Clear Skies for Cloudy Cybersecurity

May 29, 2018

ABSTRACT: Contrary to popular belief, most public cloud services companies don't guarantee data asset security. This worrisome detail hasn't stemmed enterprises' adoption of cloud services, even though their cybersecurity tools are still rooted on-premise. But on-premise tools are ineffective in public clouds, and even less so when tools from different vendors are stacked together. One company has remedied this impasse: Backed by a Silicon Valley management team that has had several exits, Sophic Capital client Nubeva (NBVA:TSXV) has a blockchain solution that bridges the enterprise disconnect between on-premise cybersecurity tools and public cloud use. It's a solution that's generating revenue from Fortune 500 clients, and there are no direct competitors. Nubeva's executive team has decades of cybersecurity and network experience, the Company's balance sheet is solid on the back of a C$10 million financing, and two high-profile NASDAQ cybersecurity IPOs along with a wave of industry consolidation have shifted investor interest into this space. Cybersecurity and blockchain are timely investment themes, and Nubeva is a public investment vehicle that couples both.

Sean Peasgood, President & CEO

Gareth Tingling, Vice President

Marcel Valentin, Vice President

www.SophicCapital.com, (647) 697-0498

Subscribe at bit.ly/2s8qnZo

Why You Need to Read this Report

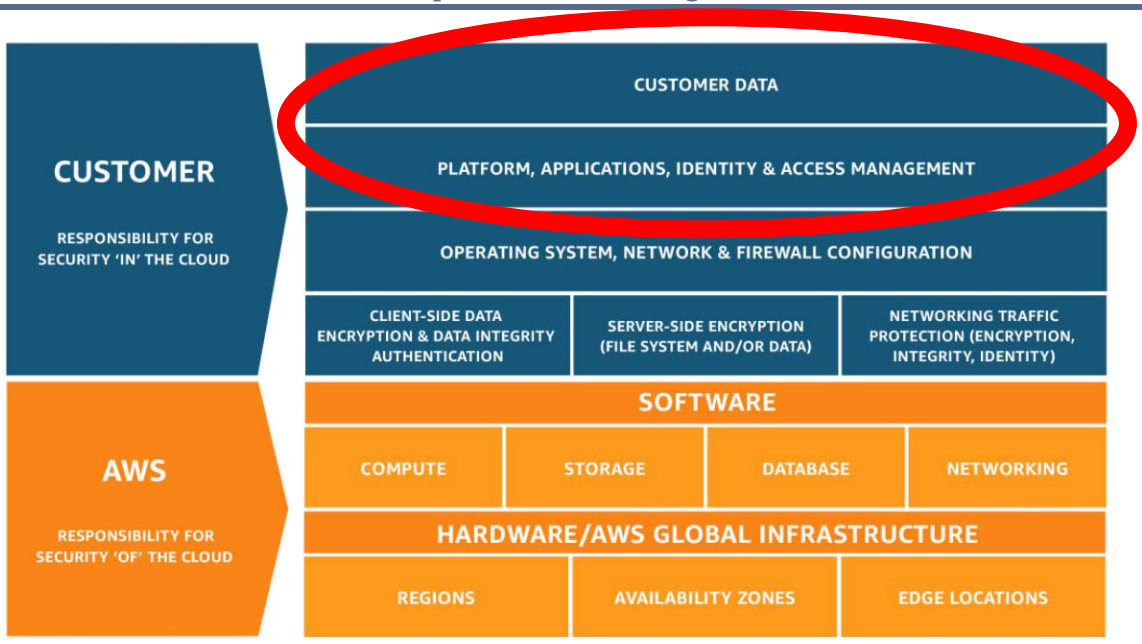
1. Enterprises are losing the battle to protect public cloud data;
2. Cybersecurity is crucial but lacking as enterprises move to cloud services;
3. Two NASDAQ cybersecurity IPOs have refocused investors on the industry;
4. See some of the 200 M&A cybersecurity transactions that occurred in 2017;
5. Sophic client Nubeva (NBVA:TSXV) has a revenue-generating blockchain cybersecurity solution that minimizes cloud cybersecurity threats by enabling best-of-breed tools.

Introduction

Although enterprises are transitioning their data centers, storage, and applications to public clouds, their cybersecurity tools remain on-premise. "So what?" you may ask; "Amazon AWS and Microsoft Azure will protect my company's data assets." Many investors may be surprised to learn that cloud service providers like AWS and Azure do *not* guarantee data security (**Exhibit 1**). With high-profile data breaches harming brand equity at Fortune 500 companies and increasing legislation protecting personal data, enterprises are scrambling to stem the attacks.

Nubeva (NBVA:TSXV), a Sophic Capital client, provides software that enables best-of-breed cybersecurity tools in public clouds. Backed by an experienced Silicon Valley team that has sold companies for several billion-dollars, a solid balance sheet strengthened by a recent C$10 million financing, no direct competitors, and partnerships with industry leaders, we believe that Nubeva is well positioned to potentially become the *de facto* solution to secure public cloud assets for enterprises.

Exhibit 1: Cloud Customers are Responsible for Securing their Own Cloud Data



Source: AWS

Enterprises Can't Contain Cyber Threats

Cybersecurity is the protection of digital assets from digital attacks and thefts. This can range from providing asset management solutions that know who has what asset and where that asset is at any given time, to installing a stack of security tools to limit internal and external access to an enterprise's data and information systems.

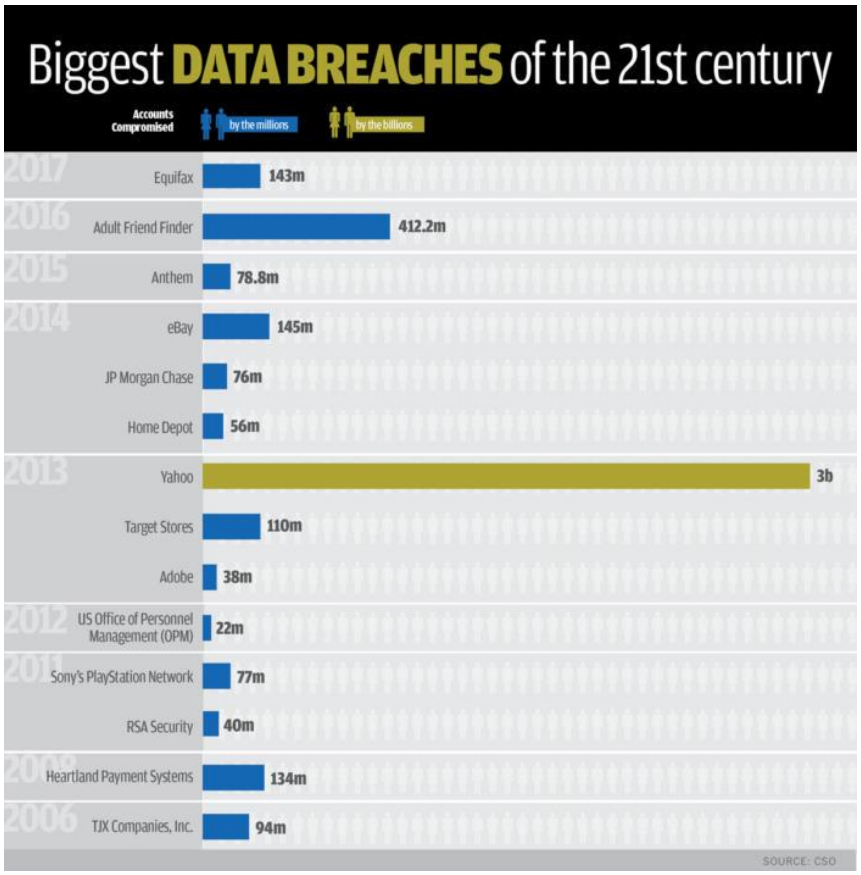
Although we'd like to believe that enterprises safeguard our personal data, this typically isn't the case. Exhibit 2 illustrates that even many Fortune 500 companies can't stem malicious attacks. One primary reason is that enterprises are moving their operations to the cloud in an effort to focus on their core competencies instead of owning and managing data centers, storage, and applications (Exhibit 3), and on-premise security tools don't work well in public clouds. Another reason is that workers are mobile, and their work tools (smartphones, tables, home offices) act as vulnerable endpoints that hackers can exploit to unlawfully access on-premise and/or cloud-based data centers.

No company wants to endure the wrath of angry customers, especially when breaches have to be publicly acknowledged. Financial penalties can be onerous when cyber breaches occur. In Yahoo!'s case, Verizon got a $350 million discount from its original $4.8 billion offer for the Internet company's core business. Heartland Payment Systems, a credit and debit card payment processor, paid an estimated $145 million for fraudulent payments and wasn't allowed to process major credit cards for about 14 months. Target's CIO and CEO resigned due to the $162 million (estimated) breach. And Uber's coverup partially contributed to a $20 billion decrease in valuation to $48 billion when the Softbank deal closed in December 2017.

Cloud Providers Aren't Responsible for your Data Assets

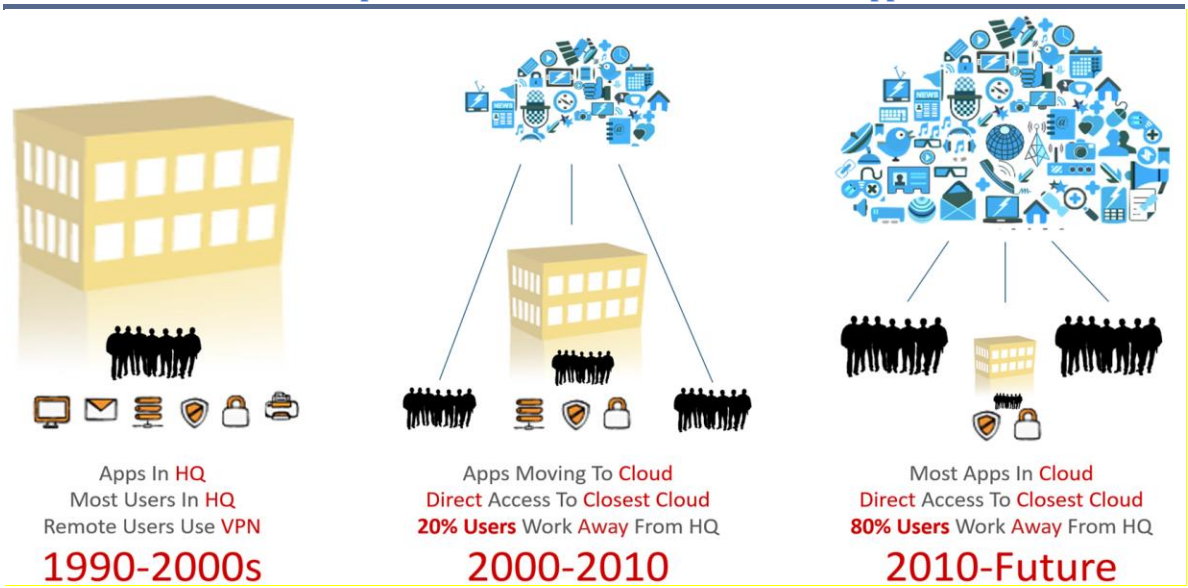
When moving data, systems, storage, and applications to the cloud, security becomes a shared responsibility between you and the cloud service provider. For example, Exhibit 1 shows Amazon AWS's policy concerning data security. "Security *of* the cloud" relates to AWS's measures for securing the underlying infrastructure that supports the cloud - that's their responsibility. Cloud customers are responsible for "security *in* the cloud" – the digital asset put into the cloud and how connections are made to the cloud. That might not sound like a big deal until you realize that until Sophic client Nubeva tackled the problem, tools didn't exist for enterprises to secure their assets in public clouds.

Exhibit 2: The Largest Reported Data Breaches



Source: CSO

Exhibit 3: Timeline of Enterprise Transition to Cloud Services and Applications



Source: Nubeva

Existing Security Tools Don't Work Well in the Cloud

Although enterprises are transitioning their data centers, storage, and applications to public clouds, cybersecurity tools remain (for the most-part) on-premise. That is, enterprises cannot effectively use their cybersecurity tools to route or monitor their data as traffic flows through public clouds unless their tools undergo extensive and expensive reconfiguration. And even after on-premise tools are reconfigured, enterprises won't have complete visibility and protection.

Enterprises lose visibility into, and some control of, traffic when data assets and applications move to public clouds. By outsourcing part of their operations to cloud providers, enterprises effectively give control of the routing of the traffic to the cloud providers. Traffic consists of tiny pieces of data called "**packets**" which are fundamental to everything we do on the Internet, on our corporate networks, and cloud usage. And most threats on-premise and in the cloud are hidden in packet data. For this reason, it is important for enterprises to monitor traffic, something that is not easily done through public clouds.

Securing on-premise data assets is straightforward and effective. Typically, enterprises will connect a series of tools from providers such as Palo Alto Networks (PANW:NYSE), Cisco (CSCO:NASDAQ), or FireEye (FEYE:NASDAQ) to act as a gatekeeper to data flowing in-and-out of and throughout the enterprise. These interconnected tools (collectively referred to as a "**security stack**") pretend to be on-premise data assets, to thwart external attacks. Enterprises deploy security stack components at strategic points within the network, and direct traffic to them as required. Enterprises also use something called "**Layer-2 impersonation**" to impersonate the enterprise data assets. For example, a hacker may believe she is communicating with an enterprise's data base when in actuality a security tool has intercepted the unauthorized communications and "pretends" to be the data base in order to protect the assets.

To connect to public clouds, enterprises can route all traffic through the on-premise security stack (also called "backhauling"). However, with enterprises constantly adding new devices ("**endpoints**") such as mobile phones and tablets, backhauling increases traffic and slows down access to on-premise and cloud resources.

A public cloud's entire customer base shares all the hardware. Given this, it's not possible to physically connect hardware in a public cloud data center to gain on-premise benefits. As well, most of layer-2 functionality is not exposed for customer use and modification in the public cloud. None of the major public cloud vendors have indicated any desire to add Layer-2 impersonation. We believe this is because:

a) their agreements stipulate that they aren't responsible for securing enterprise data assets;

b) their focus is primarily on adding Software-as-a-Service (SaaS)-revenue-generating tools, especially in artificial intelligence, and;

c) although beyond the scope of this report, enabling Layer-2 impersonation would allow all public cloud users to hack and impersonate since all users use the same data center.

Lack of Public Cloud Security Tools Isn't Stopping the Migration

According to McKinsey & Company, only 11% of enterprises transitioning to public clouds stated they are likely to backhaul their traffic three years from now. The McKinsey & Company report claims that backhauling is seen as a temporary solution and suggests that 47% of companies transitioning to public cloud plan to use a virtual perimeter and develop cloud-specific controls (also known as "**cleansheeting**") within three years. Cleansheeting is expensive but allows corporate endpoints to connect directly to the cloud without routing through an on-premise security stack.

CyberSecurity is Paramount for Cryptocurrencies

Cryptocurrencies are an asset class worth a combined US$386 billion. Given the size of the asset class, hackers are targeting this evolving and generally unsecure ecosystem of exchanges and wallets. In 2016, The DAO saw 3.6 million Ether worth about US$70 stolen over a few hours. Mt. Gox was hacked not once but twice, and the second theft saw US$473 million of Bitcoin (about 7% of the total coins in circulation) vanish. As we wrote in our December 2017 *Thoughts from North America's Largest Blockchain Expo* report "*Just because someone can code, doesn't mean he knows how to write blockchain applications, or she's a cybersecurity expert*." In fact, two cybersecurity experts hired to vet ICOs for an investment fund shared that for every 50 ICOs they scrutinize, only 1 is secure. Cybersecurity is a real issue in the crypto space, and one that must be resolved for many institutions to invest in this asset class.

Pick Your Number – Cybersecurity Spending is Big

Several independent third-parties have forecasted large global cybersecurity spends. These estimates encompass the entire cybersecurity market, not just email communications. We can't tell you which estimate is correct, but the takeaway is that the estimates are big. Consider these third-party estimates:

- Gartner estimated that global cybersecurity spending would reach US$90 billion in 2017 and grow to US$113 billion by 2020;
- Research firm IDC forecasted that 2016 cybersecurity spend would grow at an 8.6% CAGR to US$101 billion in 2020;
- Cybersecurity Ventures, a cybersecurity market intelligence firm, predicts US$1 *trillion* in cybersecurity spending from 2017 through 2021;
- B2B research firm MarketsandMarkets believes the cybersecurity market could grow from US$137.85 billion in 2017 to U$231.94 billion by 2022.

The U.S. Federal Government has significantly increased its spending on cybersecurity investment. The 2017 U.S. Budget increased cybersecurity spending 35% year-over-year to US$19 billion.

Governments Mandating Personal Data Protection

Sharing personal information is fraught with liabilities. The onus is upon enterprises to protect customer, employee, and data. More and more, this onus extends to jurisdictions where enterprises are not domiciled but conduct business and even communicate. Countries are enacting laws to penalize companies for poor cybersecurity. These laws include:

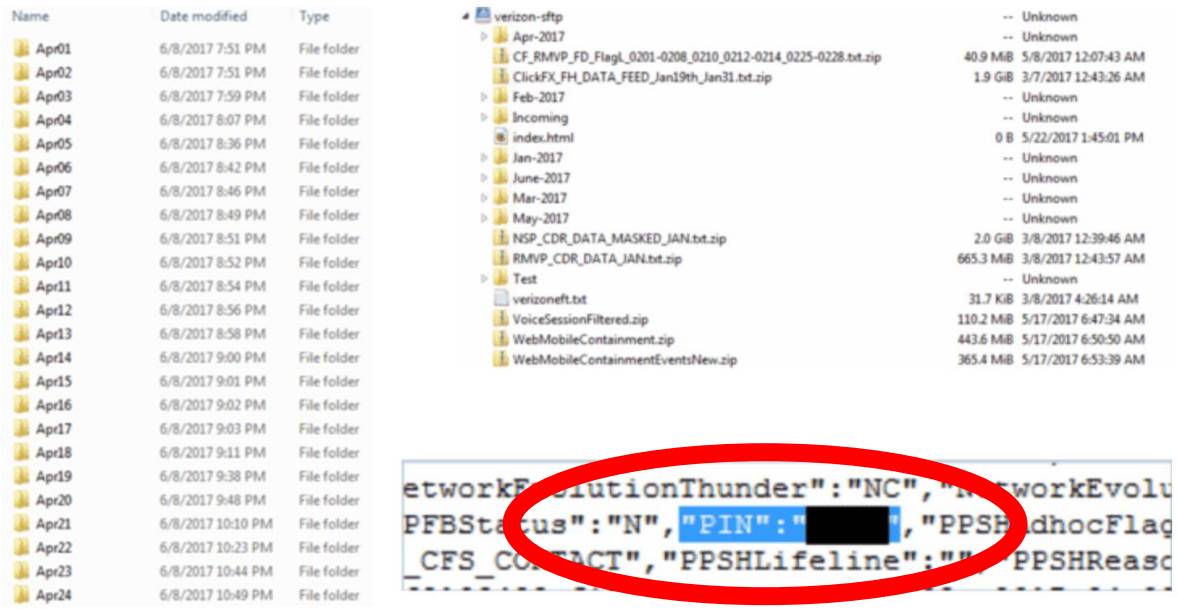
On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) came into effect to protect the data and privacy of citizens. Organizations, both European and non-European, breaching GDPR can be fined up to the greater of 4% of annual global turnover or €20 million. A company can be fined 2% for not having their records in order, not notifying the supervising authority and data subject within 72 hours of a breach, or not conducting impact assessment. Cloud providers are not exempt from GDPR regulations.

Although the United States doesn't have a comprehensive national law like GDPR that regulates the collection and use of personal data, there are some federal privacy laws. Some of these laws include:

- **The Health Insurance Portability and Accountability Act (HIPAA) sets national standards to protect medical information.** The U.S. Department of Health and Human Services can levy fines ranging from $100 to $1.5 million for violations. Some violations can carry up to 10-year prison terms.
- **The Financial Services Modernization Act regulates the collection, use and disclosure of financial information.**
- **The Federal Trade Commission Act prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies.**

As Exhibit 4 illustrates, attackers are sometimes easily able to access personal data. It doesn't matter whether data is stored on-premise or in public clouds; hackers can find a way to get it. And once attackers obtain legitimate user names and passwords, they get access to corporate info and systems and personal data. The onus is on enterprises to secure user data or risk penalties.

Exhibit 4: 1 of 14 million Verizon account PIN codes hacked after a 3rd-party vendor left them exposed on an Amazon S3 cloud server



Source: The Hacker News

Cybersecurity Industry is Consolidating

…consolidating in a BIG way. It almost seems that cybersecurity mergers and acquisition (**M&A**) activity occurs on a daily basis. In 2017 alone, there were over 200 cybersecurity M&A deals. Exhibit 5 shows ***some*** of the more notable take-outs.

Exhibit 5: M&A is Rampant in the Security Space

Date	Acquirer	Target	Deal Size (US$MM)	Total Target Funding (US$MM)*
Dec. 24, 2017	Amazon	Blink	N/A	$5.8
Dec. 21, 2017	Mercury Systems	Themis Computer	$180	$5.3
Dec. 17, 2017	Thales	Gemalto	$5,430	N/A
Dec. 15, 2017	StarHub	D'Crypt	$90	N/A
Nov. 29, 2017	Proofpoint	Weblife.io	$60	N/A
Nov. 28, 2017	Thoma Bravo	Barracuda Networks	$1,600	$121.0
Nov. 15, 2017	K1 Capital Management	Actiance	$100	$43.6
Nov. 7, 2017	Proofpoint	Cloudmark	$110	$39.0
Nov. 3, 2017	Continental A	Argus Cyber Security	$400	$25.1
Nov. 2, 2017	Synopsis	Black Duck Software	$565	$75.5
Oct. 31, 2017	DigitCert	Symantec website security business	$950 +30% DigiCert Stock	N/A
Sept. 27, 2017	SAP	Gigya	$350	$106.0
Sept. 17, 2017	Mantech International	infoZen	$180	N /A
Sept. 1, 2017	Microfocus	HPE's IT Management	$8,800	N /A
July 27, 2017	Open Text	Guidance Software	$240	$65
July 18, 2017	Rapid7	Komand	$50	$1.3
June 7, 2017	Fingerprint Cards	Delta ID	$113	$15.1
May 31, 2017	Gemalto	3M's ID management business	$850	N/A
May 26, 2017	Vector Capital	Sandvine	C$562	$63.0
May 24, 2017	Microsoft	Hexadite	$100	$10.5
May 11, 2017	CyberArk Software	Conjur	$42	$2.6
April 19, 2017	Advent International	Morpho	$2,700	N/A
March 13, 2017	Intel	Mobileye	$15,300	$515
March 7, 2017	CA Technologies	Veracode	$614	$114
Feb. 28, 2017	Palo Alto Networks	LightCyber	$100	$36.5
Feb. 8, 2017	Sophos	Invincea	$100	$55.5
Jan. 17, 2017	Auxilio	CynergisTek	$34.3	N/A
Jan. 9, 2017	Amazon Web Services	Harvest.ai	$19	$2.8
Jan. 9, 2017	LLR Partners	BluVector	$50	N/A

* Crunchbase.com

Source: Company reports, Crunchbase

Industry Leaders

IBM Security

Under its parent IBM (IBM:NYSE), IBM Security delivers enterprise security intelligence, integration, and expertise to protect businesses from cyber security threats. In addition, it protects critical business and client information against breaches and enables organizations to effectively manage risk and defend against emerging threats. IBM Security operates one of the world's broadest security research/development/ delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Cisco

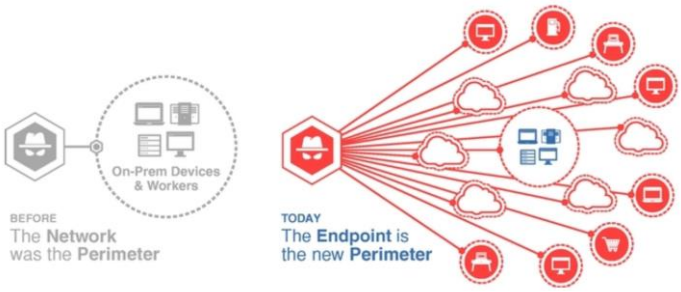
Cisco (CSCO:NASDAQ) designs and sells a broad range of technologies that have been powering the Internet since 1984. The Company's products deliver effective network security and incident response by integrating a comprehensive portfolio of security technologies that include: next-generation firewalls, intrusion prevention systems, secure access systems, security analytics, and malware defense. The company offers web and email security, network security, and cloud security. All of Cisco's technology is supported with in-depth threat and malware intelligence to keep ahead of the latest cyber-attacks.

Cato Networks

Cato Networks (private) is building the new Software-defined wide-area network (WAN), in the cloud, protected by a tightly integrated set of security services. The Cato Cloud connects all business endpoints including data centers, branches, mobile users and cloud infrastructure into a simple, secure and unified global network without expensive connectivity services, complex point solution deployments, capacity constraints, maintenance overhead, or restricted visibility and control.

Carbon Black

Carbon Black (CBLK:NASDAQ) is an endpoint cybersecurity company that leverages the big data, analytics, and the cloud to transform security and turn the tables on attackers. The company's technology ingests unfiltered endpoint data in real-time and gives its customers a comprehensive view of everything occurring. Carbon black also applies advanced "streaming analytics" to predict and prevent attacks that lie hidden within systems, including attack methods that have never been seen before. Carbon Black completed its initial public offering on May 4, 2018 and closed the first day of trading with a US$1.4 billion enterprise value.



Carbon Black's predictive security cloud platform continuously captures, records and analyzes unfiltered endpoint data

Zscaler

Zscaler (ZS:NASDAQ) was founded in 2008 to develop a security solution that leverages the company's private cloud network. Zscaler provides an architectural approach to secure IT transformation, the backbone of which is a security cloud spread over 100 data centers. The company's ZIA solution securely connects users to externally managed applications, including SaaS applications and internet destinations, regardless of device, location or network. ZIA lies between users and the internet, safeguarding users from malware and preventing corporate data from leaking out. Zscaler's other offering, ZPA, offers authorized users secure and fast access to internally managed applications hosted in enterprise data centers or the public cloud. ZPA does not expose the identity or location of these applications and provides only the necessary and appropriate levels of access. While traditional remote access solutions, such as VPNs, connect a user to the corporate network, the ZPA solution connects a specific user to a specific application, without bringing the user on the network, resulting in better security. Zscaler started trading on the NASDAQ on March 16, 2018 and has a US$3.3 billion enterprise value.

Zscaler routes users to the Internet, on-premise data centers, and public clouds via the Company's security cloud which is deployed across 100 data centers

Nubeva – Enabling Best-of-Breed Cybersecurity in Public Clouds

Nubeva (NBVA:TSXV), a Sophic Capital client, is a San Jose, California-based company that develops software that uses Blockchain Routing to accelerate migration to public Azure and AWS clouds. Although enterprises are moving their data, databases, and operations to the cloud, their cybersecurity is stuck on-premises. Nubeva has a solution that bridges premise and cloud operations.

Nubeva launched StratusEdge, its proprietary cloud-based security delivery platform that monitors and provides visibility into public cloud traffic. Unlike on-premise data centers, public clouds don't allow enterprises to control physical infrastructure - enterprises can only control basic routing, giving little visibility and control about traffic and connectivity since there are no predictive paths for traffic to follow. StratusEdge creates predictive paths for enterprise traffic.

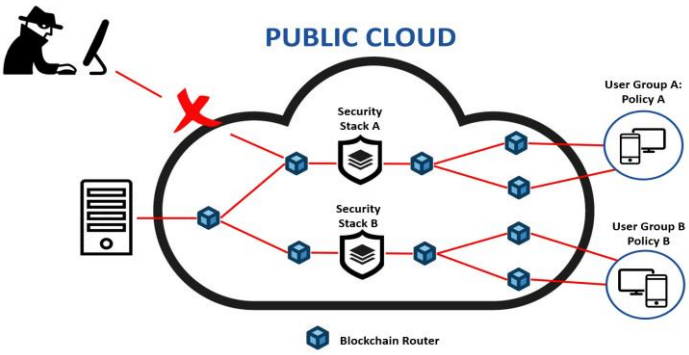
Technology Differentiator

Nubeva's StratusEdge is designed to work with best-of-breed solution providers. Most enterprises don't source their security tools from a single source. For example, an enterprise won't exclusively have Cisco gear; instead, the firm will likely use a combination of tools, say, Cisco, Palo Alto, and Blue Coat (which was acquired by Symantec in 2016 for US$4.65 billion in cash). As mentioned, enterprises historically could not physically wire their security tools in a public cloud data center. Nor could enterprises utilize Layer-2 impersonation to protect their public cloud assets.

They couldn't until Nubeva's StratusEdge came along with a technology called blockchain routing.

Blockchain routing is key differentiator for Nubeva. StratusEdge programs each public cloud route used by an enterprise – from user to destination - and then forms a blockchain on the routing tables created. Blockchain routing does this by inspecting packets to ensure they contain the correct routing information – otherwise, the packet is rejected. This also creates audit trails, providing visibility on how traffic routes through the public cloud and what connections are made. Audit trails are the same diagnostic information that enterprises use for their on-premise data centers.

Nubeva's StratusEdge allows enterprises to leverage their on-premise security stack. Blockchain routing allows packet routing within the security stack. This virtually moves on-premise security tools into the cloud, regardless of what tools enterprises use. This helps enterprises to effectively transition their data assets and applications to public clouds.



Nubeva's blockchain routing provides predictive paths in public clouds without compromising security stack tools

No Data Centers to Scale

Unlike Zscaler, Nubeva doesn't have to build data centers. When AWS and Azure add new data centers, this benefits Nubeva without any cost. Nubeva doesn't have to manage maintenance or expansion of public clouds but reaps the benefits of public cloud expansion roadmaps.

Experienced Silicon Valley Management

Nubeva's management team has over 80 years of cybersecurity, cloud, networking, storage, and blockchain experience and have had led several prior companies through successful billion dollar exits. CEO Randy Chou was co-founder and CEO of privately-held Panzura, a cloud network attach storage company. Mr. Chou, CTO Greg Bannister, and CMO Steve Perkins are Aruba alumni, which was sold to HP for US$3.0 billion. CFO Juliet Jones has held prior CFO positions at publicly-listed, Canadian technology companies.

Nubeva entered into an agreement on May 15, 2017 with Optiv, a North American security reseller with annual revenues in excess of US$ 2.5 billion, for Optiv to sell StratusEdge under the Optiv brand, powered by Nubeva. CMO Steve Perkins was the CMO of Optiv – he left in December 2016 and joined Nubeva in January 2017.

Conclusion

Cloud cybersecurity is a real problem with real financial and reputational consequences for enterprises. Enterprises are moving their data assets to unsecured public clouds; however enterprise cybersecurity remains on-premise. Nubeva (NBVA:TSXV), a Sophic Capital client, has a unique blockchain-based cybersecurity solution that bridges on-premise security to cloud data assets and applications. Nubeva's solution is tool vendor agnostic, meaning it works with the major network vendors such as Cisco and Palo Alto networks. The cybersecurity industry is hot, with consolidation rapidly accelerating. With a solid balance sheet, no direct competitors, and a low-cost SaaS model, we believe Nubeva will capture a large piece of the growing, multi-hundred billion dollar cybersecurity industry.

Acronyms Used in this Report

IPO	Initial Public Offering
M&A	Merger and Acquisition
WAN	wide-area network

Disclaimers

The information and recommendations made available here through our emails, newsletters, website, press releases, collectively considered as ("Material") by Sophic Capital Inc. ("Sophic" or "Company") is for informational purposes only and shall not be used or construed as an offer to sell or be used as a solicitation of an offer to buy any services or securities. You hereby acknowledge that any reliance upon any Materials shall be at your sole risk. In particular, none of the information provided in our monthly newsletter and emails or any other Material should be viewed as an invite, and/or induce or encourage any person to make any kind of investment decision. The recommendations and information provided in our Material are not tailored to the needs of particular persons and may not be appropriate for you depending on your financial position or investment goals or needs. You should apply your own judgment in making any use of the information provided in the Company's Material, especially as the basis for any investment decisions. Securities or other investments referred to in the Materials may not be suitable for you and you should not make any kind of investment decision in relation to them without first obtaining independent investment advice from a qualified and registered investment advisor. You further agree that neither Sophic, its employees, affiliates consultants, and/or clients will be liable for any losses or liabilities that may be occasioned as a result of the information provided in any of the Company's Material. By accessing Sophic's website and signing up to receive the Company's monthly newsletter or any other Material, you accept and agree to be bound by and comply with the terms and conditions set out herein. If you do not accept and agree to the terms, you should not use the Company's website or accept the terms and conditions associated to the newsletter signup. Sophic is not registered as an adviser under the securities legislation of any jurisdiction of Canada and provides Material on behalf of its clients pursuant to an exemption from the registration requirements that is available in respect of generic advice. In no event will Sophic be responsible or liable to you or any other party for any damages of any kind arising out of or relating to the use of, misuse of and/or inability to use the Company's website or Material. The information is directed only at persons resident in Canada. The Company's Material or the information provided in the Material shall not in any form constitute as an offer or solicitation to anyone in the United States of America or any jurisdiction where such offer or solicitation is not authorized or to any person to whom it is unlawful to make such a solicitation. If you choose to access Sophic's website and/or have signed up to receive the Company's monthly newsletter or any other Material, you acknowledge that the information in the Material is intended for use by persons resident in Canada only. Sophic is not an investment advisory, and Material provided by Sophic shall not be used to make investment decisions. Information provided in the Company's Material is often opinionated and should be considered for information purposes only. No stock exchange anywhere has approved or disapproved of the information contained herein. There is no express or implied solicitation to buy or sell securities. Sophic and/or its principals and employees may have positions in the stocks mentioned in the Company's Material, and may trade in the stocks mentioned in the Material. Do not consider buying or selling any stock without conducting your own due diligence and/or without obtaining independent investment advice from a qualified and registered investment advisor.