STATE OF NEW YORK

TAX APPEALS TRIBUNAL

In the Matter of the Petitions of **SECUREWORKS, INC.** for Revision of Determinations or for Refund of Sales and Use Taxes under Articles 28 and 29 of the Tax Law for the period September 1, 2011 through November 30, 2015.	:	DECISION DTA NOS. 828328 AND 828329

Petitioner, Secureworks, Inc., filed an exception to the determination of the Administrative Law Judge issued on January 14, 2021, regarding its consolidated petitions. Petitioner appeared by Ryan, LLC (Charles Rice, Esq., of counsel). The Division of Taxation appeared by Amanda Hiller, Esq. (Stephanie Scalzo, Esq., of counsel).

Petitioner filed a brief in support of the exception. The Division of Taxation filed a brief in opposition. Petitioner filed a reply brief. Oral argument was heard by teleconference on August 26, 2021, which date began the six-month period for the issuance of this decision.

After reviewing the entire record in this matter, the Tax Appeals Tribunal renders the following decision.

ISSUE

Whether petitioner's managing and monitoring services are protective and detective services subject to sales tax pursuant to Tax Law § 1105 (c) (8).

FINDINGS OF FACT

We find the facts as determined by the Administrative Law Judge, except that we have modified finding of fact 1 for clarity. As so modified, the findings of fact are set forth below.

1. Petitioner, Secureworks, Inc., is an information technology (IT) security services provider that offers managed and monitored security services, giving customers information to prevent, detect, respond to, and predict cyberattacks. Petitioner's customers are made aware of potential threats in the critical areas of their IT infrastructure. Petitioner is headquartered and has its principal address in Atlanta, Georgia.

2. Several of petitioner's services have a management component and a monitoring component. When petitioner is performing management services, it is making changes to the device or software to help the customer keep the device or software operating properly. Petitioner's monitoring services involve reviewing the events that a device or software is producing and advising customers when they should investigate an event further. The components of a security infrastructure generate thousands of events each day. Petitioner helps its customers determine which events require their attention. Most of petitioner's services are sold as a monitoring service or as a monitoring service plus management.

3. When petitioner discovers a new threat actor as part of its managing and monitoring services, the threat actor is included in its threat intelligence services, which are described below.

4. Petitioner manages and monitors firewalls. These services are sold as annual subscriptions. A firewall is a security device that is connected to a customer's network. The firewall controls the connections that are allowed access into the customer's network and the connections from the customer's network to outside the company. The firewall is configured to block unauthorized access to a customer's computer. Vulnerabilities arise when certain connections need to be allowed through the firewall, creating an opportunity for unauthorized access. Petitioner does not sell the firewall with its managing and monitoring service. Its customers purchase firewalls from other manufacturers.

Firewalls generate security events that indicate when someone is connected to a site or when a connection has been blocked. Petitioner monitors those events and notifies its customers when it thinks they should be aware of an event and investigates further for things such as a virus or software designed to gain unauthorized access to a computer system to disrupt or damage the system. Petitioner does not identify who is attempting the unauthorized access or assess any damage that was done.

Petitioner's website provides that "[f]irewall management is resource-intensive and requires a high level of expertise to prevent unauthorized access and costly breaches. Devices must be provisioned, deployed, upgraded and patched to keep up with the latest threats." Managing a firewall includes updating a firewall's security policies and configurations, implementing software upgrades and performing patch maintenance. This service involves petitioner obtaining the software upgrade or patch from the manufacturer and testing it to determine whether it will help prevent the latest threats. If petitioner thinks the upgrade or patch is beneficial, it will work with the customer to determine when to apply it and petitioner will apply it for the customer. The management service also includes petitioner configuring the firewall with intelligence from its "global visibility" and Counter Threat Unit (CTU) research to look for signatures or patterns in the network traffic for signs of malicious intent. This is referred to as "policy management." This includes integrating information from petitioner's Attacker Database of Internet Protocol (IP) addresses associated with known threats.

Petitioner performs this same service for "Integrated Appliances." These are referred to in the industry as next generation firewalls. They are firewalls that do more than just monitor the network connections. These devices may be able to serve other security functions such as operating as an intrusion detection system, which is explained below.

5. Petitioner provides network intrusion detection/prevention services, including an advanced endpoint threat detection (AETD) monitoring service, and monitoring and/or managing intrusion detection systems (IDS) or intrusion prevention systems (IPS) and iSensor services. Petitioner's AETD service is based on endpoint intelligence developed by petitioner's CTU research team. Under the AETD service, petitioner provides constant detection and analysis of potential threats to a customer's endpoints, such as a server, laptop or desktop, so that it can respond quickly and whenever necessary. As stated on petitioner's website "AETD goes beyond identifying a threat to accessing extensive intelligence on threat actors and their tradecraft, helping you to accelerate your response by pinpointing exactly which systems are compromised, how it happened and how you can repair them." Petitioner claims that it knows what to look for and can detect more threats than its competition. Customers have access to petitioner's hosted cloud solution that sends alerts through telephone or email depending on the severity level of the issues.

6. For petitioner's managed and monitored IDS/IPS service, petitioner provides proactive administration 24 hours a day, 365 days a year. Petitioner's security experts perform all activities to keep the devices operating at peak performance. IDS and IPS look for patterns in the traffic that may show that someone is trying to breach or compromise a client's network. The IDS or IPS include a hardware device or software that can create and/or monitor security events. One piece of equipment, or software, can be configured to be either an IDS or an IPS. The customer will install and configure it based on how the customer wants it to function. An IDS looks at the network traffic watching for signs of malicious intent. It records the connections, but it cannot prevent a connection. An IPS acts like a firewall, where traffic has to go through it, and it can be configured to block access to the client's network. The IPS has to be in the middle of the network traffic so that it can stop the connections when it detects something

malicious. If a customer purchases an IDS or an IPS device from a company other than petitioner, petitioner will provide management and/or monitoring services for it.

Petitioner's management and monitoring services to IDS and IPS are similar to the services petitioner provides for a firewall. When managing the device, petitioner configures the IDS or IPS device to look for signatures or patterns in the network traffic for signs of malicious intent. Petitioner then maintains this configuration. Policies are continuously assessed and updated to prevent threats from accessing petitioner's customer's networks. Like with their service to firewalls, petitioner also tests any patches from the manufacturer of the IDS and IPS and installs them.

When monitoring the device, petitioner tracks events produced by the IDS or IPS and evaluates them to determine whether its customers need to investigate an event further. The events the IDS and IPS produce will indicate whether there was malicious intent. They do not confirm whether there has been a breach of a customer's network. This service does not identify the person causing the breach or the damage done by any breach.

7. Petitioner sells a product called an iSensor, which is an IDS or IPS that petitioner sells as part of a managed and monitored service. There is no separate charge for the iSensor. Customers install their own iSensor. When installed as an IPS, an iSensor performs the same functions as a firewall.

8. Petitioner offers a security event monitoring service that involves monitoring of information security activity across a customer's network. Petitioner refers to this service in its brief as "Server/Network Infrastructure Monitoring" and a similar but more limited service as "SIM On-Demand Server/Maintenance Infrastructure." The primary difference between these two services is that the Server/Network Infrastructure Monitoring service offers a human component where, if petitioner finds something worth a customer's attention, it will call the

customer any time, day or night. The SIM on-Demand service only communicates issues to the customer through the customer portal.

Petitioner gives its customers a virtual counter threat appliance (CTA) or an inspector that connects to a customer's network to capture events from servers and network devices, including routers, firewalls, and intrusion detection systems to reveal security threats. The customers are responsible for directing the events to the CTA, which condenses them and sends them back to petitioner for analysis.

The service is provided to customers using petitioner's counter threat platform (CTP). The CTP provides health checks on managed and monitored devices. The CTP can aggregate events from most devices. The CTP technology processes event information to identify events of interest. The CTA or inspector will compare events to known malicious activity and known normal activity. Security experts then conduct further analysis and escalate security incidents to customers. Customers can view the events and incidents through petitioner's customer portal, which features integrated business intelligence and analytics tools to assist customers in making better security decisions.

9. Petitioner also offers a subscription for a log retention service. Logs are repositories that collect security events that come from devices such as firewalls, IDSs, IPSs, servers and routers. Petitioner's website provides that "[e]very security appliance, business-critical system, noncritical server and endpoint . . . generates extensive event logs daily that must be managed to provide an early warning system for fast response to security events." Petitioner offers a LogVault, which is a device that customers connect to their network and stores all of their events. Petitioner also offers virtual log retention appliances. There is one combined charge for the LogVault and the service. Petitioner helps the customer configure and implement the LogVault or software, it monitors it to ensure it is operating properly, and it patches and

upgrades it periodically. Petitioner also manages log retention devices purchased from other vendors. Petitioner reports the events created through its customer portal.

10. Petitioner also offers a log monitoring service. This service involves the effective management and monitoring of log retention appliances. The service includes the same initial tasks as the log retention service of configuring and implementing the retention appliance and ensuring it is operational. This service also then involves monitoring and analyzing customers' events generated across their networks. Petitioner reviews the events and notifies its customers of anomalies that aid in a customer's response to threats. Petitioner also uses this information when compiling data for its threat intelligence service.

11. Petitioner's threat intelligence service is a subscription service. The goal of this service is to educate customers about the likelihood that their organization will be breached. Petitioner's witness testified that threat intelligence service "is a collection of information services that we provide to our clients related to the threat landscape." The knowledge for these services comes from the internet, a national vulnerability database, common feeds that contain information about new vulnerabilities, and any new threat actor petitioner discovers as part of its managing and monitoring services it provides to its customers. This service allows customers to take advantage of petitioner's threat intelligence knowledge acquired through access to thousands of client environments around the world. Customers access this service through petitioner's customer portal or a data feed. The primary components of the threat intelligence service are its vulnerability data service, its threat analysis service, its advisory data service and its monthly security intelligence webinars.

In petitioner's vulnerability data service, customers are provided with detailed descriptions and analysis of current vulnerabilities. Vulnerabilities are software flaws that may be exploited to allow a malicious user or code to attack the software or operating system.

Vulnerabilities are processed from public and private data feeds, enriched by petitioner's researchers and reported to customers through the customer portal. This service is different from petitioner's vulnerability scanning service, which is explained more fully below and is unique to the vulnerabilities present on a single customer's network.

The threat data service component of petitioner's threat intelligence service involves petitioner's CTU research team publishing a detailed breakdown of malware or threats twice a month. Petitioner's advisory data service component involves petitioner providing reports analyzing attack data across petitioner's monitored security devices, including threats targeting many of its customers. Petitioner's monthly security intelligence webinar is open to all of petitioner's customers who subscribe to the threat intelligence service and involves the CTU research team hosting a monthly webinar security briefing where it describes current security threats and reviews current security concerns and hacker activities.

Petitioner also provides threat intelligence service customers a data feed of its attacker database. The database, which is updated daily, includes attack information, such as lists of malicious IP addresses and domains, processed from thousands of monitored security devices. This service is an add-on service that is charged separately.

12. Petitioner also offers a targeted threat hunting service. This service involves performing searches of a customer's networks and endpoints, such as laptops or tablets, to identify the presence of vulnerabilities and entrenched threat actors operating on a customer's environment. Petitioner's service assists its customers in determining how the threat got there, what its purpose is, and who may be behind it. Pursuant to petitioner's website, petitioner will also "provide specific guidance on appropriate response and remediation steps to contain and eradicate the threat and actor from your environment." Petitioner will also give

recommendations on security improvements. This service complements security event monitoring.

13. Petitioner also offers enterprise brand surveillance, which is one of its add-on threat intelligence services. The service consists of researchers conducting research and analysis to report and alert on security threats that are specific to a customer. Petitioner will analyze publicly accessible resources on the internet and use "open source intelligence" collection capabilities and other research capabilities. "Open source intelligence" was defined by petitioner in its service description as "any non-classified, unclassified, or publicly available information, as opposed to information that is acquired through covert or clandestine means for official purposes." Non-proprietary sources of information are used to acquire and synthesize data. Customers will give petitioner key words or terms and petitioner will search different portions of the internet, including surface web, which is the normal part of the web, and dark web and deep web, where more criminals are present.

Petitioner will provide its customers with a report of its findings through an encrypted email. Petitioner will report and alert on security threats that are specific to the customer on a monthly basis. The information collected is representative of what an attacker could compile about a customer's organization, to either capitalize on the information for malicious purposes or to serve as a basis for a future attack against a customer's organization. The customer can use the information to detect and prevent threats and threat actor activity. The components of the service involve a threat profile, monthly monitoring reports, monthly update meetings and monitoring and alerting. The reports are only provided to the customer who requests it.

14. Petitioner offers a vulnerability scanning service that scans network devices, servers, web applications, databases and other assets both at a customer's place of business and in cloud environments to find exposures to exploitation by threat actors so that its customers can eliminate

them. Petitioner's website provides that vulnerabilities can arise daily within networks, web applications, and databases, due to software defects or system misconfigurations. This service is delivered using petitioner's CTP and consists of automated and recurring vulnerability scanning and delivery of such scanning, along with remediation workflow tools. The customer portal features integrated business intelligence and analytics tools to assist its clients in obtaining meaningful insights and perspectives to make better IT security decisions. Petitioner's clients can run reports on demand using the client portal.

Included with this service is a license to use the scanning product Qualys, 24-hour access through petitioner's customer portal and 24-hour access to petitioner's counter threat operations center, to enable customers to ask questions related to the service. Petitioner also provides a quarterly telephone review of each customer's scan results.

15. Petitioner also provides incident response services. When a customer concludes that there has been a breach, it can hire petitioner to analyze, contain and help the customer recover from the breach.

16. For all of petitioner's monitoring services, when petitioner finds something that the customer needs to be apprised of, it generates a ticket that goes to the customer in petitioner's customer portal. If it is something petitioner believes is worth a customer's immediate investigation, petitioner will call the customer if it is in the customer's service agreement, and the customer will begin its own investigation to determine whether the event was a threat.

17. Another service petitioner provides is resident security operations. For this service, petitioner provides one of its employees to work at a customer's offices. Each agreement for the services performed by the resident security operations is custom to the customer. However, the most common usage involves petitioner's employee working at the customer's office receiving phone calls from petitioner regarding events and reviewing the events created by a client's

equipment and then determining whether the customer should be notified of the event or if another device in the customer's network that petitioner may not have access to blocked the threat. On its website, petitioner states that its "expert residents can help you design, implement, and manage full-scale security programs to protect your organization against cyber threats."

18. On June 27, 2014, the Division of Taxation (Division) sent a letter to petitioner scheduling an appointment at petitioner's office in Texas for February 9, 2015, to commence a sales and use tax field audit of its business for the period September 1, 2011 through August 31, 2014. The Division's letter requested that all books and records pertaining to petitioner's sales and use tax liability for the audit period be available for review. Enclosed with the letter to petitioner was an information document request (IDR), requesting specific records including the general ledger, cash receipts journal, federal income tax returns, state tax returns, purchase invoices, sales contracts providing details/support for the invoiced charges, fixed asset purchase invoices, cash disbursements journal, bank statements, canceled checks and deposit slips for all accounts, and exemption documents. In response to the IDR, the Division received some electronic sales information prior to the scheduled February 9, 2015 visit.

19. On September 14, 2015, October 13, 2015 and January 14, 2016, the Division sent a second IDR, requesting service orders/invoices and line item descriptions, such as service level agreements, service descriptions, and terms and conditions that are provided as explanation to the customer for each item number that they are purchasing on the service order/invoice. This was requested because the sales records were provided to the Division in Excel, and the line items that were charged did not have a description to determine what sale or service was being provided to the customer. The Division was provided with a few sample invoices at petitioner's offices in Texas, but was not provided any additional invoices during the course of the audit.

The Division did receive additional documents explaining some of the descriptions relating to some of the charges.

20. The Division also sent petitioner a letter on January 14, 2016, advising petitioner that the Division expanded the audit period from September 1, 2011 through November 30, 2015. The January 14, 2016 copy of the second IDR included the expanded audit period as the sales tax quarters being covered. A third IDR was also sent on January 14, 2016, requesting all of the records requested in the first IDR for the expanded audit period.

21. On March 11, 2016, the Division sent petitioner a fourth IDR, again requesting descriptions for the line item charges, including those that are available on petitioner's website. Petitioner directed the Division to the company's website for an explanation of the services they offer. Contracts, service level agreements, terms and conditions, and service descriptions relating to petitioner's service charges were not provided.

22. Petitioner ultimately provided the Division with a spreadsheet listing the categories of service petitioner provided, followed by a description of that service, and a link to petitioner's website for more information about the service. The categories included: professional service, log retention, monitoring, network intrusion detection/prevention, firewall, scanning, and threat intelligence information service. The professional service category was described as "[p]rofessional consulting services typically billed on the basis of time and expenses incurred." Log retention was described as the capturing and archiving of network events for future analysis by the customer. Monitoring and network intrusion detection/prevention were both described as "network monitoring services." The firewall service was described as "management, monitoring, and maintenance of network firewall." Scanning was described as "[s]canning of network to identify and isolate viruses, malware, or other potential threats." The threat intelligence

information service was described as "typically delivered in the form of periodic reports to client regarding threats."

23. In January, February and March of 2017, the Division sent three additional IDRs regarding the location of devices petitioner was servicing. Petitioner asserted that some of the devices it was servicing were being billed to New York addresses but were located outside of New York and were not subject to sales tax. The Division requested the IP address information for these devices.

24. The Division's review was split between customers with in-state addresses (in-state customers) and customers receiving services in-state but having billing addresses outside the State (out-of-state customers). Because some customers with billing addresses in New York had devices located outside of the state, the Division believed that there were customers where the bill was being sent to them in other states, but the devices were located in New York, and should be taxed.

25. Ultimately, the Division issued a separate assessment for in-state customers and out-of-state customers. On May 26, 2017, the Division issued to petitioner a notice of determination with assessment ID L-046509898, which asserted $1,098,799.27 in additional sales and use taxes due, plus interest, for the period September 1, 2011 through November 30, 2015, for petitioner's in-state customers. The Division's assessment was the result of a detailed review of petitioner's records.

26. After notice number L-046509898 was issued, petitioner provided the Division with additional IP address information for petitioner's in-state customers that had devices outside of New York despite being billed in New York and exemption certificates for two of petitioner's other customers. After reviewing the additional documentation, assessment L-046509898 was reduced to a total tax due of $932,892.50, plus interest.

27. Because petitioner did not provide the requested information regarding the IP addresses for petitioner's customers before the audit was closed, the Division used the sales information from petitioner for the sales billed to in-state customers and the reductions made on those sales for devices that were then shown to be located outside of New York, and calculated an error rate of 32.99%. The Division then multiplied the quarterly sales made to customers who were billed outside of New York by the 32.99% error rate for the entire audit period, to determine the calculated taxable sales and ultimately, the tax due on petitioner's sales to out-of-state customers. The Division issued a second notice of determination on May 26, 2017, with assessment ID L-046509501, assessing tax due for petitioner's customers who were billed outside of New York but who had devices in New York, for a total tax due of $12,352,700.56 plus interest.

28. After the assessment was issued, petitioner provided the Division with IP address information for its out-of-state customers. The tax was then recalculated using the total percentage of devices that were shown to be in New York for each customer, multiplied by the total charges for that customer, and that amount was deemed subject to tax. These adjustments resulted in the tax due being reduced from $12,352,700.56 to $215,394.04 for assessment L-046509501.

THE DETERMINATION OF THE ADMINISTRATIVE LAW JUDGE

The Administrative Law Judge began her determination by setting forth the section of the Tax Law imposing sales tax on the sale of protective and detective services. The Administrative Law Judge noted that while the words of the statute should be construed according to their plain meanings, where the words are ambiguous, other methods of determining legislative intent should be considered.

The Administrative Law Judge observed that because the Tax Law does not define protective or detective services, it is appropriate to look to statutes concerning the same subject matter. Turning to the General Business Law, the Administrative Law Judge adopted the definition of "watch, guard or patrol agency" for purposes of construing the meaning of protective and detective services. The Administrative Law Judge found the definition provided therein to be applicable to the protective and detective services in the Tax Law.

The Administrative Law Judge found petitioner's managing, monitoring and scanning services to be protective services subject to tax in that petitioner, based on its industry experience, configures policies for its customers' devices to prevent connections to its customers' networks by threat actors. Furthermore, petitioner tests patches and installs updates to its customers' devices to improve the level of protection afforded. According to the Administrative Law Judge, the purpose of these services is to protect or guard a customer's network from malicious activity, and thus such services are clearly subject to tax.

The Administrative Law Judge rejected the Division's argument that petitioner's management services are taxable information services, reasoning that petitioner's protective devices and configuration services did not involve the collection, compilation or analysis of information as contemplated under the Tax Law.

The Administrative Law Judge found petitioner's monitoring services to be taxable protective and detective services because such services entail reviewing and reporting of suspicious events on its customers' networks, notwithstanding petitioner's argument that such services do not amount to protective or detective services because it does not identify who is attempting unauthorized access. The Administrative Law Judge found that the statute imposed tax on services provided by alarm systems of every nature and found petitioner's monitoring services to be analogous. The Administrative Law Judge found such services to not qualify as

information services subject to tax, despite the Division's argument to contrary, as petitioner merely converted the information received from one form to another and did not add information to these events.

The Administrative Law Judge then discussed petitioner's vulnerability scanning service and targeted threat hunting service, which she also found to be taxable protective services. The Administrative Law Judge observed that petitioner notifies its clients of weaknesses in their networks that require remediation in providing its vulnerability scanning service. Similarly, the targeted threat hunting service searches for vulnerabilities in petitioner's customers' networks and endpoints and thus qualifies as a taxable protective service. The Administrative Law Judge also found these services to be integrated services, providing both protective services and information services, although their primary function is to protect the networks of its customers from security threats.

The Administrative Law Judge found that petitioner's resident security operations consisted of the same monitoring services previously found to be taxable protective services, differing in that such services have an on-site component. The Administrative Law Judge also found that petitioner failed to present evidence of the contract terms for these services and thus failed to demonstrate how these services were not subject to tax.

The Administrative Law Judge dismissed petitioner's interpretation of our decision in ***AlliedBarton Sec. Servs., LLC*** (Tax Appeals Tribunal, February 16, 2016), finding that petitioner's reading of the decision was too narrow. According to the Administrative Law Judge, ***AlliedBarton*** does not set down a rule that the only act that constitutes a protective or detective service is the guarding of property, and thus petitioner's reliance was misplaced.

The Administrative Law Judge found petitioner's threat intelligence service to be a taxable information service, as it adds information to basic data to provide a customer with

intelligence it did not previously have. She found that petitioner reviews and processes information gleaned from its customer's vulnerabilities, enriches that data with its knowledge, and furnishes reports of its findings to its customers. Similarly, the Administrative Law Judge found that its attacker database add-on service provided its customers with intelligence they did not previously have and thus constitutes a taxable information service.

Having concluded that these services were taxable information services, the Administrative Law Judge next considered whether such services were excluded from tax as being personal in nature and not substantially incorporated in reports furnished to other persons. The Administrative Law Judge found that the reports produced for these services are not unique to each customer and thus the threat intelligence services qualify as an information service subject to tax.

Turning to petitioner's enterprise brand surveillance, the Administrative Law Judge found that petitioner compiles reports of information gleaned from public sources based on keywords from its customers. The Administrative Law Judge noted that customization of publicly available information into a report does not render it personal or individual in nature, and thus concluded that such a service is a taxable information service.

Finally, the Administrative Law Judge considered petitioner's log retention service. She noted that log retention is not an enumerated taxable service under the Tax Law, and maintaining devices for retention of network events is not a protective service subject to tax. Because petitioner merely reports the events in the customer portal without adding any information, log retention does not qualify as a taxable information service either.

The Administrative Law Judge thus concluded that petitioner had demonstrated that its log retention services were nontaxable, but otherwise sustained the notices of determination.

ARGUMENTS ON EXCEPTION

On exception, petitioner argues that the Administrative Law Judge erred in holding that its monitoring and management services qualify as protective and detective services pursuant to Tax Law § 1105 (c) (8). As it did below, petitioner asserts that its monitoring services do not attempt to prevent unauthorized access to a customer's computer network, nor do such services try to identify the individuals attempting unauthorized access. Petitioner claims that our decision in ***AlliedBarton*** requires that a service must directly guard or protect persons or property in order to be deemed a taxable protective service under Tax Law § 1105 (c) (8). Petitioner asserts that its monitoring services are analogous to the hybrid reception service found not to be a taxable protective service in ***AlliedBarton***. Petitioner explicitly rejects the Division's comparison of its monitoring and management services to an alarm system, pointing out that alarm systems typically prevent unauthorized access, unlike its services, which report suspicious activity only after the fact. Similarly, petitioner argues that its management services merely consisted of applying device upgrades provided to its customers by the device manufacturers, and thus petitioner did not provide taxable protective and detective services within the meaning of Tax Law § 1105 (c) (8).[1]

The Division argues that the Administrative Law Judge correctly determined the issues presented at the hearing below and asks that the determination of the Administrative Law Judge be affirmed. It contends that the plain language of Tax Law § 1105 (c) (8) controls, which means that taxable protective and detective services include all services provided by protective systems of every nature, including alarm systems. According to the Division, taxable protective services include services intended to protect against unauthorized access or malicious activity

[1] Petitioner did not take an exception to the portion of the determination that held that certain services constituted taxable information services.

and also include monitoring for unauthorized access or vulnerabilities. Contrary to petitioner's argument, the Division posits that our decision in ***AlliedBarton*** does not limit taxable protective services to provision of security officers, but rather broadly encompasses alarm and protective systems of various types. Lastly, the Division reiterates that petitioner's resident security operations are generally similar to its monitoring services, differing only insofar that its own employees are on site to communicate with petitioner's customers, and thus taxable for the same reasons.

OPINION

Section 1105 (c) of the Tax Law imposes sales tax upon the provision of certain enumerated services. Included in such tax, as relevant here, are protective and detective services, described as follows:

> "[p]rotective and detective services, including, but not limited to, all services provided by or through alarm or protective systems of every nature, including, but not limited to, protection against burglary, theft, fire, water damage or any malfunction of industrial processes or any other malfunction of or damage to property or injury to persons, detective agencies, armored car services and guard, patrol and watchman services of every nature other than the performance of such services by a port watchman licensed by the waterfront commission of New York harbor, whether or not tangible personal property is transferred in conjunction therewith" (Tax Law § 1105 [c] [8]).

It is axiomatic that the plain language of a statute "is the clearest indicator of legislative intent and courts should construe unambiguous language to give effect to its plain meaning" (***Matter of the Walt Disney Co. and Consol. Subsidiaries***, Tax Appeals Tribunal, August 6, 2020, quoting ***Matter of DaimlerChrysler Corp. v Spitzer***, 7 NY3d 653, 660 [2006]; ***Matter of Watchtower Bible and Tract Socy. of New York, Inc.***, Tax Appeals Tribunal, July 16, 2020). In questions of statutory interpretation where, as here, the issue is the imposition of a tax, a statute cannot be read to allow the government to tax anything more than its clear terms allow (***see Matter of Grace v New York State Tax Commn.***, 37 NY2d 193, 196 [1975], ***lv denied*** 37 NY2d

816 [1975], ***appeal denied*** 338 NE2d 330 [1975]; ***Debevoise & Plimpton v New York State Dept. of Taxation & Fin.***, 80 NY2d 657 [1993]). Even with this construction, the burden to prove that the services at issue were not protective or detective services within the meaning of the statute remains with petitioner (Tax Law § 1132 [c] [1]).

As noted, Tax Law § 1105 (c) (8) broadly defines the services taxable thereunder as including "alarm or protective systems of every nature, including . . . protection against burglary, theft . . . or any other malfunction of or damage to property or injury to persons . . . ." In our view, such language plainly encompasses the IT security services at issue. We agree with the Administrative Law Judge that petitioner's managing, monitoring and scanning services, including managing and/or monitoring a firewall or integrated appliance, petitioner's AETD monitoring service, managing and/or monitoring IPS or IDS (including the iSensor), security event monitoring and log monitoring are protective services subject to sales tax.

In providing device management services (i.e. when managing firewalls, IPS/IDSs or integrated appliances), petitioner uses its experience in the industry and information collected from its customer base and other sources to configure those devices' security policies to prevent connections from outside threats. This constitutes preventing the theft or damage of property within the meaning of Tax Law § 1105 (c) (8). Additionally, petitioner protects its customers' networks by configuring these devices to create reportable events when certain outside connections are made. Petitioner's testing and patching of updates produced by the device manufacturers is done with the goal of helping its customers prevent the latest threats to their IT infrastructure.

Petitioner argues that managing these devices does not include actively and directly guarding or protecting its customers' IT infrastructures, but merely represents nontaxable consulting services advising its customers what steps they should take to protect their own

networks and endpoints. Petitioner claims this is comparable to the hybrid reception services at issue in ***AlliedBarton***, where we held that the reception services, consisting of checking identification of visitors and issuing temporary passes, did not qualify as taxable protection and detective services for purposes of Tax Law § 1105 (c) (8). We disagree. Our holding in ***AlliedBarton*** was not so narrow as to exclude services that do not actively and directly guard or protect property or persons. As observed by the Administrative Law Judge, while petitioner may not take overt action to block attempted connections by threat actors at the moment they occur, by configuring their customers' appliances to determine who is allowed access and maintaining them to ensure they are operational with the most current policies, petitioner is actively protecting and guarding its customers' networks from threats. The purpose of managing these devices and software is to protect or guard a customer's network from malicious activity. Therefore, we agree that such services are taxable protective services.

We also agree with the Administrative Law Judge that petitioner's monitoring services represent protective and detective services subject to tax pursuant to Tax Law § 1105 (c) (8). In monitoring firewalls, IDS/IPSs, and performing AETD services, security event monitoring, and log monitoring services, petitioner reviews the logged events and reports suspicious activity to its customers through its customer portal or by calling and notifying its customers of such activity. Petitioner argues that these monitoring services do not qualify as protective services because petitioner does not identify who is attempting the unauthorized access, does not stop the access and does not assess any of the damage that was done. However, petitioner's argument diminishes the import of the plain language of the statute, which imposes sales tax on "all services provided by or through alarm . . . systems of every nature" (Tax Law § 1105 [c] [8]). When petitioner reviews network events reported by the devices under its management with the purpose of notifying its customers when petitioner believes an event or events may be a threat to

its customers' networks, such review and notification is analogous to an alarm system within the meaning of Tax Law § 1105 (c) (8).

Turning next to petitioner's vulnerability scanning service and targeted threat hunting service, we agree with the Administrative Law Judge that these are integrated services in that both provide protective services together with an information component (***compare*** Tax Law §§ 1105 [c] [1] ***with*** [c] [8]). Petitioner's vulnerability scanning service, in addition to identifying specific exposures that pose risks to its customers, provides reports of insights and perspectives to answer its customers' questions and assists them in making security decisions. Similarly, petitioner's targeted threat hunting service searches for the presence of malware or evidence of threat actors and provides guidance where threat actors are found. Where a service is integrated, determining whether it is subject to tax requires assessing what the primary function of the service is in its entirety as opposed to reviewing the service by components or how the service is effectuated (***see Matter of SSOV '81 Ltd.***, Tax Appeals Tribunal, January 19, 1995). Clearly, the primary function of both of these services is to protect its clients' networks from malicious activity. The information services provided by petitioner to its customers in performing these services are incidental aspects of the protective services and thus represent taxable protective services for purposes of Tax Law § 1105 (c) (8).

Petitioner's incident response service is also a protective and detective service subject to tax. This service entails petitioner analyzing, containing and helping its customer recover from a breach of the customer's IT infrastructure. As noted by the Administrative Law Judge, petitioner's containing of the breach prevents it from spreading to more of a customer's network. Analyzing and containing the breach constitutes a protective service within the meaning of Tax Law § 1105 (c) (8).

Petitioner's resident security operations service is customized according to the customer's needs. The service was described by petitioner at the hearing as being generally similar to its monitoring service, except that petitioner's employee is stationed on-site at the customer's location to monitor the events created by the various systems and receive phone calls from petitioner regarding events. Additionally, we note that relevant resident security operations contracts were not made a part of the record at the hearing below. Petitioner has thus failed to meet its burden of establishing that its resident security operations services were not protective and detective services subject to tax (***see*** Tax Law § 1132 [c] [1]).

Accordingly, it is ORDERED, ADJUDGED and DECREED that:

1. The exception of Secureworks, Inc., is denied;

2. The determination of the Administrative Law Judge is affirmed;

3. The petitions of Secureworks, Inc., are granted to the extent indicated in the determination of the Administrative Law Judge, but are otherwise denied; and

4. The notices of determination dated May 26, 2017, as modified by the determination of the Administrative Law Judge, are sustained.

DATED: Albany, New York
February 17, 2021

/s/ Anthony Giardina
Anthony Giardina
President

/s/ Dierdre K. Scozzafava
Dierdre K. Scozzafava
Commissioner

/s/ Cynthia M. Monaco
Cynthia M. Monaco
Commissioner