

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE**

**Portus Singapore Pte LTD, and  
Portus Pty Ltd.,**

*Plaintiffs,*

v.

**Schneider Electric USA, Inc.,  
a Delaware corporation,**

*Defendant.*

CASE NO. \_\_\_\_\_

**Jury Trial Demanded**

**COMPLAINT FOR PATENT INFRINGEMENT**

Plaintiffs Portus Singapore Pte Ltd. and Portus Pty Ltd. (“Plaintiffs”) file this complaint for patent infringement against Defendant Schneider Electric USA, Inc. (“Defendant”) and in support alleges as follows:

**NATURE OF THE ACTION**

1. This is a civil action arising under the Patent Laws of the United States, 35 U.S.C. § 271, *et seq.*

**THE PARTIES**

2. Plaintiff Portus Singapore Pte Ltd. is a company organized under the laws of the Republic of Singapore.

3. Plaintiff Portus Pty Ltd. is a subsidiary of Portus Singapore Pte Ltd., and a company organized under the laws of Australia.

4. Defendant Schneider Electric USA, Inc. (“Schneider”) is a corporation organized and existing under the laws of Delaware that maintains its principal place of business at 800 Federal

Street Andover, MA, USA 01810, and having a registered office at Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808.

### **JURISDICTION AND VENUE**

5. This Court has jurisdiction over the subject matter of this action asserted herein under the Patent Laws of the United States, United States Code, Title 35. This is an action for patent infringement that arises under the patent laws of the United States, 35 U.S.C. § 271, *et seq.*

6. This Court has original subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

7. This Court has personal jurisdiction over Defendant. Defendant has sustained and systematic activities in this District and is committing infringing acts in Delaware and this District. Defendant regularly conducts business in the State of Delaware and within this District, including the sales of the accused products that are the subject of this patent infringement lawsuit.

8. Venue is proper in this District as to Schneider pursuant to 28 U.S.C. § 1400(b). Defendant is a corporation registered in Delaware and thus resides in this District.

9. Infringement is occurring within the State of Delaware and this District through Defendant's distribution and sales of video management systems and IP camera devices (the "Accused Products," which are further defined below).

10. Venue is further proper because Defendant has placed the Accused Products into the stream of commerce knowing or understanding that such products would be used in the United States, including in the District of Delaware. Defendant has manufactured, distributed, sold, and/or offered to sell the Accused Products to customers for use throughout this District.

11. This Court has personal jurisdiction over Defendant at least because Defendant has made, used, offered to sell and sold the accused products within the District, thus committing acts of infringement within the District, and placed infringing products into the stream of commerce

knowing or understanding that such products would be used in the United States, including in the District of Delaware.

### **FACTUAL BACKGROUND**

#### **Plaintiff Portus**

12. Portus is the original creator of the smart home. Portus pioneered the technology for viewing your home when you are away, as well as understanding and managing household energy use, so its users could live in more enjoyable, affordable homes.

13. With Portus' patented technology, users have the freedom to monitor and control their home from anywhere.

14. With Portus' patented technology, Portus enables a home to be safer and more efficient through a connected environment.

15. As well as helping households, Portus facilitated utilities by providing insight into their customers' energy use. The understanding of consumers' energy demands the technology gives is invaluable to a household's or company's planning capacity and carbon constraints.

16. Further, Portus' technology facilitates utilities' demand management by providing insight into their customers' energy use. The understanding of consumers' energy demands the technology gives is invaluable to companies' planning capacity and carbon constraints.

17. Initially founded in Australia, Portus moved to Singapore after winning equity funding through an investment arm of the Singapore government.

18. Portus Singapore Pte Ltd. is the owner by assignment from the inventors, Charles Cameron Lindquist and Timothy John Lindquist, of all right, title, and interest in and to Portus is the owner, by assignment, of the two patents-in-suit: U.S. Patent Nos. 8,914,526 (the '526 Patent) attached as Exhibit A; and 9,961,097 (the '097 Patent) attached as Exhibit B.

19. Portus Pty Ltd. is the exclusive licensee of the '526 and '097 Patents.

20. Tim Lindquist, one of the Portus founders, is one of the inventors of the asserted patents and is recognized as an inventor of the Connected Home. Tim was proclaimed as a pioneer of the Smart Grid by Smart Grid Today.

**The '526 Patent**

21. Portus Singapore Pte Ltd. is the owner by assignment from the inventors, Charles Cameron Lindquist and Timothy John Lindquist, of all right, title, and interest in and to United States Patent Number 8,914,526 (the "'526 Patent"), titled "Local and Remote Monitoring Using a Standard Web Browser" including the right to sue for all past infringement.

22. Portus Pty Ltd. is the exclusive licensee of the '526 Patent.

23. Attached to this Complaint as Exhibit A is a true and correct copy of the '526 Patent.

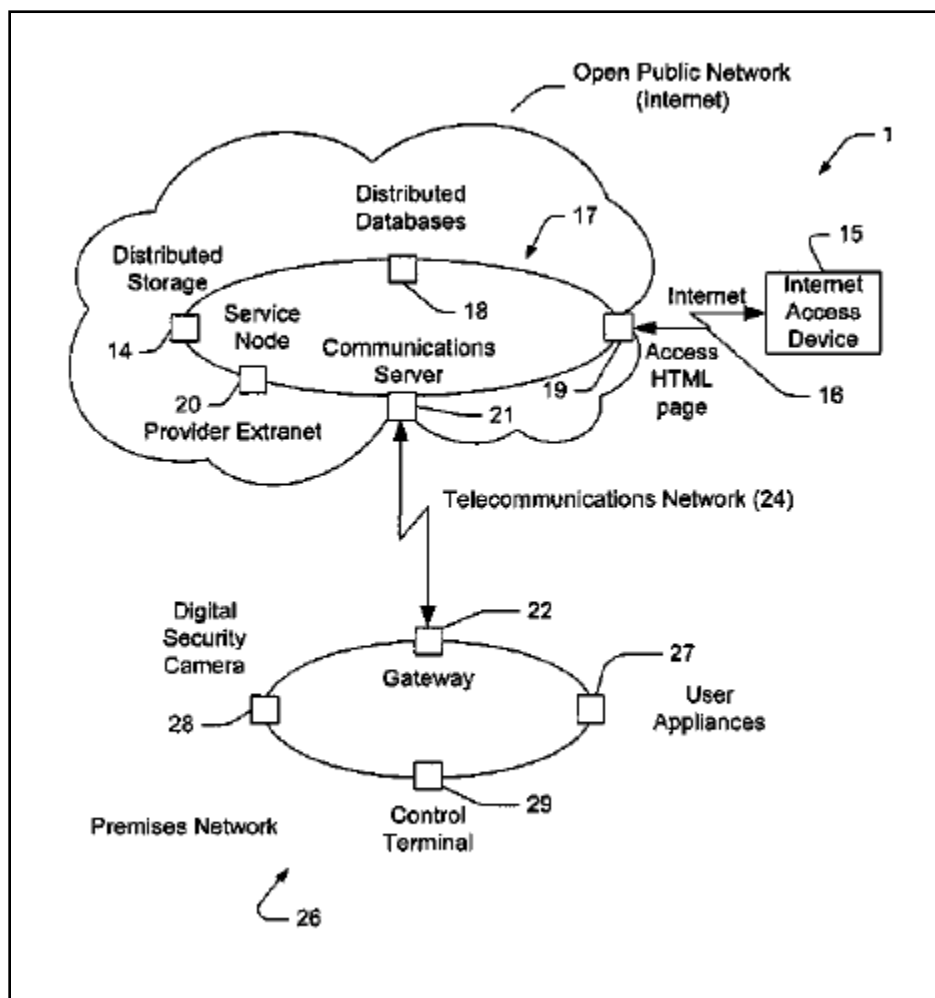
24. The '526 Patent issued from United States Patent and Trademark Office application no. 09/868,417, which was based on a PCT application no. 99/01128, which was filed on December 17, 1999. That PCT application was based on Australian patent application (PP 7764) filed on December 17, 1998.

25. The Patent Office issued the '526 Patent on December 16, 2014, after a full and fair examination.

26. The '526 Patent is valid and enforceable.

27. The '526 Patent abstract describes a home security and control system for monitoring and controlling an external environment such as a home environment comprising: an Internet browser connectable to an external network, which includes but is not limited to an extranet; an external network located external to the home environment and accessible via the Internet browser; a communications server located in the external network and adapted to interconnect on demand with one of a series of connection gateways located in predetermined home environments; and a connection gateway located in the home environment adapted to control and/or monitor the operation

of at least one security device in the home environment; wherein upon accessing a predetermined address by the Internet browser on the external network, the communications server connects to a predetermined one of the connection gateways to control and/or monitor the operation of the security device.



28. The inventors of the '526 Patent recognized that home automation and security systems had become more advanced and that the “[u]sers often have a common need to control and monitor such systems both locally and remotely.” ’526 Patent at 1:35-36. However, despite the growing complexity of these systems, users “generally must resort to non-visual monitoring and control mechanisms for remote operation [such as] by telephone through codes entered via a telephone handset.” *Id.* at 1:38-41.

29. The '526 Patent provides several advantages over the prior art such as: a) allowing remote control of a home security system through operation of a website rather than through the cumbersome automated systems and choices provided via telephone; b) providing a geographically independent standard interface for remote connection to a home security system that is universally accessible and not platform or hardware dependent.

30. A person of ordinary skill in the art at the time of the invention would have recognized that the steps (and combination of steps) claimed in the '526 Patent were, at the time of invention, unconventional and describe remote monitoring of home security and automation systems in a way that, at the time of the invention, was not routine.

31. A person of ordinary skill in the art at the time of the invention would have understood that, at the time of the invention, there was no conventional manner in which to use a web browser remotely to monitor and control home automation and security systems. A skilled artisan, at the time of the invention, would have recognized the problem that such remote monitoring at the time of the invention could only be accomplished via cumbersome telephone-based input and automation systems.

32. The '526 Patent provides technical solutions to this problem not solved in the prior art. The inventions disclosed in the '526 Patent achieves that “when a customer connects to their home, their home effectively appears to them as a website, with all devices, security and otherwise, accessible for monitoring and control.” '526 Patent at 2:49-52.

33. A person skilled in the art at the time of the invention would have understood that the system of using an Internet browser; an external network external to the user premises and accessible via the Internet browser; a plurality of connection gateways that are part of the home network; and a communications server located in the external network and adapted to communicate on-demand with

the connection gateways was not, at the time of the invention, conventional, well-understood, nor routine.

34. A person of ordinary skill in the art at the time of the invention would have understood that the system described in claim 57 of the '526 Patent was not, at the time of the invention, conventional, well-understood, or routine.

35. A person skilled in the art at the time of the invention would have understood that the claims recite steps and structural limitations operating in an unconventional manner to achieve an improved operation of home security and automation.

36. These technological improvements provide greater cost savings and efficiencies in allowing remote monitoring of a home security and automation systems through a web browser.

37. The novel use and arrangement of the specific system recited in the '526 claims were not well-understood, routine, nor conventional to a person skilled in the relevant field at the time of the inventions.

### **The '097 Patent**

38. Portus Singapore Pte Ltd. is the owner by assignment from the inventors, Charles Cameron Lindquist and Timothy John Lindquist, of all right, title, and interest in and to United States Patent Number 9,961,097 (the "'097 Patent"), titled "System for Remote Access of a User Premises" including the right to sue for all past infringement.

39. Portus Pty Ltd. is the exclusive licensee of the '097 Patent.

40. Exhibit B is a true and correct copy of the '097 Patent.

41. The '097 Patent issued from application no. 14/536,784 filed on November 10, 2014.

42. The Patent Office issued the '097 Patent on May 1, 2018, after a full and fair examination.

43. The '097 Patent is valid and enforceable.

44. The '097 Patent provides several advantages over the prior art such as: a) allowing remote control of a home security system through operation of a website rather than through the cumbersome automated systems and choices provided via telephone; b) providing a geographically independent standard interface for remote connection to a home security system that is universally accessible and not platform or hardware dependent.

45. A person of ordinary skill in the art at the time of the invention would have recognized that the steps (and combination of steps) claimed in the '097 Patent were, at the time of invention, unconventional and describe remote monitoring of a home security and automation systems in a way that, at the time of the invention, was not routine.

46. A person of ordinary skill in the art at the time of the invention would have understood that, at the time of the invention, there was no conventional manner in which to use a web browser remotely to monitor and control home automation and security systems. A skilled artisan, at the time of the invention, would have recognized the problem that such remote monitoring at the time of the invention could only be accomplished via cumbersome telephone-based input and automation systems.

47. The '097 Patent provides technical solutions to this problem not solved in the prior art. By using a web browser so that “when a customer connects to their home, their home effectively appears to them as a website, with all devices, security and otherwise, accessible for monitoring and control.” '097 Patent at 2:64-67.

48. A person skilled in the art at the time of the invention would have understood that the system of using an Internet browser; an external network external to the user premises and accessible via the Internet browser; a plurality of connection gateways that are part of the home network; and a communications server located in the external network and adapted to communicate on-demand with



the connection gateways was not, at the time of the invention, conventional, well-understood, nor routine.

49. A person of ordinary skill in the art at the time of the invention would have understood that the system described in claim 1 of the '097 Patent was not, at the time of the invention, conventional, well-understood, or routine.

50. A person skilled in the art at the time of the invention would have understood that the claims recite steps and structural limitations operating in an unconventional manner to achieve an improved operation of home security and automation.

51. These technological improvements provide greater cost savings and efficiencies in allowing remote monitoring of a home security and automation systems through a web browser.

52. The novel use and arrangement of the specific system recited in the '097 claims were not well-understood, routine, nor conventional to a person skilled in the relevant field at the time of the inventions.

### **Defendant**

53. On information and belief, Schneider owned a subsidiary named Pelco and offered products, such as MultiSight, indicating both Schneider and Pelco as the product provider and/or product brand. See <https://web.archive.org/web/20180314230235/http://www.multisight.com/the-multisight-difference.html>.

54. In 2002, Portus had dealings with a company called Clipsal. Clipsal is a major player in the switch/automation and energy monitoring markets, which are related to Portus' technology. Schneider acquired Clipsal in or around 2003. Schneider sold the Wiser energy monitoring product line under the Clipsal brand before recently rebranding Wiser under the Schneider name.

55. Individuals from Schneider, including Benoit Toulouse from Schneider Electric Ventures, contacted Portus in 2006 to explore strategic investment. Following this meeting, additional discussions continued into 2007.

56. In 2007, Portus met with Schneider, including with Dieter Hadrian, to discuss Portus and its technology.

57. Portus contacted Schneider again in 2008. Portus sent Schneider an investment proposal identifying Portus' Intellectual Property, including patent ownership, via email. Portus discussed this investment proposal with Schneider via telephone in 2008.

58. In 2011, Schneider was again sent a different investment profile presentation, which again outlined Portus patented technology. Communications between Portus and Schneider occurred in January, May, and August 2011.

59. In 2015, Portus, through a broker, alerted Schneider of its infringement of Portus' patents asserted in this lawsuit. Schneider was sent a set of linked claim charts and, on information and belief, received claim charts outlining infringement of the Schneider MultiSight product and other similar products.

60. Schneider has been on notice of infringement of the '526 patent since at least 2015.

#### **Defendant's Infringing Products**

61. Defendant provides camera solutions with a series of smart cameras, and together sold products such as the Multisight platform, VideoXpert video management platform, and other IP camera platforms, which embody some of the Accused Products.

62. Schneider also sells accused products such as real time energy monitoring products such as the Wiser and Wiser Air products. Schneider also sells a brand of EVlink Charging Stations, which include modems and remote monitoring functionality. Each of these are Accused Products that

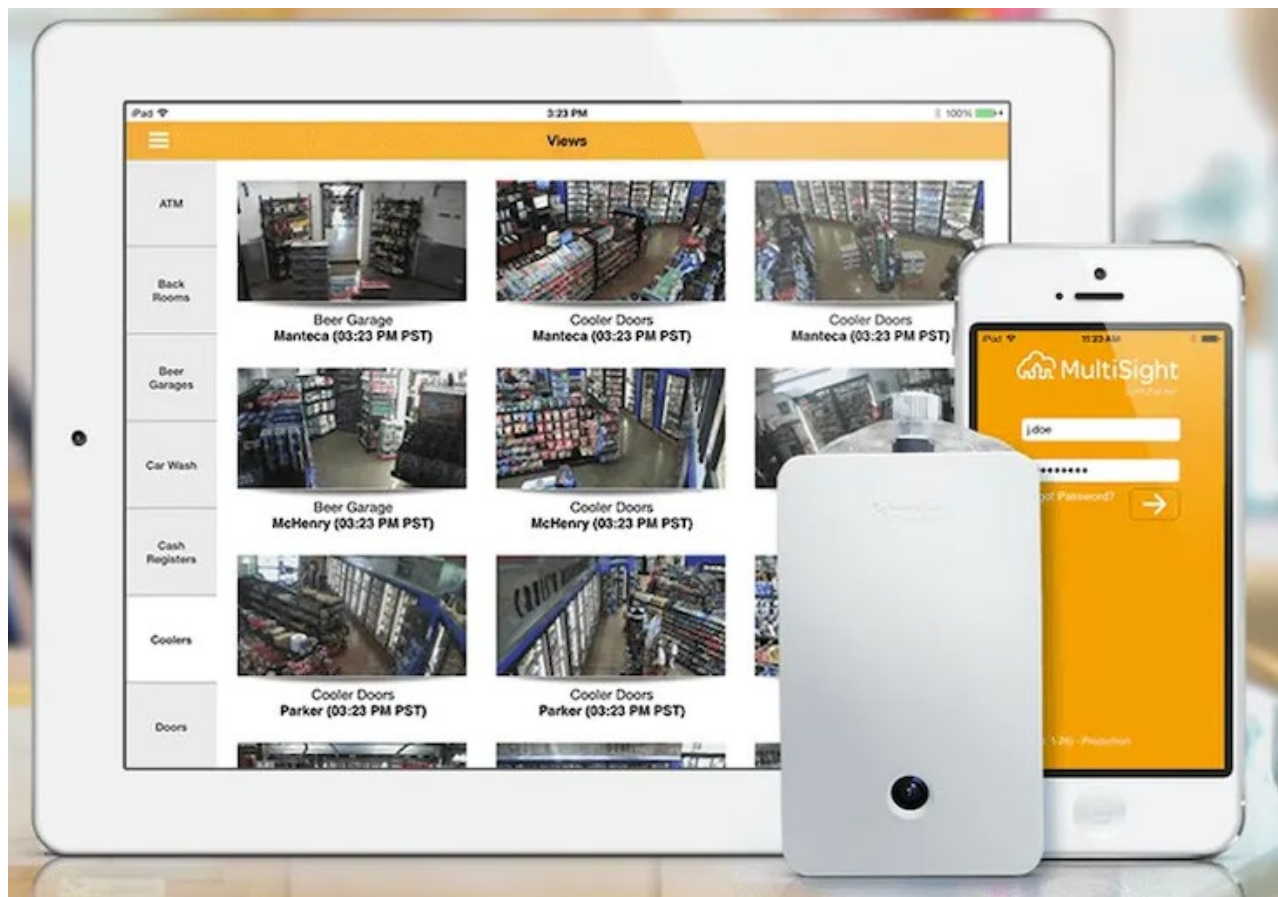
allow for external monitoring and control of devices in accordance with the claims of the Asserted Patents.

63. The sale of the Wisier Air products constitutes the sale of a complete system, including a hardware user access device and connection gateways networked together.



64. The Accused Products are sold in combination with various other devices and include various models and series numbers—each of those variations is an Accused Product. The Accused Products also include functionality whereby the Defendant is able to access and process the personal data of its users—users are required to agree to provide this information for the benefit of the Defendant in order to use the Accused Products.

65. By means of further illustration, the MultiSight Product is shown and described below:



<https://www.securityinfowatch.com/video-surveillance/product/12061104/pelco-by-schneider-electric-pelcos-multisight-video-service>

**MultiSight is a Video Surveillance as a Service (VSaaS) solution that leverages the power of video to deliver operational efficiency to retailers, restaurants, convenience stores, and other multi-location businesses.**

MultiSight® 2017 Schneider Electric | Pelco | Privacy Policy | Press

<https://web.archive.org/web/20180314230235/http://www.multisight.com/the-multisight-difference.html>

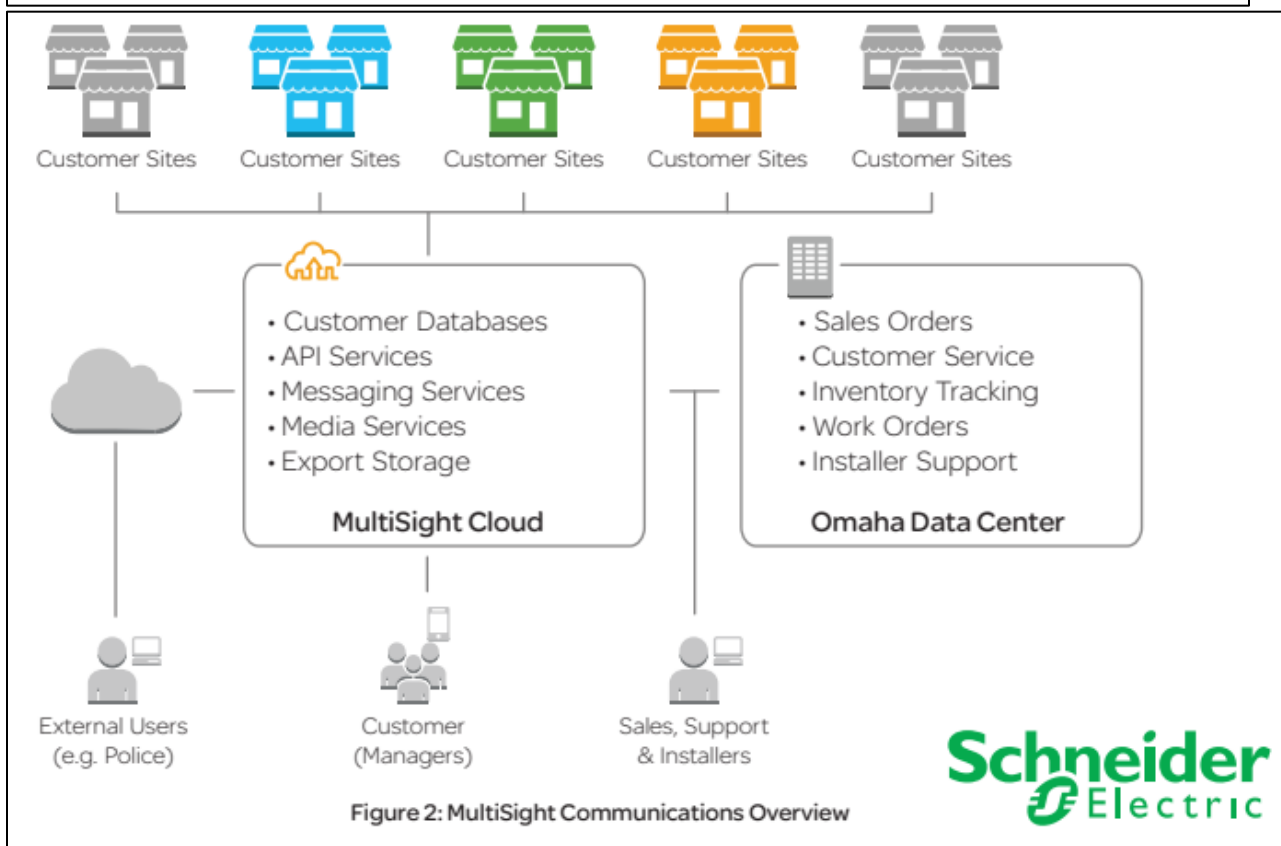
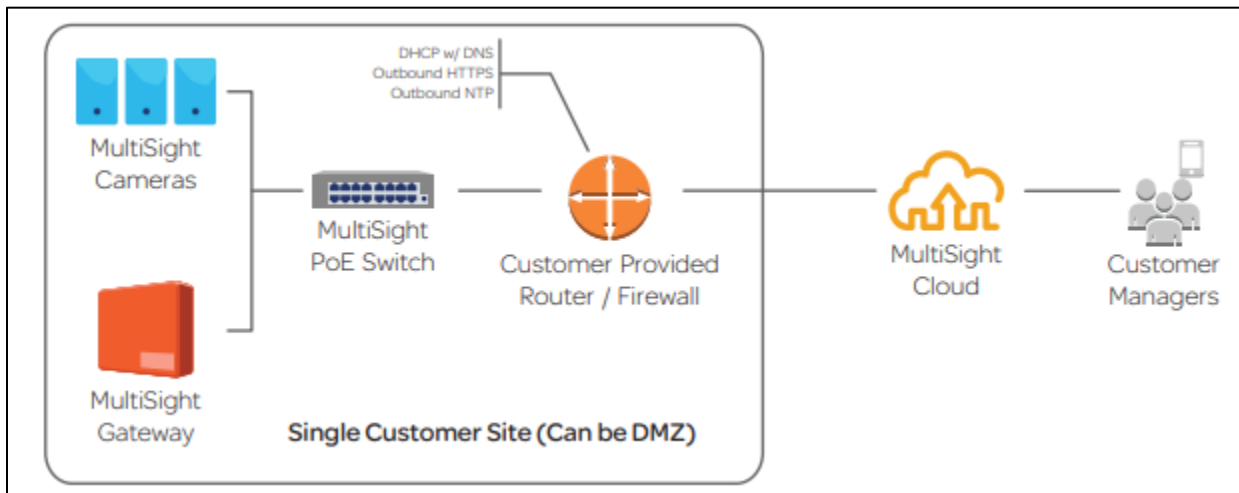


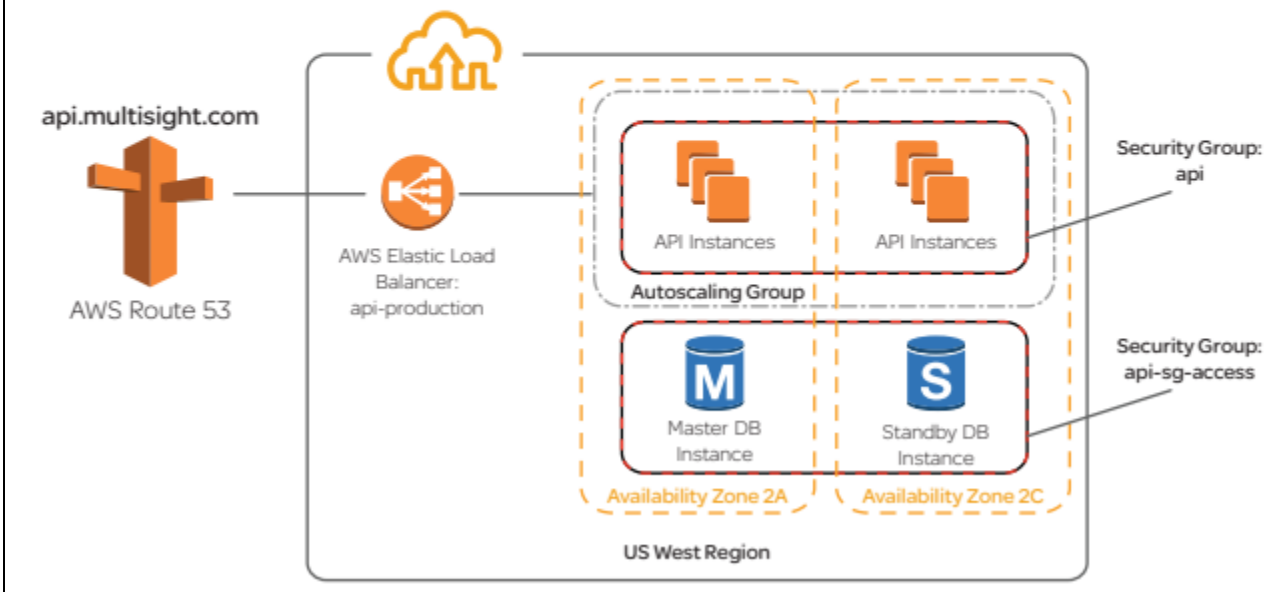
Figure 2: MultiSight Communications Overview



### MultiSight Cloud Security

MultiSight Cloud is operated on Amazon Web Services, and enjoys many of the security benefits built into the AWS infrastructure. Amazon's security features are documented in the following whitepaper:

[http://media.amazonwebservices.com/pdf/AWS\\_Security\\_Whitepaper.pdf](http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)



<https://web.archive.org/web/20170316004740/http://www.multisight.com/pdfs/multisight-security-whitepaper.pdf>



**MultiSight Camera**

<https://web.archive.org/web/20190713063959/http://www.multisight.com/pdfs/tech-specs-camera.pdf>

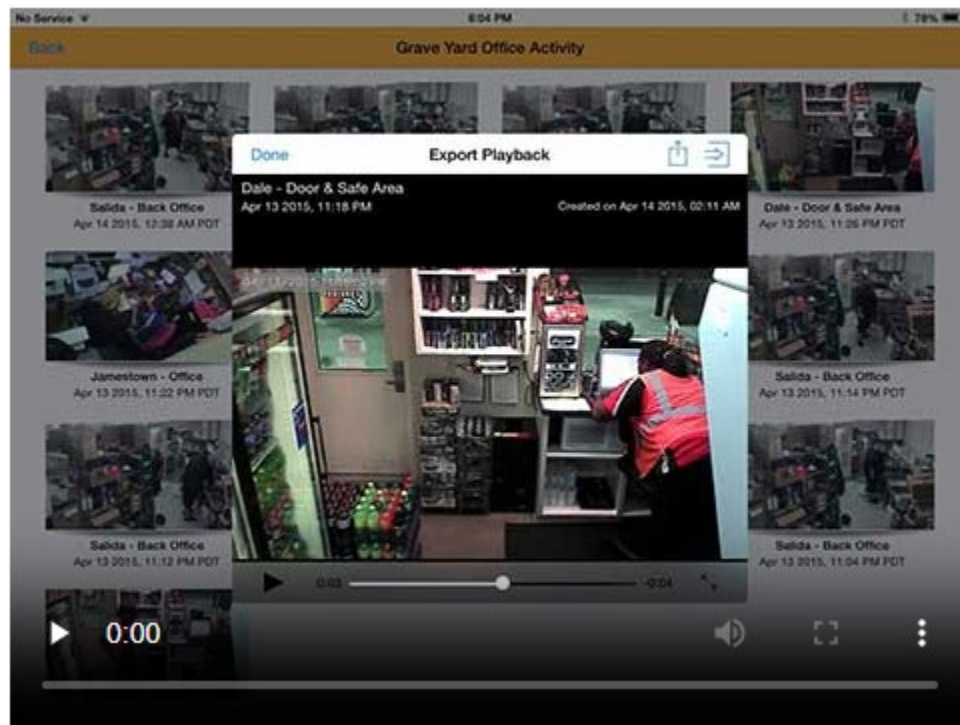


MultiSight Gateway

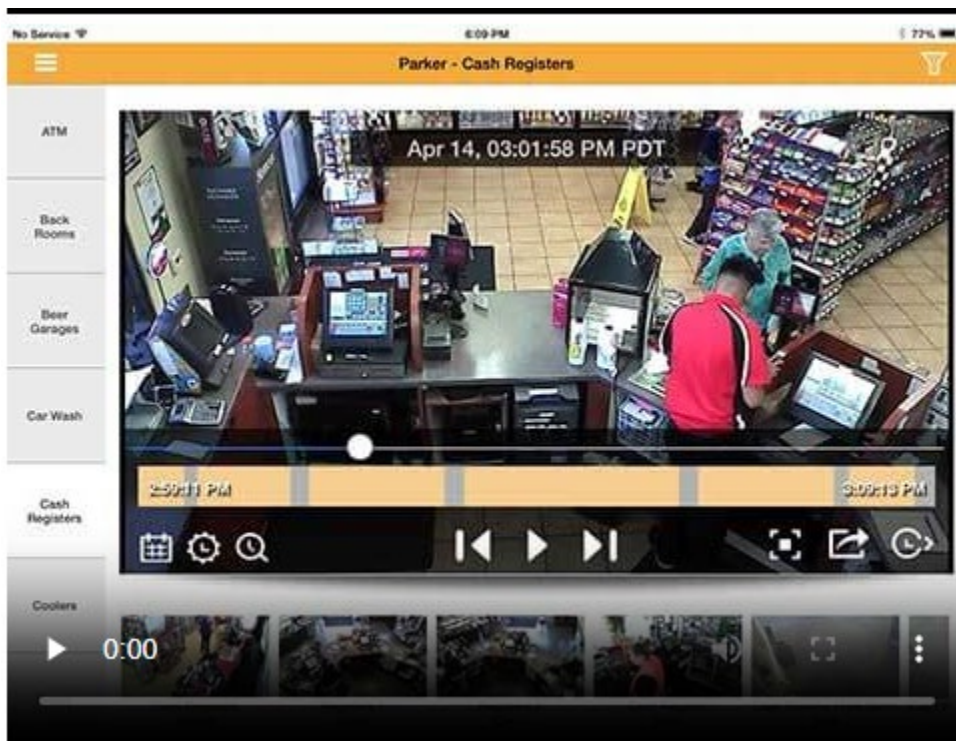
<https://web.archive.org/web/20190713093235/http://www.multisight.com/pdfs/tech-specs-gateway.pdf>

## A surveillance camera app made for business.

Designed with input from retailers like you, MultiSight's suite of apps and analytics help you manage your stores, wherever you are







<https://web.archive.org/web/20180321091555/http://www.multisight.com/surveillance-camera-app.html>



<https://web.archive.org/web/20180815194026/http://multisight.com/documentation.html>

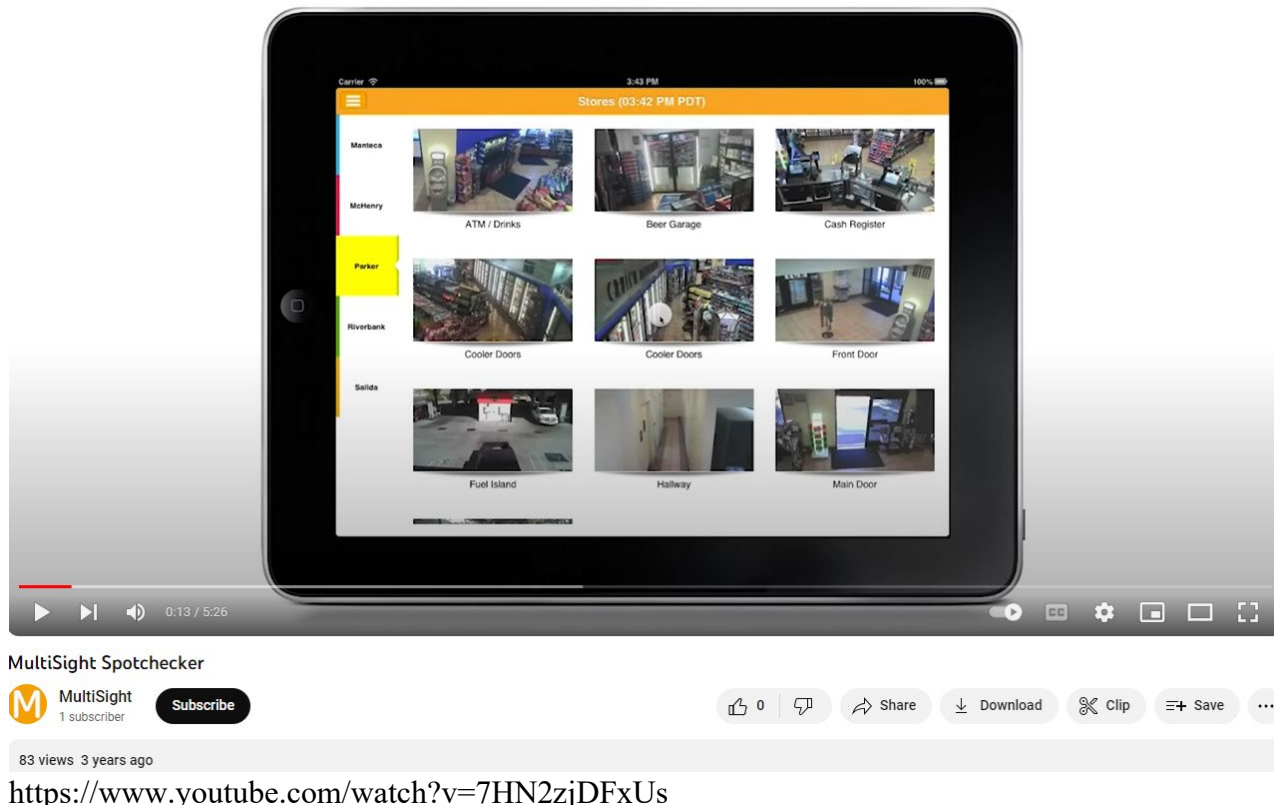
66. The Accused Products provide an internet web portal and smartphone applications for monitoring camera and devices such as through <https://webview.multisight.com/> and the Defendant App or smartphone application like Spotchecker (the “Defendant System Apps”).





67. Defendant provides promotional and instructional videos promoting the Accused Products online on websites such as youtube.com.

Pull down to refresh thumbnails



68. The Defendant’s System includes Defendant’s servers that form a network (first network), sometimes referred to as the MultiSight Cloud, located external to a user’s premises (home) and is accessible via an Internet browser (referred to as “Defendant’s External Network”). The Defendant’s External Network includes a plurality of communications servers with hardware processing circuitry (second hardware processing circuitry) (referred to interchangeably as “Defendant’s Communication Servers” or “Defendant’s Servers”).

69. The Defendant’s System includes a plurality of devices, such as the Defendant’s Cameras and energy monitoring devices and corresponding gateways, some of which, like the Defendant’s Multisight Gateway, also serve as “Connection Gateways”. The Defendant’s

Connection Gateways, in normal operation are located in a user’s (home/office) premises and are part of a local (home/office) network in such premises (referred to as “Defendant’s Home Network”). The Defendant’s Servers are configured to connect to the Defendant’s Connection Gateways.

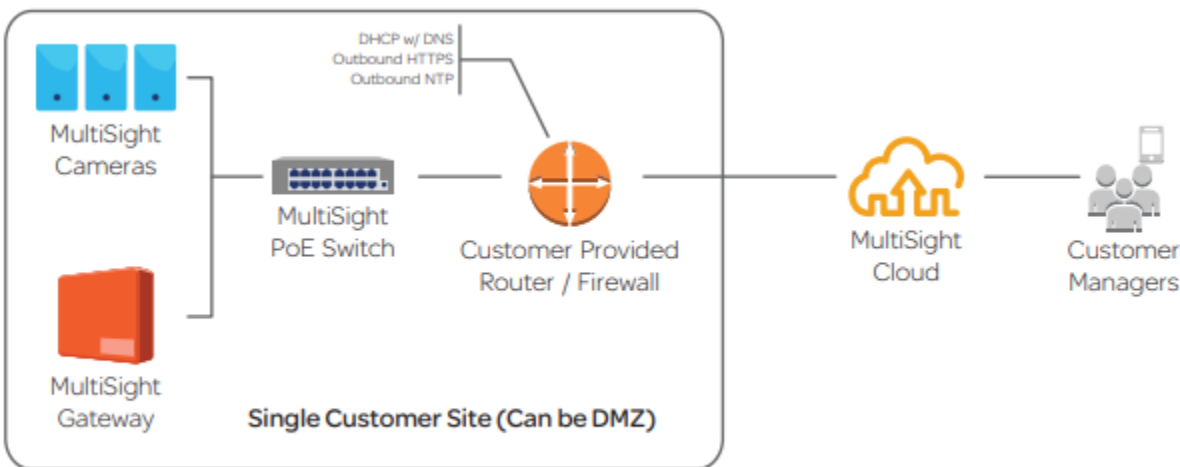


Figure 1: MultiSight On-Site Architecture

70. The Defendant’s Servers are adapted to interconnect on-demand with the Defendant’s Connection Gateways and are accessible via the Defendant’s System Apps.

71. When Defendant’s System App is used to access the Defendant’s External Network to monitor or control devices in the Defendant’s Home Network, authorization data is provided by the Defendant’s System App.

The MultiSight Gateway does not accept inbound network connections from the public Internet. Only two communication paths are necessary between the MultiSight Gateway and any outside devices:

1. Communication to the MultiSight Cloud are initiated via outbound HTTPS connections from the MultiSight Gateway to the MultiSight Cloud.
2. Communication between the MultiSight Gateway and the MultiSight Cameras on the LAN are via discovery of the camera’s SSDP advertisements, followed by an RTSP connection initiated by the gateway to the camera.

The MultiSight Cameras never communicate outside the LAN to the internet.

<https://web.archive.org/web/20170316004740/http://www.multisight.com/pdfs/multisight-security-whitepaper.pdf>

**COUNT I – DIRECT PATENT INFRINGEMENT OF THE '526 PATENT**

72. Portus re-alleges the foregoing paragraphs as if fully set forth herein.

73. Defendant's infringing Accused Products include all remote security, camera, and automation control systems with the same or similar features and functionality that satisfy each element of one or more asserted claims.

74. Defendant has directly infringed the '526 Patent in violation of 35 U.S.C. § 271(a) by one or more of the following: (1) making the Accused Products which embody the patented inventions of at least claim 57 of the '526 Patent, by combining all elements of the Accused Products as described above, in a manner that meets each limitation of at least claim 57 of the '526 Patent; and (2) putting into service and by operating the Accused Products when all elements of such system are combined as described above, thus meeting each limitation of at least claim 57 of the '526 Patent.

75. The Accused Products satisfy various elements of the claims of the '526 Patent, including certain devices that are Connection Gateways or networked components of the respective home network, or both.

76. For example, through the Defendant's Accused Products, Defendant infringes claim 57 of the '526 Patent. The Defendant's Accused Products form a system for remote access of user premises networks in respective user premises, the system comprising:

- a. a first network (a) located external to said user premises (e.g., *the Defendant External Network, which is located external to the user premises*), (b) including a first arrangement of processing circuitry comprising at least one hardware processor programmed to control network access (e.g., *the Defendant Servers have processors programmed to control network access through a username and password*), and (c) including a hardware user access browser device that comprises a processor running an access browser (e.g., *Defendant's Accused Products have a user interface accessible by a user through the Defendant System Apps*); and
- b. a plurality of second arrangements of processing circuitry each comprising at least one hardware processor programmed to control network access, each of at least a subset of

which is located in a respective one of the user premises and part of the respective user premises network of the respective user premises (e.g., *the Defendant System includes a plurality of connection gateways, such as at least the Defendant Cameras and Gateways*);

- c. wherein:
- d. said first circuitry arrangement is adapted by its programming to initiate an establishment of network connections to said second circuitry arrangements (e.g., *the Defendant's Servers are configured to connect to the Defendant's Connection Gateways*);
- e. the user access browser located on the first network is usable, by input of Uniform Resource Locators (URL), for locating and examining information on said first network and said user premises networks (e.g., *the Defendant's System is configured to be responsive to the input of a URL, when the Defendant's External Network and a Defendant's Server are accessed as a result of the input of the URL at the Defendant's System Apps, the Defendant's Server provides Defendant's System Apps information like images or videos*);
- f. each of the at least the subset of second circuitry arrangements is accessible by the first circuitry arrangement (e.g., *the Defendant's Servers are configured to connect to the Defendant's Connection Gateways*);
- g. responsive to user-input of a URL in accordance with which said user access browser accesses a predetermined location on said first network to which address the URL corresponds, said first circuitry arrangement subsequently, by execution of its programming (e.g., *the Defendant's System is configured to be responsive to the input of a URL, at the Defendant's System Apps, to access an address on the Defendant's External Network, such that the Defendant's System Apps provide authorization data*);
- h. determines which one of said user premises networks in which one of said second circuitry arrangements is located authorization data indicates authority to at least one of monitor and control (e.g., *when a Defendant's System App is used to access the Defendant's External Network to monitor or control devices in the Defendant's Home Network, authorization data is provided by the Defendant's System App*): and
- i. initiates an establishment of a network connection to said one of said second circuitry arrangements to create a new communications session for a temporary interconnection between said first network and said determined one of said user premises networks to at least one of control and monitor operation of at least one of the one or more devices of said user premises network, by which communications session the first network (e.g., *the Defendant's Server creates a new communications session between itself and the Defendant Connection Gateway in a user's home network that was determined to be indicated by the authorization data. In normal operation of the Defendant's System, the new communications session is used to at least monitor or control at least one service or networked component in user's home network*):
- j. obtains information contained within the user's premises network from the second circuitry arrangement of the determined user's premises network (e.g., *after the new communications session is created, the Defendant's External Network obtains/receives*

*information contained within the determined user's home network from the Defendant's Connection Gateway (for example, from one of the networked components)); and*

- k. using a web server, serves to the user's access browser the information from the second circuitry arrangement of the determined user's premises network (e.g., *the system provides such information to the Defendant's System Apps*);
- l. the communications session provides a seamless access to information stored on said determined one of said user's premises networks from said user's access browser (e.g., *the system stores such information from the Defendant's System Apps for subsequent review by a user without requiring the user to provide the authentication data*); and
- m. the, at least one of, control and monitoring of at least one device using the first circuitry arrangement is possible only by interaction with information served by said one of said second circuitry arrangements (e.g., *the Defendant's devices may only be remotely controlled and monitored by providing information from the device to the Defendant's External Network*).

77. Defendant sell a variety of products that infringe based on similar functionality as the Defendant's Accused Products.

78. Defendant condition use of the remote access features of the Accused Products and its customers' receipt of a benefit upon performance of the limitations of the asserted claims in the Asserted Patents, and Defendant establish the manner or timing of that performance. Defendant requires that a user agree to terms and conditions that allow Defendant to track content, use, and performance information of user and the Accused Products. For example, users must agree to allow Defendant to access its personal data, or otherwise the users will be unregistered from the service and products: "It is always up to you whether to disclose personal information to us, although if you elect not to do so, we reserve the right not to register you as a user or provide you with any products or services.." <https://web.archive.org/web/20180817200436/https://www.schneider-electric.us/en/about-us/legal/data-privacy.jsp>. The Privacy Policy states that Defendant collects personal information about users:

"Schneider Electric collects and uses your personal information to better serve you and personalize your experience and interaction with Schneider Electric. Such collection is done with appropriate notice and consent, along with required filings with data protection authorities, where applicable. Personal information (or personal data) means any information

relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. This privacy statement does not cover personal information rendered anonymous or where pseudonyms are used. Data is rendered anonymous if individual persons are no longer identifiable or are identifiable only with a disproportionately large expense in time, cost, or labour. The use of pseudonyms involves the replacement of names or other identifiers with substitutes, so that identification of individual persons is either impossible or at least rendered considerably more difficult. If data rendered anonymous becomes no longer anonymous (i.e., individual persons are again identifiable), or if pseudonyms are used and the pseudonyms allow identification of individual persons, then this privacy statement will again apply. It is always up to you whether to disclose personal information to us, although if you elect not to do so, we reserve the right not to register you as a user or provide you with any products or services. The types of personal information we collect from you may include:

- your name, company, email address, phone number, billing address and shipping address
- customer type, job function, job title, purchasing authority, purchasing timeframe and others
- product and service preferences, contact preferences, educational and employment background, and job interest data
- your Schneider Electric user ID and password (where applicable)
- credit card information (where applicable)
- IP address (see chapter on cookies).”

79. The Privacy Policy goes on to describe all of the different ways Defendant uses and shares its customers' information. This is available at: <https://web.archive.org/web/20180817200436/https://www.schneider-electric.us/en/about-us/legal/data-privacy.jsp>.

80. The Accused Products, when combined and used as described above, satisfy each and every element of each asserted claim of the '526 Patent either literally or under the doctrine of equivalents.

81. Defendant's infringing activities are and have been without authority or license under the '526 Patent.

82. The preceding discussion of claim 57 in the '526 Patent serves as an example only. The Accused Product infringes other claims in the '526 Patent upon same or similar grounds. Portus reserves its right to identify additional claims and additional infringing products as supported by discovery in the case.

83. As a result of Defendant's unlawful infringement of the '526 Patent, Portus has suffered damage. Portus is entitled to recover from Defendant the damages suffered by Portus as a result of Defendant's unlawful acts of infringement.

84. On information and belief and at a minimum, Defendant has been aware of its infringement of the '526 Patent since 2015 when it was contacted by a representative of the Plaintiffs and provided with infringement claim charts.

85. Given Defendant's prior knowledge of the '526 Patent and its own infringement of the same, Defendant has induced its users' and contributed to its users' direct infringement of one or more claims of the '526 Patent through the Defendant's advertisements, instructions, advice, and guidance as provided by user manuals and instructions, the Defendant's websites, and Defendant's support and help services.

86. Moreover, Defendant's infringement has been willful and egregious. Because of Defendant's willful and egregious infringement, Portus is entitled to enhanced damages, in the form of treble damages, under 35 U.S.C. § 284.

87. To the extent Defendant did not learn of the '526 Patent and its infringement before the filing of this complaint by virtue of its monitoring of prior art and published patents and communications from Portus and its agents, Defendant was willfully blind to its infringement of the '526 Patent.



88. Furthermore, because Defendant's infringement of the '526 Patent is willful, this action is "exceptional" within the meaning of 35 U.S.C. § 285, entitling Portus to its attorneys' fees and expenses.

## **COUNT II – INDIRECT PATENT INFRINGEMENT OF THE '526 PATENT**

89. Plaintiffs reallege and incorporate by reference the allegations set forth above, as if set forth verbatim herein.

90. Defendant also has infringed, and continue to infringe, at least claim 57 of the '526 Patent by actively inducing others to use, offer for sale, and sell the Accused Products. Defendant's users, customers, agents or other third parties who use those devices in accordance with Defendant's instructions infringe claim 57 of the '526 Patent, in violation of 35 U.S.C. § 271(b).

91. Defendant knows that the Accused Products are especially designed for and marketed toward infringing use by Defendant's customers, to implement camera and energy monitoring features. Defendant induced, caused, urged, encouraged, aided and abetted its direct and indirect customers to make, use, sell, offer for sale and/or import one or more of the Accused Products. Defendant provides step-by-step instructions for installation, setup, and use of the Accused Products to infringe, either literally or under the doctrine of equivalents, at least claim 57 of the '526 Patent. These instructions are provided by Defendant as user manuals and online content made available by Defendant through its website and other online locations. Such conduct by Defendant was intended to and actually did result in direct infringement by Defendant's direct and indirect customers, including the making, using, selling, offering for sale and/or importation of the Accused Products in the United States. Defendant knows that its customers are infringing by performing the steps of claim 57 because it operates the servers and cloud that store the data and information and communicates with the users' devices.



92. Defendant contributes to the infringement of at least claim 57 of the '526 Patent by its customers and end users of at least the Accused Products and is therefore liable for indirect infringement under 35 U.S.C. § 271(c). The Accused Products are especially designed for controlling and monitoring use of smart home devices in the manner described above. Upon information and belief, the Accused Products have no substantial non-infringing use, as they are specifically designed and marketed for use by customers for controlling and monitoring use of smart home devices. Setup and use of the Accused Products by Defendant's customers in the manner constitutes direct infringement, either literally or under the doctrine of equivalents, of at least claim 57 of the '526 Patent. Defendant knows that its customers are infringing by performing the steps of claim 57 because it operates the servers and cloud that store the data and information and communicate with the user devices.

93. By way of further examples of Defendant's intent to infringe, Defendant intentionally instructs customers to infringe through training videos, demonstrations, brochures and user guides. For example, as shown in the myriad examples above (see paragraphs 57-66 and 72), Defendant has published in its instructional and marketing materials instances of Defendant using the Accused Products. In paragraph 58, Portus has provided screenshots from Defendant's video posted on YouTube showing Defendant's own use of the Accused Products through Defendant's System App on a smartphone. Likewise, in paragraphs 57 and 59, Portus has included snippets from Defendant's own publications showing its use of the Accused Products through Defendant's System Apps and access browsers on smartphones, tablets, and computers. Again, in paragraph 62, Portus has provided a snippet from Defendant's promotional and instructional materials showing its use of the Accused Products through Defendant's System Apps and access browsers on a smartphone and Defendant's Access Browser Device.

94. Defendant has been on notice of its infringement of the '526 patent since at least 2015. Defendant received a notice letter from Portus or its agent, alerting it of infringement by the Accused Products, and inviting Defendant to an auction to buy the asserted patents. In the notice letter, Portus included a detailed claim chart setting forth its infringement accusations for the MultiSight system, which was representative of other infringing products. Thus, there is no doubt that Defendant received the notice letter from Portus, and it was clearly aware of patents-in-suit and on notice of its own infringement.

95. By the time of filing the original complaint in this lawsuit, Defendant knew and intended that its continued actions would actively induce and contribute to the infringement of at least claim 57 of the '526 Patent, and Defendant is thereby liable for infringement of the '526 Patent under 35 U.S.C. § 271(b) and (c).

### **COUNT III – DIRECT PATENT INFRINGEMENT OF THE '097 PATENT**

96. Plaintiffs reallege and incorporate by reference the allegations set forth above, as if set forth verbatim herein.

97. Defendant's infringing Accused Products and other remote camera, monitoring, and automation control systems with the same or similar features and functionality that satisfy each element of one or more asserted claims.

98. Defendant has directly infringed the '526 Patent in violation of 35 U.S.C. § 271(a) by one or more of the following: (1) making the Accused Products which embody the patented inventions of at least claim 1 of the '097 Patent, by combining all elements of the Accused Products as described above, in a manner that meets each limitation of at least claim 1 of the '097 Patent; and (2) putting into service and by operating the Accused Products when all elements of such system are combined as described above, thus meeting each limitation of at least claim 1 of the '097 Patent.

99. For example, through the Defendant's Accused Products, Defendant infringes claim 1 of the '097 Patent. The Defendant's Accused Products form a system for remote access of a user premises comprising:

- a. a first hardware processing circuitry running an access browser module (*e.g., the Accused Products utilizes an access browser hardware device including a processor to access the internet through the Defendant's System Apps*);
- b. a second hardware processing circuitry located in a first network (*e.g., the Accused Products include a second processor in the Defendant's External Network that is located external to the user premises*); and
- c. a connection gateway that is located in, and is part of a local network of, the user premises (*the Accused Products include a plurality of connection gateways (e.g., Defendant's connection gateways, such as the Defendant's Camera and base station) each comprising at least one hardware processor and each of at least a subset of which is located in a respective one of the user premises and is part of the respective home network of the respective user (e.g., connected to the home network via Ethernet)*);
- d. wherein:
- e. the second hardware processing circuitry is external to the user premises, is accessible via the access browser module, and is configured to communicate on-demand with the connection gateway (*e.g., the Accused Product includes a communications server (e.g., Defendant's Servers) comprising at least one hardware processor and located in said external network and adapted to interconnect on-demand with said connection gateways (e.g., users are able to access their devices through the Defendant's System Apps)*);
- f. the connection gateway is integrated with or communicatively coupled to one or more networked components of the local network of the user premises (*e.g., the connection gateways are accessible by the external network and are integrated with networked components (e.g., Defendant's devices) of the respective home network*); and
- g. the system is configured such that user-input of a Uniform Resource Locator (URL), in accordance with which the first hardware processing circuitry, using the access browser module, accesses an address on the first network, begins a sequence in which the second hardware processing circuitry responsively serves to the first hardware processing circuitry, via the access browser module, information regarding at least one of the one or more networked components of the local network, which information the second hardware processing circuitry obtains from the connection gateway without a direct communicative coupling between the second hardware processing circuitry and the at least one networked component of the local network (*e.g., the Defendant's web application is responsive to user-input of a Uniform Resource Locator (URL) (e.g., when accessing Defendant's System Apps and the Defendant's applications) in accordance with which said app accesses a predetermined address on said external network to which the URL corresponds, in which accessing said app provides information (e.g., videos)*);

*contained within the home network from the connection gateway of the determined home network and Defendant's servers or external network are not directly communicatively coupleable to a user's Defendant's devices (e.g., certain Defendant's devices only communicate through connection gateways); in which accessing said app provides authorization data to the external network (e.g., a login and password));*

- h. wherein the sequence includes the first hardware processing circuitry transmitting to the second hardware processing circuitry authentication data indicating authority to access the at least one networked component of the local network, the transmission of the authentication data being required for the serving of the information to the first hardware processing circuitry (e.g., *the connection gateways for the Accused Products require that the user first provide authentication data in which accessing said app provides authorization data to the external network to access the networked components*), and wherein:
  - i. the user premises is one of a plurality of user premises (e.g., *Defendant's Accused Products serve multiple users and multiple premises*);
  - j. the connection gateway is one of a plurality of connection gateways, each of which is located in, and is part of a respective local network of, a respective one of the plurality of user premises, and to each of which the second hardware processing circuitry is configured to connect (e.g., *Defendant's Accused Products serve multiple users and multiple premises, which each include at least one connection gateway located in and connects to a respective local network of the premises*); and
  - k. the sequence further including the second hardware processing circuitry determining which one of the local networks the authentication data indicates authority to access (e.g., *Defendant's server is configured to use the user's login credentials to determine which home network is the user's home network and is further configured to provide authorization data to allow the user to access devices in the user's home network*);
  - l. the sequence further including the second hardware processing circuitry establishing a new communication session between the first hardware processing circuitry and the connection gateway of the respective local network that the authentication data indicates authority to access upon verification of the authentication data (e.g., *Defendant's servers create a new communications session between the external network and one of the Defendant's Connection Gateways to monitor operation of the Defendant's devices contained within the home network, which is determined based on the authentication*); and
  - m. wherein the second hardware processing circuitry receives, via the connection gateway, selected information from at least one of the networked components of the local network of the user premises, and stores the selected information in the first network for subsequent review by a user associated with the user premises, without requiring the user to provide the authentication data (e.g., *in the Accused Products, information from the Defendant's devices, such as video data, is stored in the first network, which may then be reviewed by a user associated with the user premises without requiring the user to provide the authentication data (e.g., a user in the first network may be automatically logged in*

*to the Accused Products without having to subsequently enter their login information));*  
and

- n. wherein the authority to access the at least one networked component of the local network by transmitting the authentication data also provides authority to access and review the previously stored selected information in the first network via the access browser module (*e.g., the Defendant's user app and Defendant's servers communicate such that authority is provided to access Defendant's device in a local network and review the previously stored selected information via authentication data*).

100. Defendant sells a variety of products that infringe based on similar functionality as the Defendant's Accused Products.

101. Defendant's condition use of the remote access features of the Accused Products and its customers' receipt of a benefit upon performance of the limitations of the asserted claims in the Asserted Patents, and Defendant establishes the manner or timing of that performance. Defendant requires that a user agree to terms and conditions that allow Defendant to track content, use, and performance information of user and the Accused Products. For example, users must agree to allow Defendant to access its personal data, or otherwise the users will be unregistered from the service and products: "It is always up to you whether to disclose personal information to us, although if you elect not to do so, we reserve the right not to register you as a user or provide you with any products or services.." <https://web.archive.org/web/20180817200436/https://www.schneider-electric.us/en/about-us/legal/data-privacy.jsp>. The Privacy Policy states that Defendant collects personal information about users:

"Schneider Electric collects and uses your personal information to better serve you and personalize your experience and interaction with Schneider Electric. Such collection is done with appropriate notice and consent, along with required filings with data protection authorities, where applicable. Personal information (or personal data) means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. This privacy statement does not cover personal information rendered anonymous or where pseudonyms are used. Data is rendered anonymous if individual persons are no longer identifiable or are identifiable only with a disproportionately large expense in time, cost, or labour. The use of pseudonyms involves the replacement of names or other identifiers with substitutes, so that identification of individual persons is either

impossible or at least rendered considerably more difficult. If data rendered anonymous becomes no longer anonymous (i.e., individual persons are again identifiable), or if pseudonyms are used and the pseudonyms allow identification of individual persons, then this privacy statement will again apply. It is always up to you whether to disclose personal information to us, although if you elect not to do so, we reserve the right not to register you as a user or provide you with any products or services. The types of personal information we collect from you may include:

- your name, company, email address, phone number, billing address and shipping address
- customer type, job function, job title, purchasing authority, purchasing timeframe and others
- product and service preferences, contact preferences, educational and employment background, and job interest data
- your Schneider Electric user ID and password (where applicable)
- credit card information (where applicable)
- IP address (see chapter on cookies).”

102. The Privacy Policy goes on to describe all of the different ways Defendant uses and shares its customers’ information. This is available at: <https://web.archive.org/web/20180817200436/https://www.schneider-electric.us/en/about-us/legal/data-privacy.jsp>.

103. The Accused Products, when combined and used as described above, satisfy each and every element of each asserted claim of the ’097 Patent either literally or under the doctrine of equivalents.

104. Defendant’s infringing activities are and have been without authority or license under the ’097 Patent.

105. The preceding discussion of claim 1 in the ’097 Patent serves as an example only. The Accused Product infringes other claims in the ’097 Patent upon same or similar grounds. Portus reserves its right to identify additional claims and additional infringing products as supported by discovery in the case.

106. As a result of Defendant's unlawful infringement of the '097 Patent, Portus has suffered and will continue to suffer damage. Portus is entitled to recover from Defendant the damages suffered by Portus as a result of Defendant's unlawful acts of infringement.

107. On information and belief and at a minimum, Defendant has been aware that the claims in the application that became the '097 Patent were allowed before the filing of this complaint.

108. On information and belief, given Defendant's prior knowledge of the '097 Patent and its own infringement of the same, Defendant has induced its users' and contributed to its users' direct infringement of one or more claims of the '097 Patent through the Defendant's advertisements, instructions, advice, and guidance as provided by user manuals and instructions, the Defendant's websites, and Defendant's support and help services.

109. Moreover, on information and belief, Defendant's infringement has been willful and egregious. Because of Defendant's willful and egregious infringement, Portus is entitled to enhanced damages, in the form of treble damages, under 35 U.S.C. § 284.

110. To the extent Defendant did not learn of the '097 Patent and its infringement before the filing of this complaint by virtue of its monitoring of prior art and published patents and communications from Portus and its agents, Defendant was willfully blind to its infringement of the '097 Patent.

111. Furthermore, because Defendant's infringement of the '097 Patent is willful, this action is "exceptional" within the meaning of 35 U.S.C. § 285, entitling Portus to its attorneys' fees and expenses.

**JURY DEMAND**

112. Portus hereby demands a trial by jury.

**PRAYER**

WHEREFORE, Portus prays for judgment in its favor and against Defendant as follows:

- a. A judgment that Defendant has infringed, directly or indirectly, either literally or under the doctrine of equivalents, one or more claims of the Asserted Patents;
- b. An award of damages adequate to compensate for the infringements, but in no event less than a reasonable royalty made for use of the inventions of the Asserted Patents, together with interest and costs as determined by the Court, and an accounting of all infringing acts including, but not limited to, those acts not presented at trial;
- c. An award of enhanced damages under 35 U.S.C. § 284, in the form of treble damages;
- d. An award of on-going royalties for any continuing or future infringement of the claims of the Asserted Patents;
- e. An award of Plaintiffs' reasonable attorneys' fees, costs, and expenses pursuant to 35 U.S.C. §§ 284 and 285 or as otherwise permitted by law;
- f. Such other and further relief at law or in equity as the Court determines is just and proper.



Dated: September 5, 2023

STAMOULIS & WEINBLATT LLC

/s/ Richard C. Weinblatt

Stamatios Stamoulis (#4606)  
Richard C. Weinblatt (#5080)  
800 N. West Street, Third Floor  
Wilmington, DE 19801  
(302) 999-1540  
stamoulis@swdelaw.com  
weinblatt@swdelaw.com

Manoj S. Gandhi (*pro hac vice* to be filed)  
CLAYTON, MCKAY & BAILEY, PC  
1919 Decatur Street  
Houston, TX 77007  
Phone: (832) 782-4964  
manoj@cmlaw.com

**ATTORNEYS FOR PLAINTIFFS  
PORTUS SINGAPORE PTE LTD AND  
PORTUS PTY LTD**