Gartner

Cool Vendors in Security for Technology and Service Providers, 2017

Published: 4 May 2017 **ID:** G00321937

Analyst(s): Ruggero Contu, Lawrence Pingree, Deborah Kish, Dale Gardner

These Cool Vendors are pioneering new directions and potential opportunities in the security market. Technology and service providers looking to partner with these vendors should examine their innovative security technologies.

Key Findings

- The convergence between IT, operational technology and broader IoT is driving demand for technology aimed at securing new vulnerabilities introduced by industry-specific initiatives.
- The shortfalls of established security technologies along with the mounting pressure from sophisticated attackers are creating opportunities for innovative startups in the areas of security intelligence, data protection and application security.
- Digital business requirements will continue to drive innovation and opportunities for security. New security demands will sustain the momentum and opportunities for startups in security.

Recommendations

In order to exploit security market dynamics, TSPs should:

- Align with the Gartner security taxonomy to take better advantage of market opportunities across different security intelligence areas.
- Exploit the limitations that traditional security controls have in fighting advanced targeted attacks. Leverage the new set of technologies being made available, which can provide interesting market opportunities as stand-alone and integrated offerings.
- Understand and plan for the different audiences and buying centers interested in operational technology security. Go-to-market and marketing approaches must align to their different requirements. With the increasing convergence of IT and operational technology areas, identify cross-selling opportunities.

- Ensure marketing messages for DLP products include coverage of capabilities for cloud applications, cloud storage and mobile data use cases, which can be developed organically or by partnering with or acquiring vendors in the cloud access security broker market.

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

Gartner has once again identified a new crop of security Cool Vendors that are leveraging innovations.

These Cool Vendors are related in the way they integrate and automate the use of security intelligence. They are also similar in how this intelligence is correlated to the detection techniques deployed by the different products and services offered. These Cool Vendors have innovative go-to-market approaches as part of a novel product offering and/or in the way the channel-to-market strategy has been built. These innovative go-to-market approaches have the opportunity to disrupt market dynamics.

This Gartner Cool Vendors report is aimed at technology and service providers (TSPs) and investors looking to expand partnering strategies and invest in innovative companies operating in emerging market areas with interesting go-to-market approaches.

These vendors' highly innovative technologies and business models may not be suitable for every enterprise's needs, but they are all worth evaluating. For assessments of Cool Vendors in other important security market segments, see the following:

- "Cool Vendors in Identity and Fraud Management, 2017"
- "Cool Vendors in Cloud Security, 2017"
- "Cool Vendors in Monitoring and Management of Threat to Applications and Data, 2017"

Trillium

Tokyo, Japan (www.trillium.co.jp)

Analysis by Ruggero Contu

Why Cool: Trillium has developed technology expertise that caters to the specialized needs of the evolving automotive industry. The industry is currently underserved by established security providers at a time when initiatives relating to connected and autonomous vehicle manufacturers are rampant. This company is also cool because of its work in developing alternative business models. For example, it plans to offer a subscription-based security service to users through car insurance companies, wireless data carriers, security providers and other partners. This model would transform an original equipment manufacturer's (OEM's) costs into an OEM recurring revenue stream.

Trillium's technology leverages artificial intelligence and machine learning to automate the detection capabilities of its proprietary firewall technology. The company provides three core solutions aimed at securing different elements of a connected vehicle's technology architecture:

- The SecureCAR module is deployed to secure communication between vehicles' electronic control units (ECUs) on the in-vehicle networks (IVNs). It also provides certificate-based authentication and dynamically changing key-lock pairing.
- A vehicle and cloud-based proprietary firewall (SecureIXS) provides intrusion protection and detection technology using dynamic whitelisting and blacklisting capabilities, as well as machine-learning-based anomaly detection.
- The cloud-based, real-time security updating services from SecureOTA are based on a dynamic threat library.

Trillium has developed a patent-pending, lightweight and high-performance Internet of Things (IoT) security software kernel and key management system to secure the data of resource-constrained automotive and IoT systems.

Challenges: Trillium is a startup from Japan, and it has the relatively common challenge of gaining visibility and extending its reach globally. This is significant for a company that is based in a country where the know-how and culture of developing a startup security business are limited. The company must invest heavily in extending its sales force and logistics, while balancing its investments in marketing, in order to remain successful.

Who Should Care:

- TSPs with an interest in the area of connected vehicle security
- Automotive industry channel partners, such as Tier-1 components suppliers
- Car manufacturers wanting to integrate cloud-based security solutions to tackle the emerging threats arising from vehicles connecting to external networks and connected vehicles' internal subsystem vulnerabilities

Schedule1

Toronto, Canada, (www.datapassports.com)

Analysis by Deborah Kish

Why Cool: Schedule1 is cool because it uses infonomics to provide a security risk assessment or a calculation of risk to derive a dollar value for an organization's data assets, or what Schedule1 calls the "Risk Value Indicator" (RVI). The RVI is used by DataPassports to create trusted data objects that protect data from end-to-end. This creates new value for end users in the majority of cases. For example, chief information security officers (CISOs) need to see how much a data exfiltration incident will cost in terms of dollars. Schedule1's value-added approach can help determine potential loss and provide the information needed for decisions on security budgets, cyberinsurance investments and controlling end-to-end data encryption. Schedule1's use of infonomics provides a high level of security intelligence. This intelligence is valuable to organizations because it assists in quantifying the information's value, and will be useful for organizations in determining how data assets are handled.

Schedule1 is a startup that is focused on the financial services space. It offers algorithms that enable its customers (mostly in Canada) to better aggregate and parse data into usable information that can be actioned in real time. Its product portfolio spans four data protection and privacy modules aimed at end-user data security concerns with a focus on data asset value and protection through "DataPassports," its flagship platform. Each module — "Security by Choice," "Value by Choice," "Privacy by Choice" and "Classification by Choice" — utilizes the data in DataPassports by applying intelligence, machine learning and risk value based on the assigned criticality of the data it serves.

Security by Choice applies intelligence and data-centric protection to data assets in an organization based on what and how the data is used. Privacy by Choice uses big data, analytics, and information and processing, allowing end users to apply a consent model to be in compliance with regulatory mandates, such as the EU's General Data Protection Regulation (GDPR). Classification by Choice takes feeds from the Security by Choice product, enabling classification based on a critical data's asset value. Value by Choice utilizes the information driven through DataPassports to create infonomics, helping organizations to measure and monetize this information.

Challenges: Being a new vendor, Schedule1 might find it difficult to explain the value proposition of its products, particularly when various business units in organizations are fighting for budget. To do this, it will need to provide proof points with customer endorsements of savings and perceived

value. Schedule1 needs to increase its ecosystem to include data-centric audit and protection (DCAP) and data loss prevention (DLP) technology providers to expand its visibility and customer reach beyond the financial vertical. Schedule1 does not have visibility within the Gartner customer base. Therefore, it also must devise and execute a solid marketing plan to increase visibility and attract new customers.

Who Should Care:

- C-level personnel in any vertical market responsible for, or who are currently assessing, DCAP and DLP tools and are making decisions around purchasing cyberinsurance
- Data owners of high-level data that are responsible for adhering to data security policies, including data regulations and safeguarding the integrity of the business unit data
- Technology strategic planners tasked with creating a baseline of asset values and innovative ways to monetize data assets
- Managed security service providers (MSSPs) looking for additional revenue streams to bring a value-add to their security product portfolio

Centripetal Networks

Herdon, Virginia (www.centripetalnetworks.com)

Analysis by Lawrence Pingree

Why Cool: Centripetal Networks is cool because it offers a stand-alone threat intelligence defense (STIDS) appliance that helps security teams detect and block advanced threats with its platform, QuickThreat. Centripetal Networks is unique in its ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds.

The QuickThreat Gateway appliance enhances customers' ability to perform more comprehensive threat detection and blocking than traditional network security appliances. The QuickThreat Gateway appliance performs analytics and provides threat alerts by leveraging Centripetal Networks' QuickThreat Manager solution, which correlates and visualizes threats by factors such as severity, reliability and geography. The QuickThreat intelligence service synchronizes and normalizes threat intelligence from more than 40 third parties. The system is unique because it enables threat feeds, internal or external, to be integrated.

The QuickThreat Gateway appliance currently has the largest number of third-party threat intelligence service integrations in the network security market. It claims to be able to use up to 5 million indicators simultaneously. Meanwhile, other multifunction or network security appliances are typically limited to the detection and prevention of only tens of thousands of threat indicators. The QuickThreat system also provides subscriptions to a wide variety of community (such as Financial Services' Information Sharing and Analysis Center [FS-ISAC] and government) and open-source feeds. The system is valuable and cost-effective for enterprises of all sizes. Current customers span

from small companies to the very largest financial services, retail and government customers in the world.

Challenges: Although a very cool solution, Centripetal Networks is largely oriented toward larger enterprises because of its need to leverage a wide variety of threat intelligence sources. As such, coupling multiple threat intelligence feeds from third parties into a single form factor can incur more service fees and contribute to a higher cost of ownership. The company must overcome the challenge of being viewed as a high-end, large enterprise offering by developing virtual appliances, other form factors, and threat intelligence service bundles in order to entice and attract buyers down-market.

In addition, the threat intelligence indicators currently offered are limited to IP addresses or blocks of IP addresses, 5-tuples, fully qualified domain names, URLs, DNS and Transport Layer Security (TLS) indicators. This allows the company to enforce a large number of indicators, but it lacks some coverage that could be offered through deeper inspection of the application layer.

However, the ability to load large indicator datasets makes Centripetal Networks cool. The company will release a virtual appliance option this year, which is ideal for cloud and virtualization infrastructure deployments. Centripetal Networks currently supports integrations with Splunk, QRadar, and other security information and event management (SIEM) tools. With these integrations, security analysts are able to see and stop threat activity immediately and automatically from their current visibility tools. This feature reduces analyst workload significantly.

Who Should Care: Technology product management leaders should seek to operationalize their own security threat intelligence feeds and services with Centripetal Networks. They should consider integrating the solution with their threat telemetry to respond to a detected threat. This capability reduces security workloads and significantly increases security posture. For example, security technology markets — such as network access/admission control, distributed deception platform and firewall providers — could benefit from incorporating Centripetal Networks' appliances with their own functionality to enrich threat detection and enhance their responsiveness in the enterprise environment.

Signal Sciences

Venice, California (www.signalsciences.com)

Analysis by Dale Gardner

Why Cool: Signal Sciences' product offers security teams a unique approach to protect web applications, microservices and APIs. It combines the flexibility of multiple deployment options with a cloud-based analysis engine, offering enhanced detection capabilities derived from a view of attack and anomaly data across a broad range of organizations.

Leveraging security intelligence across a broad community is illustrative of a capability common to the vendors highlighted in this report. Attacks against web applications represent the leading attack vector for data breaches. Traditional defenses, typically web application firewalls (WAFs), have struggled to move beyond basic attack protections. However, runtime application self-protection

(RASP) products promise more accurate and broader protection against attacks, but have been slow to gain market traction.

Signal Sciences addresses these challenges in two distinctive ways. First, the company's product offers multiple deployment options. While the various options are not new, their availability within a single product provides security and operations teams with greater flexibility in implementation, including different approaches for individual applications. Choices include what founders have dubbed a "next-generation" WAF module, supported across a mix of popular web servers and operating systems; a code-based lightweight RASP version (supporting .NET and Java); and the ability to implement the protection module directly within scripting code (including Python, JavaScript, Node.js and PHP).

In addition, information about ongoing attacks and anomalous activity is fed into a cloud-based decision engine capable of analyzing activity (including activity across customers). It then responds with updated "signals" (essentially detection and response rules and guidance) to individually deployed detection modules. Using custom detection rules, Signal Sciences detects and prevents not just "routine" vulnerabilities, but also business logic faults, authentication errors and other more complex weaknesses that have eluded existing solutions. Centralized management and reporting is included, along with multiple enterprise integrations.

Challenges: Signal Sciences' most pressing challenge — beyond market visibility as a newcomer — arises from the product's flexible approach to web application protection. Although a strength of the product, alternative implementation approaches expand the number of potential competitors. These include competitors from the $500-million market for WAFs, where close to 20 established vendors already vie for buyer attention and sales. The company also faces competition from over a dozen companies pursuing the emerging RASP market.

Operationally, Signal Sciences must demonstrate the ability of its back-end analysis platform to keep pace with growing traffic and activity as it attracts additional customers. Its cloud-based analytics platform presents a double-edged sword. On one hand, the ability to analyze and assess activity from multiple points of view yields a positive, beneficial network effect that should produce faster and more accurate responses to attacks for all customers. However, the company must address the inevitable privacy concerns arising from such an approach, most obviously among vertical and geographic markets with a low tolerance for data exposure risks and significant regulatory burdens around the same.

Who Should Care: Signal Sciences' innovative solution presents partnership and acquisition possibilities for a variety of technology business unit leaders in the application security arena. Chief among those are existing WAF vendors that lack more advanced analytical capabilities or RASP functionality (or both), which would complement and extend their existing offerings. Additionally, vendors in adjacent markets (such as content distribution, load balancing and application runtime vendors) could leverage Signal Sciences' technology to gain entry to security buyers.

Where Are They Now?

Blueliv

San Francisco, California and Barcelona, Spain (www.bluelIv.com)

Analysis by Deborah Kish

Profiled in "Cool Vendors in Communications Service Provider Security, 2015"

Why Cool Then: Blueliv was selected as a cool vendor in 2015 because its platform provides a significant enhancement to how organizations deal with threat intelligence. Its cloud-based cyberthreat intelligence, analytics and information platform provides not only better visibility, but automation on what is usually error-prone and manual work. The platform offers a simplistic front-end GUI that allows for large scale and multitenancy.

Blueliv is also cool because of its strategy of working with institutions and partners on a one-to-one basis to better understand how they will individually use the platform.

Where They Are Now: Blueliv has continued to build its business by doubling its employee numbers since 2015. Through its recent round of funding, it has notably increased its sales force. Since 2015, Blueliv has continued to develop its threat intelligence product by adding new sources, features and modules, such as a dedicated dark web channel. It has also added a "Media Tracker" module so customers can track where their company is mentioned in media forums. These modules provide MSSPs with new sources to collect data from and to increase their customers' ability to understand their threat exposure. MSSPs can also provide customized data based on specific verticals. Blueliv has launched its own crowdsourced blog community, the "Threat Exchange Network," where members can share threat intelligence information on their threat experiences and how they were handled.

Blueliv has been working to form technical alliances with other vendors, such as Check Point (IntelliStore), Anomali and several antivirus companies. These alliances will allow Blueliv to boost its ingestion capabilities and gain a wider overview of threat intelligence and threats associated with Blueliv's customers.

Blueliv also introduced machine learning to give communications service providers (CSPs) greater visibility on specific malware being hosted on their networks. It is also working with university experts to develop mathematical models to define specific risk profiles, which can be beneficial in determining predictive behaviors. Its continued roadmap includes a threat actors catalog (with indicators of compromise [IOC] related to them), kill-chain graphical visualization, automated vulnerability scanning, vendor risk management, an IoT module and segmenting distributed denial of service (DDoS) threats during 2017.

Who Should Care:

- Organizations with lean forward security programs
- MSSPs looking to more efficiently consume and process threat intelligence

- MSSPs looking for partnering opportunities to take to the market
- CSPs (fixed and mobile) that are interested in protecting their own network from the "outside in" in the face of an always evolving threat landscape

The Blueliv solution is competitive and functional. Also, due to its SaaS delivery model, it provides fast ROI for an organization implementing or reselling the technology.

Gartner Recommended Reading

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

"Cool Vendors in UEBA, Fraud Detection and User Authentication, 2016"

"Cool Vendors in Security Infrastructure Protection, 2016"

"Cool Vendors in Security Threat Intelligence, 2016"

"Predicts 2017: Security Solutions"

This document is published in the following Market Insights:

Security Solutions Worldwide

Gartner

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