angelbeat

bringing the cloud down to earth

OKC Jan 23 Agenda

7:30 - 8:50: Registration Begins, Breakfast, Coffee and Snacks Served, Exhibit Area Open with Product Demonstrations, Time For Peer Networking/Interaction

8:50 – 9:10: 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.

9:10 – 9:30: The Challenges and Solutions for Securing Public Cloud Computing and DevOps 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.

9:30 – 9:50 Improving Network/Application Resilience and Performance, Given Recent Internet Outages with

ThousandEyes

Recent Internet outages, caused by DDoS, Route Leaks and other cybersecurity attacks, plus natural/weather disasters and other factors, have impacted Amazon's S3 file storage service (Feb 2017), Dyn's DNS service (Oct 2016), and other infrastructure/technology providers, causing large-scale disruptions of mission-critical SaaS, IaaS and internally-hosted services.

During this technical, informative and highly informative session featuring Rob Danz, Senior Solutions Engineer at ThousandEyes, you will learn how to respond to these issues **before** they impact your customers, services and revenue, ensuring that your organization runs smoothly. You can quickly and precisely pinpoint the root cause of problems, then immediately share these insights with your vendors and customers.

ThousandEyes is a Network Intelligence platform that delivers visibility into every network an organization relies on, enabling them to optimize and improve application delivery, end-user experience and ongoing infrastructure investments. Leading companies such as ServiceNow and Twitter, as well as eBay and other members of the Fortune 500, use ThousandEyes to improve performance and availability of their business-critical applications.

9:50 - 10:15: Private/Public/Hybrid Cloud Strategies, Microsoft Support for Both Linux & Windows Dockers/Containers, DevOps Benefits, Integration with Microsoft Azure Cloud Services

Shawn Weisfeld, world-renowned Cloud Architect/Technology Evangelist at Microsoft and a dynamic/engaging presenter, is the featured keynote speaker. His session begins with an overview of Microsoft's Azure public cloud platform, including some newly released features plus strategies for integrating Azure with onsite hardware and software computing resources as Windows Server 2016. He will present a framework to help you design an optimal private, public and/or hybrid cloud strategy for your organization.

His presentation then transitions to Dockers and Containers, which are widely deployed for cloud applications. He starts with a technical assessment of the similarities and differences amongst Containers, Serverless and Virtual Machine cloud architectures, followed by a walk through/demonstration of enabling, creating, deploying and managing Linux and/or Windows containers/dockers resources. There will be an evaluation of when to use which containers, why and how. FYI, a container is an isolated and portable operating environment, often viewed as the next evolution of virtualization that works at the Operating System (not Hardware) level. It provides a mechanism for IT to deploy services in a portable, repeatable and predictable manner.

For those who are new to containers, this content serves as a jumpstart to accelerate your learning of containers. If you already have experience on Linux containers, the session familiarizes you with the specifics of Windows containers, plus helps bridge and extend your skills for bringing business value to both Linux and Windows communities. Finally, these insights will greatly enhance your organization's DevOps initiatives.

Coffee and Snack Break, Product Exhibition and Demonstration Area Open, Peer Networking

10:45 – 11:10: 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.

11:10 - 11:35: 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

11:35 – 12:00: 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.

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