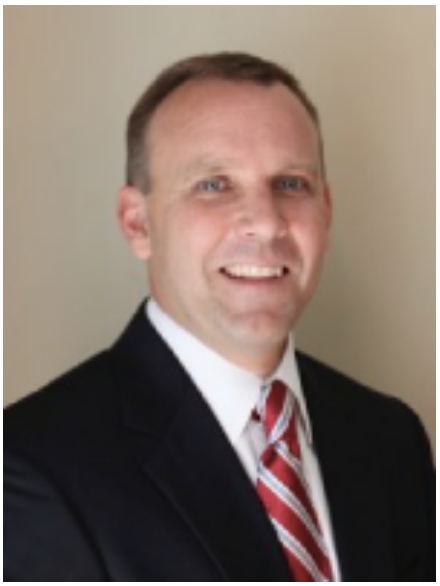
2017 TAG CYBER SECURITY ANNUAL VOLUME 2

Cyber Security Industry Luminary Interviews

Expert Advisory Research

Dr. Edward G. Amoroso
Chief Executive Officer, The Amoroso Group (TAG Cyber)

Version 1.0 – September 2016



Virtual Software-Defined Segmentation

Mitigating Weaknesses in Modern Enterprise Security Perimeters

David Keasey, CEO of Catbird

As enterprise teams have come to recognize that the traditional perimeter no longer works at stopping or even slowing advanced persistent threats from nation state actors, the need for alternative solutions has never been more urgent. Since 2013, David Keasey has focused his efforts on helping enterprise CISO teams build software defined segmentation solutions, which are designed to support advanced protections for emerging hybrid cloud infrastructure. Techniques that make use of the power of virtualization are likely to be compatible with clear trends in cloud-based data centers, as well as software defined wide area and mobile networks.

EA: Is virtualization truly a reality in the modern enterprise? Or are most businesses still operating in the more traditional manner?

DK: We definitely see accelerations in virtualization and hybrid IT, which involves combinations of private cloud workloads across multiple hypervisors, public cloud workloads, and bare metal. While enterprises continue to have significant legacy workloads on bare metal in traditional data center environments, those are static, and new applications are being deployed using a different model. Our team at Catbird has met with some of the largest financial institutions, retailers, government agencies, and global leaders in other industry verticals over the past year, and nearly every one of them has IT projects on-going that are focused on building next generation cloud infrastructures for their companies. Nearly every one of them is a multi-hypervisor, multi-cloud project where they would like a single pane of glass to manage automated deployment, monitoring, and enforcement across all workloads in a consistent manner. Most of these next-generation cloud projects are also looking to deploy a micro-segmentation strategy across all workloads.

EA: Do you see any differences in the adoption rates? For example, are large companies moving to virtualize more quickly – or perhaps less quickly – than their smaller counterparts?

DK: I think large companies have a greater ability to build large project teams to evaluate options than smaller companies. We've had meetings with global financial firms, for example, where literally a dozen or so business units might be represented in the meeting. This is promising, because it demonstrates commitment to the virtualization approach. But what we *have* seen sometimes, unfortunately, is that because virtualization represents such a new approach, it can lead to challenges in the alignment of goals and the prioritization of requirements amongst the various teams. This can really hurt these organizations in moving their projects forward, so the security industry needs to provide them with improved support, platforms, and processes – not to mention education and training on cloud and virtualization.

EA: Does software defined networking make things better for security teams? Or do you think that it could introduce serious new security risks?

DK: SDN has the potential to simplify and improve the application of security policy. I would argue that the foundation of every SDN provider's pitch is security, and in the end, I do believe the technology will have the ability to deliver stronger security, so long as the customer adopts the security components of the SDN solution, many of which can also be delivered without implementing SDN. Because of the prevalence of legacy systems, and the relative immaturity of many teams to understand and adopt SDN, there are a lot of partial implementations out there today. For example, VMware has been successful in deploying its NSX capability to many customers, but many of those customers are probably still struggling to properly implement the NSX Service Composer and its partners' security controls. And without doing so, these customers are not really enhancing security and receiving the benefits of a micro-segmentation strategy. Companies like Catbird and others in the software-defined segmentation space can deliver the value and enhanced security of micro-segmentation without requiring full SDN adoption. And for customers who truly want to take full advantages of the agility and efficiency of SDN in their networking strategy, then the synergy of improved security and SDN benefit can be achieved.

EA: Just about everyone is talking about East-West traffic threats. What's been your experience working with customers of the Catbird solution? Is it really possible to virtually segment cloud workloads?

DK: Yes. It is absolutely possible, and even straightforward, to logically segment virtual workloads to achieve stronger security overall, and to provide visibility into East-West traffic, which is not typically visible with perimeter based security – and this is an important goal. Consider, for example, that East-West traffic represents over 80 percent of all network traffic. Furthermore, data breach reports from

Symantec, Verizon, Mandiant, and others provide similar statistics regarding the number of days bad actors are inside a network before being detected. That could be as many as two hundred or so days for a breach to be lurking in an environment where most of the traffic is East-West. In my opinion, implementing a software-defined segmentation solution like Catbird provides the necessary visibility, monitoring, and enforcement to really make an impact on this problem by leading to earlier detection of anomalous network traffic.

EA: Catbird supports so-called TrustZones for virtual grouping. Can this grouping be extended across the enterprise to non-virtualized assets?

DK: We are working on two solutions to extend our TrustZone concept across the enterprise, not only to non-virtualized assets, but to deliver on our vision of a consistent approach to automated security policy deployment, monitoring, and enforcement for any workload on any platform. And this includes hybrid IT infrastructure such as private clouds, public clouds, bare metal, and containers. Today, we can extend our TrustZones to adjacent physical assets, which include bare metal workloads connected with the VMware or OpenStack clouds where Catbird is deployed. We've also done work with leading SDN providers, which allows us to extend to all physical assets via the SDN controller. A huge advantage of Catbird is our ability to deliver the functionality we have today in a non-intrusive agentless approach. That said, we believe an agent will be required at some point to cover all bare metal not covered by SDN and some public cloud platforms. At the end of the day, I think enterprises are desperate to find "one pane of glass" through which they can achieve a consistent approach to security across the enterprise.

EA: Do you see many differences in the required security solutions for proprietary cloud operating systems like VMware versus emerging open source virtual platforms?

DK: From a Catbird perspective, we believe enterprises should aim for a consistent approach to automated security policy deployment, monitoring and enforcement across all hybrid IT platforms, including all hypervisor variations. We are working diligently to make this possible in terms of improved visibility into the workloads and automated protection of the workloads. Yes, there are differences in how Catbird integrates with the various platforms an enterprise may elect to adopt, but we strongly believe enterprises will ultimately choose the solutions provider who can deliver the consistency of how policies are defined and applied across all platforms, ultimately managed through a single pane of glass.

EA: You've been in the cybersecurity industry for many years. Are you optimistic that the global IT community can start to more effectively counter these nation-state APT attacks? Or do you think we might simply be doomed?

DK: I am optimistic, but improved cyber security is dependent upon enterprises embracing the organizational change in conjunction with tools adoption to be more

effective. The status quo enterprise perimeter approach is demonstrably inadequate at stopping cyber attacks and new infrastructure protection platforms and tools such as from Catbird now exist which can significantly improve the enterprise cyber security posture with a full defense in depth approach. We're looking forward to seeing organizations lean into the new paradigm and improve both security and efficiency.