angelbeat
bringing the cloud down to earth

Little Rock January 26 Agenda

8:40 - 9:30: Registration Begins, Coffee and Snacks Served, Exhibit Area Open with Product Demonstrations, Time For Peer Networking/Interaction

9:30 – 9:50: The Challenges and Solutions for Securing Public Cloud Computing with RedLock
Security and compliance risks involved in cloud computing threaten your organization's ability to drive digital business transformation. Traditional security approaches cannot be applied to modern public cloud infrastructure. Here's why.

- Existing security processes break down in the DevOps era, where software is updated on a daily if not weekly basis, often without any security oversight, leaving you exposed with every release.

- Shared Security Responsibility of public cloud infrastructure. Cloud service providers are responsible for securing physical infrastructure. But you are responsible for securing and monitoring the network, user and resource configurations. And if you leverage multiple cloud service providers, your job just got a lot more complicated.

- Traditional security tools based on rigid policies fail in dynamic cloud environments, where for instance IP addresses are not fixed and 8constantly changing. Moreover, agent or proxy-based solutions will not work with API-driven services such as Amazon RDS, Amazon S3, and Elastic Load Balancing.

- Building custom or proprietary solutions are costly and unreliable. Point security tools provide visibility into configuration issues, user activities, or network traffic in isolation. However, assessing the true risk across your entire public cloud infrastructure requires correlation across these data sets to produce context around issues. You can achieve this by aggregating SIEM data, although extracting actionable insights involves complex correlations and artificial intelligence.

Fortunately Tom Gore from RedLock offers a proven solution that enables effective threat defense across Amazon Web Services, Microsoft Azure, and Google Cloud environments. The RedLock Cloud 360™ platform takes a new AI-driven approach that correlates disparate security data sets including network traffic, user activities, risky configurations, and threat intelligence, to provide a unified view of risks across fragmented cloud environments. With RedLock, organizations can ensure compliance, govern security, and enable security operations across cloud computing environments.

9:50 – 10:10: Integrating Managed Intrusion Prevention with Active Threat Intelligence For More Effective Layered Security, with Sentinel IPS
The term 'Threat Intelligence' is getting a lot of buzz these days, but what does it mean? And more importantly, how can it help protect your network?

Ted Gruenloh, Chief Operating Officer at Sentinel IPS, will answer these questions, within the context of a layered security approach that integrates managed Intrusion Prevention Systems plus Active Threat Intelligence, with existing security methodologies. There will be real-world examples that illustrate how Threat Intelligence improves a network's defenses at the perimeter, while allowing administrators to gain more visibility on the inside.

10:10 – 10:30: Open Converged Infrastructure for Hybrid Clouds with Datrium
Gone are the days that IT staff want to configure, manage and troubleshoot their infrastructure. IT administrators demand simplicity; all that matters is that applications run simply, reliably and fast.

Hyperconverged Infrastructure ("HCI") took a first step towards enabling this new computing paradigm, which according to Gartner will reach $10 Billion in sales by 2021.

The next step is Open Converged Infrastructure ("OCI"), which provides a powerful, cost-effective yet simple approach to increasing system/application performance under increased workloads. This new breed of convergence is:

- Simpler than Hyperconverged without vendor lock-ins
- Faster than All Flash Arrays
- No Backup Silos

Covering this highly relevant content is Brian Lester from Datrium, which delivers a new breed of tier 1 converged infrastructure with consumer-grade simplicity by combining compute, primary and secondary storage, and cloud backup into a single platform. Datrium DVX extends beyond HCI to address both mission critical, low latency workloads as well as backup and cloud data management for hybrid clouds.

10:30 – 10:50: Reduce TCO By 80% With Optimized Data Protection & Secondary Storage, from Cohesity
Traditional secondary storage is fragmented and inefficient. It consumes about 80% of enterprise storage capacity as data is copied on average 10 to 12 times across individual storage appliances in support of different use cases like backup, analytics, test/dev, files and objects. To move data to the public cloud, organizations have to deploy yet another silo in the form of a cloud gateway.

Cohesity transforms this complex infrastructure with a simple, elegant solution. The Cohesity DataPlatform eliminates secondary storage silos with a single, purpose-built hyperconverged platform. It enables organizations to cut their total cost of ownership by 80% or more compared to traditional solutions.

This technical and informative session will feature data center and storage subject matter expert Darren Anderson

10:50 – 11:10: Deliver a Secure Digital Workspace, from any Cloud or Infrastructure, with Citrix
A secure digital workspace is a flexible and integrated way to deliver and manage the apps, desktops, data and devices your users need in a contextual and secure fashion. A unified, contextual and secure digital workspace enables you to do all of this and realize the full benefits of hybrid- and multi-cloud environments while simplifying management and overcoming security challenges.

A complete secure digital workspace must be:

- Unified: IT can configure, monitor, and manage your entire technology infrastructure through a single pane of glass to deliver a unified user experience.

- Contextual: Digital workspaces use machine learning to adapt to each worker's patterns and exceptions so they can get work done securely, wherever they are.

- Secure: A secure digital perimeter grants safe access and full visibility across the network and user ecosystem, and includes predictive analytics, so you can proactively address threats.

This incredibly powerful technology architecture will be covered by Doug Darby, Technology Manager at Citrix, together with Richard Faulkner, Solution Architect at SageNet, a leading systems integrator/consultant.

11:10 – 11:30: Managing and Optimizing a Multi-Vendor Public Cloud Architecture with Oracle Dyn
When organizations migrate their applications and data to the cloud there is risk in having a single point of failure for the entire business. Organizations that rely on just one cloud provider, be it Amazon, Google, Microsoft or another firm, are at their mercy; the financial and strategic impact from a disruption can be catastrophic.

JR Jones, a solutions engineer at Oracle Dyn, will help you understand cloud providers, offer highly relevant and current insights into their performance, reliability and security, plus provide recommendations for implementing a multi-vendor public cloud architecture.

Oracle Dyn is a pioneer in managed DNS and a leader in cloud-based infrastructure that connects users with digital content and experiences across a global internet. Its solution is powered by a global network that drives 40 billion traffic optimization decisions daily for more than 3,500 enterprise customers, including preeminent digital brands such as Netflix, Twitter, Linkedin and CNBC. Dyn's best-in-class DNS and email services, together with the Oracle cloud computing

platform, provides organizations with a one-stop shop for Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

Lunch is Served, Exhibit Area and Product Demonstrations Open, Peer Networking

12:00 – 12:20: Bitcoin and Blockchain: The Future of Digital Contracts, Microsoft Azure Blockchain-as-a-Service Cloud Capabilities
Shawn Weisfeld, world-renowned Cloud Architect/Technology Evangelist at Microsoft, takes you on an easy-to-understand journey of Blockchain technology. Blockchain is the basis of Cryptocurrencies such as Bitcoin. However, you want to get beyond the hype of Bitcoin and understand how Blockchain's future influence/impact extends way beyond cryptocurrencies, as an open-source framework for Smart Contracts.

Blockchain is an emerging way for businesses, industries, and public organizations to almost instantaneously make and verify transactions—streamlining business processes, saving money, and reducing the potential for fraud. At its core, a blockchain is a data structure that's used to create a digital-based, distributed transaction ledger that, instead of resting with a single provider, is cryptographically secured and shared among a distributed network of computers.

The result is a more open, transparent, and publicly verifiable system that will fundamentally change the way we think about exchanging value and assets, enforcing contracts, and sharing data across industries. The applications using blockchain are almost limitless, ranging from loans, bonds, and payments to more efficient supply chains to even identity management and verification.

12:20 - 12:40: Artificial Intelligence, Machine Learning, Big Data, Internet-of-Things with Microsoft
In just the last few years, data from myriads of different sources have literally and exponentially exploded, with a corresponding shift towards massive on-demand storage and computing in public clouds such as Azure and AWS. For instance, with just an internet-connected browser, the Cortana Analytics Suite gives you the ability to ingest enormous volumes of data in real time, store exabytes of unstructured or structured data, orchestrate complex data flows, create operationalized machine learning models almost trivially using drag and drop, and easily take advantage of rich visualization and dashboarding capabilities. You can even use sophisticated perceptual APIs for things such as face or speech recognition to create solutions that would have been unthinkable just a few years ago.

During this technical, educational, interactive and highly relevant session, Shawn Weisfeld, world-renowned Cloud Architect/Technology Evangelist at Microsoft, will share insights on the future of Big Data, Internet-of-Things (IoT) and related topics, giving you valuable recommendations on transforming raw data into actionable insights and valuable information for your organization. Some specific topics covered include:

- Evolve ahead of your competitors by building advanced analytics and machine learning into your business applications
- Scale up analytics with peace of mind, by leveraging cloud-based computing resources with built-in security, to easily manage complex data streams
- Leverage data analytics to better market to customers, enable more personalized messaging, drive better targeting, improve customer engagement, and there grow sales
- Seamlessly integrate existing IT Infrastructure, applications and security/compliance products with newly created Big Data/IoT/AI applications

12:40 – 1:00: Understanding Spectre and Meltdown vulnerabilities within Azure Cloud and Windows **from Microsoft**
In early January, security researchers uncovered Meltdown and Spectre vulnerabilities tied to hardware chip design.

On a phone or a PC, this means malicious software could exploit the silicon vulnerability to access information in one software program from another. These attacks extend into browsers where malicious JavaScript deployed through a webpage or advertisement could access information (such as a legal document or financial information) across the system in another running software program or browser tab. In an environment where multiple servers are sharing capabilities (such as exists in some cloud services configurations), these vulnerabilities could mean it is possible for someone to access information in one virtual machine from another.

Within the Azure cloud platform, Microsoft and its silicon partners have already implemented many updates to Windows and silicon microcode, such as new CPU instructions that eliminate branch speculation in risky situations.

Because Windows clients interact with untrusted code in many ways, including browsing webpages with advertisements and downloading apps, our recommendation is to protect all systems with Windows Updates and silicon microcode update. For example Windows Server administrators should ensure they have mitigations in place at the physical server level, to ensure they can isolate virtualized workloads running on the server.

One of the questions for all these fixes is the impact they could have on the performance of both PCs and servers. On newer CPUs such as on Skylake and beyond, Intel has refined the instructions used to disable branch speculation to be more specific to indirect branches, reducing the overall performance penalty of the Spectre mitigation. Older versions of Windows have a larger performance impact because Windows 7 and Windows 8 have more user-kernel transitions because of legacy design decisions, such as all font rendering taking place in the kernel.

1:00 – 1:45: Integrated Datacenter and Private/Public/Hybrid Cloud Infrastructure Design, Security/Compliance Considerations, with Amazon Web Services
AWS pioneered cloud computing in 2006, creating cloud infrastructure that allows you to securely build and innovate faster. AWS is continuously innovating the design and systems of our data centers to protect them from man-made and natural risks. Then we implement controls, build automated systems, and undergo third-party audits to confirm security and compliance. As a result, the most highly-regulated organizations in the world trust AWS every day.

The Infrastructure Layer is the data center building and the equipment and systems that keep it running. Components like back-up power equipment, the HVAC system, and fire suppression equipment are all part of the Infrastructure Layer. These devices and systems help protect servers and ultimately your data. Drew Dennis, Solutions Architect at Amazon Web Services, will talk about the types of security measures AWS deploys in the Infrastructure Layer of its data centers like maintaining equipment and emergency ready back up equipment.

End of Presentations/Event, Raffle Prize Drawings, Product Demonstration and Exhibit Area Remain Open