G00298567

Cool Vendors in Communications Service Provider Security Solutions, 2016

Published: 20 April 2016

Analyst(s): Deborah Kish, Akshay K. Sharma

Communications service providers are struggling to effectively compete with cloud-based providers and maintain revenue streams. New vendors are emerging with robust network security solutions and services that CSP CIOs and CTOs should seek out to develop new revenue streams and reduce churn.

Key Findings

- The vendor landscape continues to grow and has become crowded with consolidation expected to continue between cloud access security brokers and data loss prevention providers.
- New data security and encryption offerings are evolving to protect the network and customer data, and provide security as a service.
- Vendors can use older methodologies and algorithms, but the secret sauce is in proprietary technologies for achieving successful execution.

Recommendations

- Evaluate the capabilities of these cool vendors and lock in medium-term contracts with minor vendors now to achieve advantage later when these players are merged.
- Explore new security data and threat analysis offerings that can be leveraged to provide security as a service.
- Add private WAN encryption to your communications service provider portfolio of security offerings since security of data in motion is becoming more common and the cost of doing it is declining.

Table of Contents

Analysis

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

What You Need to Know

There is never a dull moment in the security space, and new vendors continue to erupt with new software-based products that aim to solve a variety of security issues faced by CSPs and end users. These Cool Vendors, however vast in terms of problems to solve for, have piqued our interest with either new ways of performing old techniques to reduce known pain points and aggravation in consumer and end-user markets. They are providers with less than $100 million in annual revenue and are chosen because of their transformative nature, newness, business models, and how their technology is used in terms of ease of configuration, helpfulness in solving a problem and cost-effectiveness.

The overall market for security products and solutions is extremely dense and, while we expect consolidation to occur, the notion of delivering software-based solutions through virtualization will accelerate the acquisition track. CSPs are moving toward software-defined networks to help reduce costs and provision services more rapidly, and give their customers multiple choices for different security services. The vendors in this report offer software-based products that can be easily provisioned to consumer and end-user markets as part of managed security services or as subscription-based new revenue streams.

As CSPs move toward software-defined networks (SDNs) and network function virtualization (NFV) architectures, network and data security will be a significant focal point and a major part of the transition. The technology providers featured are using SDN-ready solutions and cloud-delivery models to offer these platforms, which may help ease implementation and save time and effort.

These innovative vendors are on the cutting edge, and may not necessarily be market-proven or have long-term viability as startups and early ventures. However, they possess either proprietary algorithms or technologies that will be useful in fighting off the threat landscape or automation within their product set. The potential for acquisition is high, therefore it is important to take advantage of shortened contracts before they become part of a larger organization.

Identity Finder

New York, New York (www.identityfinder.com)

Analysis by Deborah Kish

Why Cool: For CSPs, Identity Finder can help their enterprise customers understand and minimize their risk exposure by locating and classifying personal identifiable information (PII), Protected Health Information (PHI), payment card industry (PCI) data, unique intellectual property and, more importantly, assist with knowing what the footprint of CPNI (Customer Proprietary Network Information) in their environment looks like. These steps in discovering and classifying sensitive data can be an instrumental part the process of staying compliant, and also securing the data from misuse, abuse, leaks and privacy concerns.

Identity Finder offers data management software that reduces an organization's sensitive data footprint. The product has capabilities such as network crawls in order to accurately discover where sensitive unstructured data resides (file shares, email servers, and cloud storage services such as Box, Dropbox, OneDrive etc.), without the false positives, and users can then apply classification to files and monitoring. This major differentiator allows its open platform to enable security technologies that most organizations already own to act on sensitive data and protect against sensitive data breaches. If documents or files that previously did not contain "Level 1" or "Confidential" sensitivity are manipulated to the extent that it does, automated reclassification is applied based on rules and policies. In turn, other products, such as DLP, can block classified files the organization now knows it needs blocked.

Identity Finder is forming partnerships with well-known data security vendors so that customers can discover, classify and monitor sensitive data with SDM and protect it with endpoint security and DLP products. Recently, Identity Finder joined McAfee/Intel Security Innovation Alliance as a Sales Teaming Partner (STP). For example, McAfee Host and Network DLP can automatically block the transit of data that customers classify. The combined solution provides customers the benefit of an integrated solution that protects sensitive data from cradle to grave.

Its product, Sensitive Data Manager, comes in two parts:

- The SDM Console provides administrators with a centralized way of managing policies organizationwide, and also allows them to schedule and review aggregated results of previous scans and real-time analysis of data being monitored.
- The SDM Endpoint is installed on clients where it monitors existing files on the machine or scans based on a schedule and also automatically classifies new files as soon as they are created. The SDM Endpoint can act as an agent/service monitoring a local file system or be deployed agentlessly to scan or monitor a remote file system, such as a multiterabyte NAS or file server.

SDM's current version increases automation of classification and data loss prevention (DLP) security controls, extending to cloud environments to manage sensitive data. The addition of user-driven data classification also allows organizations to take a hybrid approach to integrated DLP management, enabling them to leverage both automated and manual classifications.

Identity Finder has been named as an ISACA (Information Systems Audit and Control Association) partner for developing frameworks and to be part of the certification platforms for IT audit, security, governance and risk certification program. This is good for a new, smaller vendor, as it shows that it can be part of the value chain in a variety of use cases.

Challenges: Competition from larger, well-known data security vendors, such as Symantec, McAfee/Intel Security, Digital Guardian and Microsoft, may prove to be challenging. Also, as the data security vendor landscape has become crowded, consolidation is expected to increase in the coming years. For example, Microsoft acquiring Secure Islands, and now having its own user-driven data classification capabilities as well as its existing Microsoft Classification Infrastructure, may leave vendors such as Identity Finder (and other vendors of similar size) with difficulty in gaining visibility. Identity Finder will need to continue to increase its partnerships and expand the ecosystem with complimentary solutions outside of its home base of North America to gain more visibility from CSPs and the enterprise, globally.

Who Should Care: Board Members, CIOs, and CISOs; CTOs and product managers at CSPs; enterprises looking for managed security services and, essentially, any business that is interested in locating and classifying PII and PCI, and that need to comply with regulatory mandates.

InteliSecure

Greenwood Village, Colorado (www.intelisecure.com)

Analysis by Deborah Kish

Why Cool: InteliSecure is cool because its consultants thoroughly evaluate and define each customer's critical assets and where they reside, then determining how it should best be protected from when it's created, to when it's consumed and transmitted. Then, the InteliSecure technical team builds and customizes the needed policies into security platforms at customer sites, managing the whole package. Its vendor-agnostic approach allows it to be flexible for its customers that have invested in existing technology, and it is currently expanding the list of security products it will support.

InteliSecure is a managed security service provider (MSSP) that offers a hybrid application — human intelligence and its critical asset protection program — via its Enigma Intelligence Platform (EIP) that is based on the ISO 27000 methodology. It integrates with and manages many security platforms such as secure Web and email gateways, security information and event management (SIEM), firewall (FW), intrusion detection systems/intrusion prevention systems (IDS/IPS) and data loss prevention (DLP), and partners with leading vendors in security space (Symantec, Forcepoint, Intel Security and Digital Guardian). It offers consulting and technical services, performs security assessments and incident response team services. It employs 15 penetration testers, and 15 to 20 cybersecurity analysts in the U.K. and 70 in the U.S. The company has raised $22 million in equity financing and $6 million debt financing in order to buy Pentura — a U.K. MSSP. It also will expand its operations globally and hire additional hard-to-find security personnel by seeking those with specific skill sets more relevant in today's technology world.

Challenges: Competition from larger, well known MSSPs, such as Dell SecureWorks, IBM, Symantec, HP and Verizon Business, being more global in nature and having longtime relationships with CSPs and the enterprise. Other global competition from smaller specialty consulting/ management firms, such as KPMG, EY and Deloitte, may also provide a challenge in gaining visibility. Its recent acquisition of Pentura, and plans to expand globally, will help if executed properly.

Who Should Care: CTOs and product managers at CSPs; and any enterprise looking for managed security services and a provider that can work with a wide variety of different implementations and on-premises point solutions. Enterprises that have unique security requirements and/or those that do not have the security expertise in-house should consider InteliSecure.

First Orion

Little Rock, Arkansas (www.privacystar.com)

Analysis by Deborah Kish

Why Cool: First Orion is cool because of its app, PrivacyStar, for mobile (Android) devices and in-network solutions that provides end users with the knowledge of who is calling them and why. The PrivacyStar app is cool because without mobile caller ID, enterprises and consumers are frustrated with nuisance continuous telemarketing calls. PrivacyStar helps end users (both enterprise and consumers) rid themselves of robocalls by identifying and blocking them. This includes text messages, telemarketing calls, unlawful debt collection calls and robocalls. The app also allows users to file complaints directly to the Federal Trade Commission (FTC) in the U.S. First Orion is also working toward becoming network-based to satisfy the same issues for customers, including landlines, voice over IP (VoIP) and iPhone.

First Orion's identification and blocking information is derived from the millions of PrivacyStar users that block, look up and complain against numbers. This means that thousands of telemarketer, debt collector and scammer phone numbers are constantly added and updated. It is also cool because the top-known phone scammers are automatically blocked from contacting customers using the app. First Orion is currently partnering with some of the largest global and mobile carriers and integrators, such as T-Mobile, TracFone and Sprint, and others both domestically and internationally.

Challenges: Simply put, lack of visibility from CSPs and global reach. With little in the way of competition, PrivacyStar needs to expand its CSP partnerships beyond the North American region and work toward having the application more visible on mobile devices. PrivacyStar also needs to polish its marketing strategy and roadmap in positioning its solutions for mobile operators or enterprises. These distinct business models require specific relationships with their target markets, which can be very challenging for small startup companies as they try to identify the business models for their technology and solution. It also needs to expand its marketing efforts to reach the consumer markets. It will also need to develop a business rule engine so that different rules can apply to different callers and users — based on time of day, if it is a new or repeat caller, and if caller ID or number are shown or hidden.

Who Should Care: CTOs and product managers at CSPs that are looking for new consumer revenue streams, ways to improve or enhance the customer experience, and wish to reduce churn.

Secret Double Octopus

Be'er Sheva, Israel (www.doubleoctopus.com)

Analysis by Deborah Kish

Why Cool: Secret Double Octopus offers keyless authentication and data-in-motion protection using a keyless encryption protocol based on the "secret sharing scheme" (a security algorithm) for cloud, mobile and IoT environments. Cool because for the enterprise, management of keys and the need for certificate authorities goes away. More cool because of how the software works. It breaks up data into randomized chunks that are transmitted to the intended recipient(s) through different routes, where only the recipient is able to reassemble them and access the information inside.

Innovation in the space has been inherently slow, with the industry skeptical of new encryption algorithms, and for good reason. Secret Double Octopus overcomes this by newly applying math such as secret sharing, which has been around for decades, but was previously not used for network security purposes. Secret sharing is mathematically classified as an "information theoretic secure" algorithm — one that is agnostic to the attacker's computing power.

Essentially, in order for a hacker to be successful in accessing sensitive data protected by Secret Double Octopus, they would need to first identify the network paths where the individual useless "pieces" of data are traveling through, compromise each one and put everything together despite complete obfuscation — only to then face a computational challenge comparable to modern cryptography. This is essentially ideal for prevention of man-in-the-middle and eavesdropping attacks. The secret sharing algorithm means that a real-world attacker captures information that is insufficient input for a brute force attempt, so that the startup's software is able to not only match, but exceed, the level of protection afforded by conventional cryptography, without most of the downsides.

Challenges: Secret Double Octopus, much like most startups, is largely unknown to CSPs providing managed security services and potential end users. In order to gain visibility into geographies outside of home environments, it will have to focus on developing partnerships with vendors and large service providers in regions that can expand its global reach and increase its visibility in the end-user markets, as well as invest in marketing to increase brand awareness. This solution works well for asynchronous communication (file transfers, email communications, cloud storage), as well as voice — but video traffic support is only planned for a future release.

Who Should Care: CTOs at CSPs; managed service providers offering managed security as a service, looking for additional capabilities in managed security services. Mobile banking and commerce developers requiring no-touch MFA/OTP. SMB/SMEs and midmarket organizations that are looking to unload the burden of having to manage encryption keys should evaluate Secret Double Octopus's solution.

Wedge Networks

Calgary, Canada (www.wedgenetworks.com)

Analysis by Akshay Sharma

Why Cool: Wedge is cool because they have a patented "Subsonic" engine that provides 20x-to-30x performance improvement in security scanning speed and accuracy to provide network security enforcement for all services connecting through the cloud. It can also provide new revenue streams to CSPs for security as a service products for SD-WAN, mobility and IoT security, as well as help CSPs consolidate varying hardware components such as UTMs, firewalls, and secure Web gateways for more conventional security services.

Wedge Networks offers a multitenanted SDN and NFV orchestrated solution that provides deep packet inspection and deep content inspection in conjunction with more than a dozen security VNFs for CSPs, large enterprises and vertical markets.

Current SDN and NFV solutions have been primarily focused in the data center, and address network virtualization concerns within the IT domain. They now need to be delivered within the CSP's WAN, and SD-WAN (software defined wide-area network), including with newer vCPE (virtual customer premises equipment) provided as a service.

CSPs are looking for ways to move from siloed networking appliances toward fluid and dynamic cloud-based security solutions that support end-to-end control, along with dynamic pay-as-you-grow provisioning that can be provided with virtualized and orchestrated security systems. The problems with the current technology are magnified in the WAN, because CSPs require resiliency, security, elastic scale and high performance with agile service delivery, whereas the siloed solutions of the past use legacy manual provisioning that is costly, slow and prone to errors.

Challenges: Cisco Systems, Palo Alto Networks, Fortinet, Juniper Networks and others have recently announced competing virtualized security offerings. While these vendors often mention security, service orchestration and real-time provision, this is still an emerging space.

Wedge Networks will need to show that it can provide a solution that can be deployed in a hybrid multivendor deployment and is able to provide:

- Enterprise-grade security from cloud infrastructures
- Lower total cost of ownership, with carrier-grade reliability
- Agile service delivery of newer services

- Solutions supporting end-to-end networks and across multiple vendors and network topologies (CSP-hosted, enterprise-hosted, along with hybrid fixed appliance-based solutions as well as virtual offerings from Wedge Networks)

Being a smaller firm, it will be challenged to gain visibility with larger CSPs, although it has been deployed globally, delivering security protection for tens of millions of users in Fortune 500 companies, government agencies, Internet and broadband service providers, and across many industry verticals.

Who Should Care: CISOs of large enterprises and government agencies evolving their security framework to incorporate a software-defined and virtualized security platform at the cloud layer, and CTOs at CSPs; managed service providers offering managed security as a service that need NFV-based provisioning and orchestration of virtualized security services such as UTMs, firewalls, and secure Web gateways, all should consider Wedge Networks for end-to-end service control across multiple networks.

Where Are They Now?

Centri Technology

Analysis by Deborah Kish

Profiled in Cool Vendors in Communications Service Provider Operational and Business Infrastructure, 2013.

Why Cool Then: Centri Technology was deemed cool because its technology-enabled mobile operators to reduce the bandwidth consumption of smartphones and devices that require mobile data by about 50%, with very little overhead or added latency due to its patented real-time byte-level compression techniques.

It productized its core technology across three products: BitSmart CX for network efficiency, bandwidth management, security and data protection; Insights CX for real-time reporting and analytics of services KPIs, and data stream visibility; and Premium CX for applying network policies, bandwidth control and user controls. It aimed to make the network "visible" to the application layer by exposing the intelligence that is embedded in the network.

Where They Are Now: Centri has launched its core data protection platform product on security and data protection, encryption and optimization capabilities for enterprises, technology providers and the IoT.

Who Should Care: CTOs and CIOs of CSPs should consider Centri solutions for its cloud, networks, applications, devices and IT infrastructure, to secure enterprise and customer data in all states and to optimize their data in use or in storage.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"When, Why and How to Encrypt the WAN"

"Competitive Landscape: Data Loss Prevention Market, 2015"

"Virtual Customer Premise Equipment Creates New Revenue Opportunities for CSPs in Security as a Service and SD-WAN"

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."