www.pipelinepub.com
Volume 17, Issue 1

Top 5 Security Innovators to Watch

By: Scott St. John

These are uncertain times. Uncertainty creates fear, and fear breeds more uncertainty. It can feel like an unending cycle, where the very definition of the word security is under attack. Between the global COVID-19 pandemic, sporadic civil unrest, unpredictable changes to the world order, ongoing tension between nation-states, and the advent of the new life-from-home scenario, it has been tough on virtually every level.

To make matters worse, we are under constant attack, every minute of every day, and you may not even know it. It's big business, and it's easy. The average US enterprise faces over 100 cyberattacks each year, and a cybercriminal can breach your defenses with cheap off-the-shelf software or open-source bots today, costing you tens of millions of dollars or more. They can hack into your devices, bring down your website, cease your operations and hold your data hostage. They can also take your data, sell it on the dark web or even to unscrupulous commercial websites. Scary stuff.

It gets even scarier when you consider the shift that we have undergone surrounding digital transformation, omnichannel, and the remote workforce. We're well past the tipping point, and these trends have become and will remain mission critical throughout the COVID-19 era. So, what can you do?

There is a plethora of cybersecurity companies who have been answering the call in various ways. They all provide some protection, and you probably know some of them. Many are household names, such as McAfee or Norton, and others are security offerings from major enterprise software giants like IBM and Oracle. They have been around for decades or more, none of them really scream "state of the art," and when it comes to your cybersecurity, timing is everything. There are a few red-hot newbies too, such as Crowdstrike, Cyberark, Okta, and Zscaler, but they are somewhat narrowly focused and have already received more than their fair share of media coverage. Paying them more lip service here would not be to your benefit.

Instead, this article focuses on companies that may be new to you. They are upstart innovators who are taking a fresh approach to security based on today's rapidly expanding and accelerating threat landscape. And, notably, many are tied to the trends mentioned above, making them even more important for threat mitigation.

Democratizing Security

The world of security – and more importantly the ever-changing landscapes of security threats – can be difficult to navigate. Historically, a business would have to engage with a value-added reseller (VAR) for a year or more just to sort out their needs, identify which solutions are commercially available, and then deploy them. This old VAR model doesn't work any longer, as companies shift from a physical premise during the COVID-19 pandemic, or as newer technologies around cloud and software-as-a-service solutions continue to be consumed at an unprecedented rate.

By contrast, Cyvatar is building a platform of API-based, best-of-breed cybersecurity products – like Cyberark, Okta, and Patchworx – and integrating them into a singular, click-to-consume, subscription-based, cybersecurity-as-a-service platform. The Cyvatar subscription includes installation, assessment, remediation and continuous monitoring and maintenance, a process Cyvatar calls ICARM. Cyvatar's broad and diverse portfolio of cyber-defense solutions that addresses virtually every imaginable aspect of cybersecurity.

You can also think of Cyvatar as a CISO-as-a-service, tailoring specific security solutions based upon your individual, desired business outcome. In some cases, that outcome may be driven by NIST, SOC 2, or PCI compliance; in other cases it may be driven by IT inventory management, third-party security assessments, or simply to ensure a high degree of security hygiene around passwords and patches.

By amortizing the cost of these best-of-class solutions into one platform, you save – in both time and money. A typical custom solution, going through Cyvatar's entire ICARM process, can achieve your desired business outcome in under three months and for a fraction of the cost of acquiring, integrating and deploying all the cybersecurity tools that are already at their disposal.

Dynamic Web Application Protection

As commerce continues its massive move to web and ecommerce applications, and schools and businesses shift to home learning and remote work, a whole host of new threats have emerged, such as account takeovers, code-injection formjacking, and Magecart attacks. Cymatic combines the strength of a web application firewall (WAF) with its AI-based VADR™ vulnerability, awareness, detection, and response engine to identify bad actors and remediate threats. If that

isn't innovative enough, the Cymatic solution can be installed in mere minutes, providing near instant client-side protection without having to set up complex rules, whitelists, or blacklists. To put that in perspective, its most complex deployment to date took under forty-five minutes to completely operationalize.

With a single line of javascript code installed in the header of your web application, Cymatic can "own every browser session" from every device that lands on your web app so that it can securely capture, analyze, and act on many known and unknown threats. Because Cymatic's solution doesn't rely on traditional cookies, it is invisible to the user and can go much deeper into the analysis of the user's specific behavior, streaming user-session information into its VADR™ threat-detection engine. And it does this using encrypted microservices that are fully anonymized and privacy- and data-standards compliant. It also uniquely compares normal user behavior based on your organization's specific business processes and compares that to every user session to identify anomalous behavior and suspicious users, providing contextual and dynamic policy enforcement.

Cymatic also combines typically separate components – such as dark web tracking, bot detection, IP address information, and geo-location data – with behavioral analyses of user risk markers such as authentication and session information, automation technology, browser information, device information, mouse-clicks, and user preferences. It uses this rich contextual analysis across many risk vectors to quickly analyze, identify, and remediate potential threats.

Cymatic's platform allows organizations to identify potential security vulnerabilities; detect risks and bad actors; and respond to them with a variety of actions. This includes fewer but more meaningful notifications and automated actions such as challenging or denying access, forcing the suspicious user to reauthenticate using different methods, and forensically snapshotting and recording the session. By combining many of today's cybersecurity tools into a single web application security platform that can literally be launched in minutes, Cymatic can be instantly deployed to provide immediate protection.

Next-Gen VPN

VPNs have been a mainstay in enterprise connectivity for many years. However, as more and more workers shift to work-from-anywhere, the need for both data security and privacy protection has never been greater. Virtually every enterprise has now become vulnerable to every security threat of every individual worker. The thought of a remote worker accessing sensitive corporate data on a personal PC over unsecure Wi-Fi from a Starbucks sends shivers down the spine of even the most hardened enterprise IT professional – and it should.

NordVPN offers a variety of enterprise and personal data and privacy security options while catering both to enterprises and individuals across any device. What makes NordVPN unique is the layers of security it provides. NordVPN leverages over 5,000 servers in over 50 countries using the AES 256-bit encryption standard. But while most VPNs allow you to use the IP address from

within a single secure location, NordVPN's Double VPN is an advanced VPN security feature that routes your traffic through two VPN servers instead of one, encrypting your data twice. In addition, NordVPN offers Onion Routing to provide ultimate privacy protection. Combined with Double VPN, Onion relays your traffic across a vast network of servers that add layers of encryption along the way, creating impenetrable data and privacy protection.

Mission Critical Networking

Dispersive Networks takes VPN to the next level. Perhaps the singular issue with old-school VPNs is that they are a single channel. While you can mix up the route the data takes and add layers of encryption, this may cause performance issues at hyperscale and for traditional VPNs in some of today's, and tomorrow's, massive use cases such as 5G, cloud, connected-everything, Industrial IoT, microservices, and SD-WAN optimization. Essentially, if data is a deck of cards, Dispersive shuffles the deck, and then shuffles it again and again, dealing the cards exactly where they need to be – across the optimal path – every step along the way. Dispersive takes a unique, patented approach to addressing this by combining Network-as-as-Service with Network-Security-as-a-Service into a Secure Access Service Edge ("SASE"). In this application, Dispersive splits data streams across multiple, separate, AES 256-bit encrypted channels, which connect to a network of key-authenticated Deflect server paths. If congestion, attacks, or anomalies are detected, Dispersive automatically re-routes the data stream across other trusted channels. This approach is baked into its Dispersive Virtual Networks (DVN) solution, which can provide 10 times or more performance improvement over traditional VPN services by eliminating the need for VPN concentrators and decentralizing traffic based on the best path to its intended destination.

By splitting encrypted data streams across a diverse network of its proprietary Deflect servers, enterprises can nimbly access cloud applications, enterprise networks, and transmit data based on specific, hard-and-fast performance metrics. In addition, the originating IP address for each end point is unique to, assigned by, and only known to Dispersive's secure Deflect servers – which dynamically change. Lastly, Dispersive's DVN solution has a small footprint and can be installed on all but the smallest of devices – and is cost-effective relative to other SD-WAN offerings.

Dynamically Detecting Deviant Behavior

Enterprises have mere minutes to respond to threats before serious damage can occur. The problem is that most security solutions today are built upon static workflows. This creates a multitude of alarms, where alarm fatigue can set in. By the time an average business identifies a threat and is able to respond, the damage has already been done. This is where Orchestral Networks' ON S2-D2 solution comes in, and one of the reasons they won in multiple categories in *Pipeline*'s 2020 Innovation Awards Program, including the Innovations in Security category.

ON S2-D2 combines true artificial intelligence (AI) in the form of Deep Neural Network (DNN) technology, a non-centralized virtualized representation of the network it is protecting. This is done by a series of non-centralized components, each associated with one of all the major subsystems in the network. These components communicate with each other in a dynamic fashion based on a negotiation system. These non-centralized components maintain a statistical moving-sum average of normal behavior for the subsystem that they are associated with. This moving-sum average is important because normal behavior tends to drift over time.

When deviations from normal occur, the non-centralized components negotiate with each other to determine if the behavior deviation is a result of other 'normal' changes elsewhere in the system, or if it is a true positive security alarm. If it is a true positive, then the non-centralized components negotiate with each other to determine if this particular subsystem is exhibiting symptoms of a breach elsewhere in the system, or if it is the root cause. Then, they negotiate with each other to remediate the breach. Remediation can be static or dynamic. The choice of dynamic or static remediation is determined through the negotiation process. If dynamic, it is in turn carried out through negotiation between the components. What makes it unique is the user's ability to control the level of automation. In some cases, the user may choose to manually evaluate the anomaly. However, in other cases, ON S2-D2 can automate and learn from decisions to dynamically and immediately remediate potential threats in under one second.

A Sense of Security

It seems the only thing that is certain today is uncertainty itself. However, there are commercial offerings available today that can help protect you and your business from a wide variety of attacks. I have shed a little light on a few of them throughout this article: from Cyvatar, which can create tailor-made managed security solutions; to NordVPN and Dispersive, which can provide deep data and privacy protection; or Cymatic and Orchestral Networks, which can provide advanced contextual and behavioral anomaly detection and remediation. I hope this article helps you sleep a little better tonight and that it has provide you with some sense of security – both figuratively and literally.