2019 TAG CYBER SECURITY ANNUAL
VOLUME 2
INTERVIEWS WITH CYBER LUMINARIES
Dr. Edward G. Amoroso
To the Reader:

Conducting and transcribing a detailed interview with an expert is harder than it looks. This is the third year we’ve published our questions and the corresponding answers received from various cyber security luminaries for this TAG Cyber Security Annual, Volume 2. While we would admit considerable remaining distance between our work and Cronkite’s, we do think we are getting better. In fact, we are confident you will find this series of interviews to be the most crisp and interesting content in our three volumes – probably because our interviewees did all the work.

Our primary goal in each interview was to showcase the expert views of the person being interviewed. This might sound obvious, but it is often complicated by marketing and public relations teams who certainly earn their monthly paychecks. On occasion, we would submit questions and receive back cut-and-pasted responses perfectly phrased from a brochure: “Our industry-leading security solution provides superior protection of your critical assets on both premise and in the cloud.” We tried to push back whenever we received anything vacuous like this.

For the most part, however, our experts – forty-five in total – were selected because their voice was simply worth hearing. Too many enterprise security teams avoid vendors like the plague, and this is a lose-lose situation. Enterprise teams lose out because they are deprived the amazing perspectives available from the cyber technology community; and the vendors lose out because they drive customers away by being too pushy about why their product would have solved the problems of Target, Sony, OPM, and Home Depot, not to mention stock fluctuations and global warming. Our interviews cut through all of that.

We recommend that you use these interviews in your day-to-day source selection or vendors and partners. If you are considering a purchase in some area of cyber security protection, then check to see if a principal from that firm is included here (or in our two previous volumes published in 2016 and 2017). Take a moment and read their words, because it will help provide for you with a sense of their purpose, belief, and intent. It’s been our experience at TAG Cyber that understanding what a company and its principals believe is often the most important factor in determining whether their products will fit your needs.

By the way, if you are a vendor and haven’t been included here – but believe this is an injustice the size of our galaxy, then please feel free to drop us an email at eamoroso@tag-cyber.com. We will do our best to set up time to review your solution offering. We cannot promise that we will make it together to second base, but we promise to try to listen to your message, and to try to understand what you and your team are about. Our experience dictates that this is the optimal means for any industry analysts to advance the community.

Wishing you nothing but the best in your cyber security work this year, enjoy this volume – and we hope it helps you save time, effort, and money.

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
Fulton Street Station on Broadway
2019 TAG Cyber Distinguished Vendors

Each year, we cover roughly 2000 vendors in the cyber security industry and write a one-pager for Volume 3 of this Annual. From that large group, we down-select about 200 or so to deep-dive their technology and usually to generate an article, blog, or technical article. We do this work gratis – and enjoy every bad-business-model-because-it’s-free minute of the work. Every day, we try to assist the industry – and that includes you – with this work. You should follow Edward Amoroso on LinkedIn or @hashtag_cyber on Twitter to gain access to this stream of content. In addition, however, we down-select the list to about 40 or so cyber security vendors that we believe are truly worth spending serious time with during our year. These vendors become our TAG Cyber Distinguished Vendors, and we channel their technology message to you through a series of articles, webinars, white papers, technical reports, eBooks, videos, interviews, and on and on. This report would not be possible without their technical, in-kind, time, travel, research, meeting, and financial assistance to TAG Cyber throughout the year. The list of 2019 Distinguished Vendor sponsors is provided below and I hope you’ll take a moment to review the list. These are fine companies:
Secure Access for Hybrid IT

An Interview With Sudhakar Ramakrishna
CEO
Pulse Secure, LLC

ENABLING PRODUCTIVITY while ensuring protected and compliant access to applications and resources is a challenge as enterprises take further advantage of a mobile workforce, data center virtualization, and cloud-based applications and infrastructure. Business appetite for anytime, anywhere access, and improved user experience, have resulted in an amalgamation of infrastructure and tools to quickly satisfy IT demand. As such, organization are re-assessing their technology stack that comprise secure access.

Common misperceptions are that previous access security capabilities can be readily applied across private cloud, public and SaaS. Or that new devices, including IOT and IIOT devices, and new mobile and cloud applications can be managed using the same controls as other corporate devices. Even the often-difficult question of “who is accessing what, from where, with what” has become more complex. A flexible, comprehensive platform can make the difference between simplifying secure access management and costly piece-meal approaches.

Pulse Secure is one of the few vendors focused on software-defined secure access for hybrid IT, building upon its Juniper heritage and expanding its solution set across mobile, virtual and cloud. We recently had a conversation with Sudhakar Ramakrishna of Pulse Secure to explore how the company and its customers are migrating from remote access to hybrid IT access protection.

EA: What is meant by secure access?
SR: Secure access is all about allowing IT to deliver seamless user connectivity to applications and resources- wherever, whenever and however is needed, without compromising security. These solutions provide IT the orchestration and interoperability crucial for connectivity, authentication, controls, data protection, availability and threat response on-premise and in the cloud. That is a direct definition. In practice, I am often saying that secure is “more about access, not control.” We are not talking to customers about restrictive endpoint or network security products. We ask customers how we can enable user and staff productivity among increasing requirements and limited budgets. Simply put, mobility and cloud drive greater
agility and more options, but comes with increased security and data privacy exposures. So how can we mitigate these risks to allow our customers the means to push the boundaries of mobile and cloud applications use, user experience, and data center and cloud resource optimization.

**EA: From a technology perspective, how has Pulse Secure and customers moved from Remote Access to Secure Access?**

**SR:** Remote access is straightforward using SSL VPN appliances when devices are corporate managed, and the corporate data center holds the apps and resources. With the adoption of mobile and IOT devices, mobile and cloud applications, and data center capacity leveraging virtualization and cloud computing, our customer’s operating environment and their threat surface has evolved - and our products have had to progress as well. The Pulse Secure Access suites encompass mobile, network, cloud and application access. Our unified client and policy engine allows for consistent user and device access visibility and control. Our mobile security for IOS and Android devices supports BYOD initiatives without intruding on a user’s personal space. Our VPN solution provides a wealth of MFA, VPN and endpoint compliance functionality with open standards such as SAML to enable unified remote and cloud access. Our network access solutions allow for real-time network device discovery and profile checking, as well as extensive NAC features. And our ADC acquisition from Brocade provides us with virtual and cloud application load balancing with WAF. We have over 20,000 enterprise customers and millions of users worldwide. Ultimately, we want to provide our customers the confidence that as their requirements, applications and environments evolve, Pulse Secures capabilities, interoperability and adherence to standards will meet their needs.

**EA: How does Pulse Secure provide enterprises visibility and compliance?**

**SR:** Visibility and compliance are essential, and we are hearing that from the executive boardroom to security operations. Our VPN, profiling and Network Access Control (NAC) solutions provide an incredible amount of visibility and compliance functionality. As users, devices and systems connect to data centers, applications and cloud resources, each of our solutions allow IT and security staff to gain insight on user, device and application behavior, security state, and compliance violations. This data can be easily shared with others to enhance reporting, inventory, auditing and most importantly threat response. This helps network administrators and CSOs understand if systems are accounted for, if guests and IOT devices are managed, if endpoint security is active, if their environment meets corporate, industry and regulatory obligations, and even how applications are being used. Within our Pulse One management console and Secure Access suite, administrators can get a unified, dynamic view into users, devices and applications across remote, network and cloud. The breadth of coverage and level of fidelity is extremely useful. More so, policy-based controls allow administrators to enforce access policy and invoke remediation or mitigation actions which allows reduced IT staff to gain greater oversight and protection coverage.

**EA: Where does Zero Trust play a part in Pulse Secure’s on-going development?**

**SR:** Zero Trust security is a security model that aims to advance conventional access security mechanisms to one that directly assures authentication, compliance and secure connectivity
directly between users, devices and applications/resources held in data centers or the cloud. In essence, our Secure Access solutions have always provided Zero Trust capabilities.

In particular, Software-Defined Perimeter (SD-P) solutions offer Zero Trust functionality that aim to enable more rapid deployment, less infrastructure dependencies, greater application and resource protection, and improved user experience. The SDP security model is often associated to a “zero-trust” approach of trusting nothing and verifying all. However, it does not mean that other trust models should be excluded or invalid. Every SDP approach must accommodate some level of trust that is established while creating a user session, and typically remains valid throughout the session duration. This trust can be based on a combination of current and past assessment of user identity, authorization and reputation, device compliance and reputation, client application type, originating network, geo-location and connection type, information access patterns, and other factors. Not all scenarios or resources require a true zero-trust based policy, all the time. Different applications or classes of information can be mapped to a spectrum of trust levels that need to be established, per secure access policies, in order to grant access.

That being said, current SD-P solutions are often easier to implement with web applications, less complex applications and fewer legacy IT dependencies. This limits SD-P adoption by a majority of mid-tier and large enterprise. At Pulse Secure, we see SD-P as another modality within Secure Access. Fortunately, the solutions and proven technologies that our customers rely on today are fundamental building blocks for Pulse Secure to bring an enterprise-class SD-P solution to market in the near term.
Design – Miles McDonald, Alicia Amoroso, Rich Powell
Media Services – Miles McDonald, Matt Amoroso, Laura Fanelli
Finance – M&T Bank
Administration – navitend
Lead Author – Dr. Edward G. Amoroso
Researchers – Ed Amoroso, Matt Amoroso, Felix Andersen, Liam Baglivo, Ana Bolsoni, Shawn Hopkins, Miles McDonald, Ankit Parekh, Pratik Patel, Stan Quintana, Tim Steinberg
Facilities – WeWork, NYC

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871

Copyright © 2019 TAG Cyber LLC. All rights reserved.

This publication may be freely reproduced, freely quoted, freely distributed, or freely transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system without need to request permission from the publisher, so long as the content is neither changed nor attributed to a different source.

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the author of this document nor TAG Cyber LLC assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2019 TAG Cyber Security Annual volumes.

The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Cyber LLC reserves the right to change its policies or explanations of its policies at any time without notice.