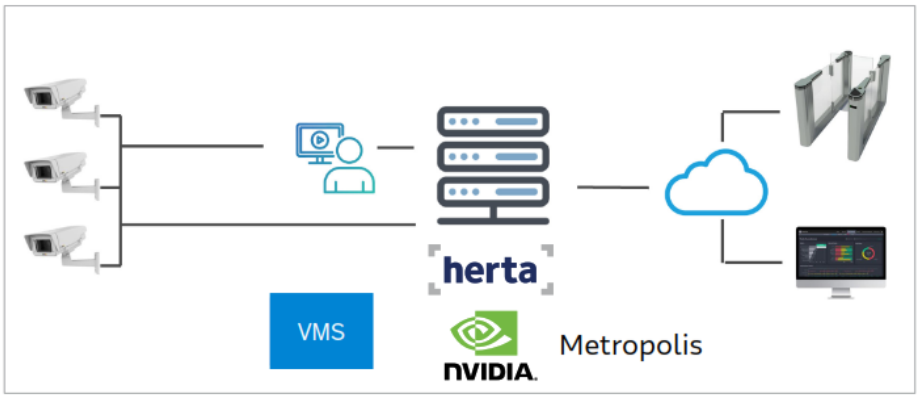
107. Defendant has offered for sale, sold and/or imported in the United States the Accused Instrumentality that directly or indirectly infringes the '314 Patent since the issuance of the '314 Patent.

108. Defendant has directly and indirectly infringed and continues to infringe the '314 Patent, for example, by making, selling, offering for sale, and/or importing the Accused Instrumentality; through its own use and testing of the Accused Instrumentality in the United States and here in Colorado. In addition, one information and belief, Defendant uses the Accused Instrumentality while providing technical support and repair services of the Accused Instrumentality to Defendant's customers.

109. One non-limiting example of the Accused Instrumentality's infringement of Claim 13 of the '314 Patent is outlined below. The Accused Nvida-Herta-Arrow System products and systems offered for sale and sold by Arrow Electronics, Inc. consisting of end-to-end, integrated solutions designed for monitoring and analyzing people, assets, and property each of which directly or indirectly infringe the '314 Patent, either literally and/or under the doctrine of equivalents.

110. Claim 13 of the '314 Patent discloses in the preamble: "A non-transitory, physical storage medium storing computer-readable program code, the program code executable by a hardware processor, the program code when executed by the hardware processor causes the hardware processor to implement." Cl. 13.

111. The NVDIA EGX Hardware, Metropolis Platform, Deepstream SDK, and Herta Security Solutions in combination with Arrow Intelligent Solutions, such as tiers of products designed specifically for analytics applications, embedded, workstation, and rack mount form factors, design support or professional services and supply chain, integration, and logistics include a non-transitory, physical, storage medium storing computer-readable program code, including a video analytics and plug-ins program code executable by a hardware processor. The program code when executed cause the hardware processor to implement the elements disclosed in Claim 1 of the '314 Patent.



Typical Solution Architecture

https://www.arrow.com/ais/wp-content/uploads/2020/12/Herta-Product-Brief_Nov-02-2.pdf.

112. Claim 13 further recites capability to "receive one or more sensory events from a sensory event analytics module that receives sensory data about a physical environment from one or more sensors and processes the sensory data from the one or more sensors to detect the one or more sensory events, wherein the one or

more sensors comprises at least an Internet Protocol (IP) video camera, and wherein the one or more sensory events are selected from the group consisting of a face detected, a vehicle detected, a license plate detected, a size of an object, and a speed of an object." Cl. 13.

113. The Accused Nvidia-Herta-Arrow Accused System can receive one or more sensory events from a sensory event analytics module that receives sensory data about a physical environment from one or more sensors and processes the sensory data from the one or more sensors to detect the one or more sensory events, wherein the one or more sensors comprises at least an Internet Protocol (IP) video camera, and wherein the one or more sensory events are selected from the group consisting of a face detected, a vehicle detected, a license plate detected, a size of an object, and a speed of an object.

114. The Herta Security application and Deepstream SDK are designed to receive one or more sensory events about a physical environment, such as facial detection, and processes the data to recognize one or more faces. https://hertasecurity.com/company-facial-recognition/about-us/. The Herta Security system works with IP cameras: "Herta is specialized in the analysis of crowded environments, making it possible to detect and identify multiple subjects at the same time through IP cameras. Our software is completely scalable and compatible with any IP camera, becoming a user friendly and accessible tool for any business organization." https://hertasecurity.com/company-facial-recognition/about-us/.

115. Claim 13 further recites "a hierarchical storage manager having access to a hierarchy of two or more data storage devices, wherein the two or more data storage devices are adapted to store data from the one or more sensors, wherein the hierarchical storage manager is adapted to manage storage and cascade of data through the hierarchy of two or more data storage devices based at least on the sensory events."

116. The Accused Nvidia-Herta-Arrow System includes a hierarchical storage manager having access to a hierarchy of two or more data storage devices, wherein the two or more data storage devices are adapted to store data from the one or more sensors, wherein the hierarchical storage manager is adapted to manage storage and cascade of data through the hierarchy of two or more data storage devices based at least on the sensory events. The NVIDIA Deepstream SDK allows data stored on edge servers to be transmitted to the cloud for further analytics processing and visualization: "The DeepStream application can run on an edge device powered by NVIDIA Jetson or on-premises servers powered by NVIDIA T4s. The data from the edge can be sent to the cloud for higher-level analytics and visualization." https://developer.nvidia.com/blog/building-iva-apps-using-deepstream-5-0-updated-for-ga.

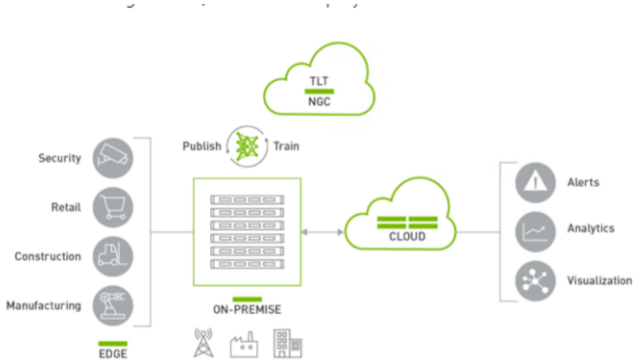


Figure 1. DeepStream – edge-to-cloud.

117. The Deepstream SDK can also provide "Smart video recording." "There is often a need to have event-based video recording. Instead of continuously recording the content, smart recording can save valuable disk space and can provide faster searchability. . . . Smart record only records the event when specific rules or conditions are met. The trigger to signal the record can come locally from the app, from some service running at the edge or from the cloud."

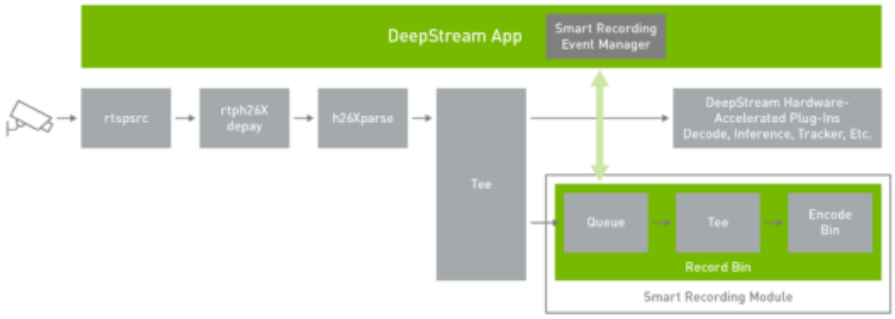


Figure 5. Smart record architecture. https://developer.nvidia.com/blog/building-iva-apps-using-deepstream-5-0-updated-for-ga/.

118. "Rich APIs are provided to build a smart recording event manager. These actions can be used to start and stop the recording at any time. When an event

must be recorded, it's useful to start saving the clip before the trigger. With the smart record API action, you can configure it to record time before the event. This is extremely useful because, by the time the anomaly is detected and triggered, there is some latency between when the anomaly happens and when the recording event manager starts the recording. Recording for some finite amount of time before the record starts to provide the entire sequence of events." *Id.*

119. "To demonstrate this feature, a smart recording event manager is built in to the deepstream-test5 application. The smart recording module keeps a video cache so that the recorded video not only has frames after the event is generated, but it can also have frames just before the event. This size of the video cache can be configured per use case. The event manager initiates the start and stop option to the smart recording module." *Id.*

120. Recording can be triggered by JSON messages received from the cloud. The smart recording demonstrates the recording of video data based on importance, and thus hierarchical storage of recorded data. The message format is as follows:

```
{
 command: string // <start-recording / stop-recording>
 start: string // "2020-05-18T20:02:00.051Z"
 end: string // "2020-05-18T20:02:02.851Z",
 sensor: {
 id: string
 }
 }
```

121. "Receiving and processing such messages from the cloud is demonstrated in the deepstream-test5 sample application. This is currently

supported for Kafka. To activate this functionality, populate and enable the following block in the application configuration file:"

> Configure this group to enable cloud message consumer.
> [message-consumer0]
> enable=1
> proto-lib=/opt/nvidia/deepstream/deepstream-5.0/lib/libnvds_kafka_proto.so
> conn-str=;
> config-file=
> subscribe-topic-list=;;

Id.

122. "Use this option if message has sensor name as id instead of index (0,1,2 etc.)." *Id.*

> sensor-list-file=dstest5_msgconv_sample_config.txt

123. "While the application is running, use a Kafka broker to publish the above JSON messages on topics in the subscribe-topic-list to start and stop recording." *Id.*

124. "For more information about how to use this feature in your application, see the Smart Video Record section of the NVIDIA DeepStream Plugin Manual. The source code for deepstream-test5 can be found in the following directory: $DEEPSTREAM_DIR/sources/apps/sample_apps/deepstream-test5/."

125. "The implementation of the smart record event manager can be found in the following file: $DEEPSTREAM_DIR/sources/apps/apps-common/src/deepstream_source_bin.c." https://developer.nvidia.com/blog/building-iva-apps-using-deepstream-5-0-updated-for-ga/.

126. Claim 13 further discloses "an event queue having access to an event database to store the sensory events for later retrieval as stored sensory events." Cl. 13.

127. The Accused Nvidia-Herta-Arrow System includes an event queue having access to an event database to store the sensory events for later retrieval as stored sensory events as demonstrated in the discussion *supra*. "There is often a need to have event-based video recording. Instead of continuously recording the content, smart recording can save valuable disk space and can provide faster searchability. Smart record only records the event when specific rules or conditions are met. The trigger to signal the record can come locally from the app, from some service running at the edge or from the cloud." https://developer.nvidia.com/blog/building-iva-apps-using-deepstream-5-0-updated-for-ga/.

128. Claim 13 further recites "a correlation module to evaluate one or more historical correlations among the stored sensory events, wherein the correlation module evaluates the stored sensory events for the one or more historical correlations across at least one of time and space, wherein the correlation module is adapted to monitor the received sensory events to identify one or more critical events, and wherein the one or more critical events are based at least on the one or more historical correlations." Cl. 13.

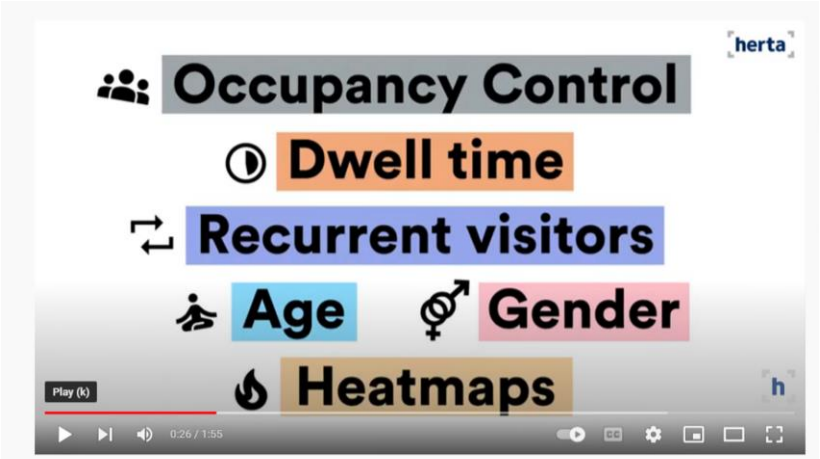
129. The Accused Nvidia-Herta-Arrow System includes a correlation module to evaluate one or more historical correlations among the stored sensory events, wherein the correlation module evaluates the stored sensory events for the one or

more historical correlations across at least one of time and space, wherein the correlation module is adapted to monitor the received sensory events to identify one or more critical events, and wherein the one or more critical events are based at least on the one or more historical correlations. The Herta Security facial recognition BioMarketing software permits evaluation of a recurring customer. *See* https://youtu.be/_puw3JQMV-Q.

130. In particular, a storage sensory event includes facial recognition. *See supra.* To detect a "recurring customer," which is a critical event, a system must correlate historical events over time. The Herta Security system provides "current and accumulated statistics" on customer recurrence, and therefore monitors such events to assess a critical event. *Id.*

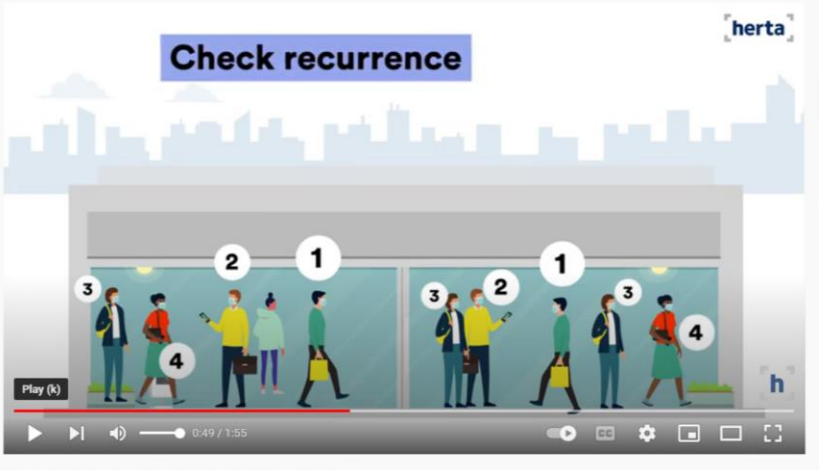
Video Analytics Solution for Retail - BioMarketing

280 views • Oct 18, 2021 3 DISLIKE SHARE DOWNLOAD SAVE ...



Video Analytics Solution for Retail - BioMarketing

280 views • Oct 18, 2021 3 DISLIKE SHARE DOWNLOAD SAVE ...



Video Analytics Solution for Retail - BioMarketing

131. The Accused Nvidia-Herta-Arrow System an alerting module to send one or more alerts based on the one or more critical events, such as for example a recurring customer. On information and belief, the "communication between the sensory event analytics module, the hierarchical storage manager, the correlation module, and the alerting module occurs over an IP network." Cl. 13.

132. Claim 13 further recites "[t]he non-transitory, physical storage medium of claim 1, wherein the sensory events are weighted based at least on one or more attribute data of the one or more sensors used to capture the sensory data." Cl. 13.

133. For example, the NVIDIA system uses the YOLO weights to detect objects in a camera. The weights are further refined using machine algorithms. *See generally*, https://developer.nvidia.com/blog/deploying-a-scalable-object-detection-inference-pipeline/.

Prayer for Relief

WHEREFORE, Plaintiff SecureNet Solutions Group, LLC respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff that Defendant has infringed, either literally and/or under the doctrine of equivalents and either directly or indirectly, U.S. Patent Nos. 9,344,616, 10,862,744 and 11,323,314;

B. A permanent injunction enjoining Defendant from committing further acts that infringe upon the Asserted Patents;

C. A judgment and order requiring Defendant to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for its infringement of the Asserted Patents, as provided under 35 U.S.C. § 284;

D. A judgment and order requiring Defendant to provide an accounting and to pay supplemental damages to Plaintiff, including without limitation, pre-judgment and post-judgment interest;

E. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendant; and

F. A post-verdict accounting; and

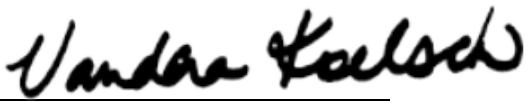
G. Any and all other relief as the Court may deem appropriate and just under the circumstances.

Demand for Jury Trial

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

DATED this 19th day of May 2022.

Respectfully submitted,



s/Vandana S. Koelsh

Vandana S. Koelsch
James S. Helfrich
Jennifer E. Schlatter
Averil K. Andrews
ALLEN VELLONE WOLF HELFRICH & FACTOR P.C.
1600 Stout Street, Suite 1900
Denver, CO 80202
Telephone: (303) 534-4499
vkoelsch@allen-vellone.com
jhelfrich@allen-vellone.com
jschlatter@allen-vellone.com
aandrews@allen-vellone.com
Attorneys for Plaintiff