Cloud Native Security; Explained

Tanya Janca
CEO and Co-Founder – Security Sidekick
What are we going to talk about today?

Cloud
What are we going to talk about today?

Cloud Native
What are we going to talk about today?

Cloud Native Security
Warning:

This talk is interactive, and I expect audience participation.
This is me.

AKA: @SheHacksPurple

I’m Tanya Janca.

Security Sidekick
CEO & Co-Founder!

WoSEC
Let’s learn stuff!
What IS Cloud?

MY CODE DOESN'T WORK

LETS CHANGE NOTHING AND RUN IT AGAIN
Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.
Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.

Wikipedia
Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, **without** direct active management by the user.
What do I mean by that?
Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.
What is Cloud Native?

Stuff that is designed specifically to run in the cloud.
Cloud Native

Applications and services that automate and integrate the concepts of continuous delivery/integration/deployment, DevOps, microservices, serverless, and containers.
What’s the difference?

Cloud VS Data Center ("on prem")
Traditional Data Center

- Manual Patching and Management
- On-Premise (your responsibility)
- “Bare metal”, physical machines
- Run your own network: Intranet
- You run AC/power/backups/everything
- You need ops staff, on call
- Offsite BCP/Disaster Recovery is advised
- Over provisioning (planning for growth)
- Apps deployed on specific servers
Cloud

- Off Premise (not your responsibility)
- Auto-scaling, no need to buy in advance
- Usually Internet available
- Infrastructure as a Service (IaaS)
- Apps can span different servers
- Maintenance is not your problem
- Centralized management/visibility
- Geographically distributed
- Lights-out
## Traditional Data Center VS Cloud

<table>
<thead>
<tr>
<th></th>
<th>Traditional Data Center</th>
<th>Cloud Data Center</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Servers</strong></td>
<td>Co-located&lt;br&gt;Dependent Failure</td>
<td>Integrated&lt;br&gt;Fault-Tolerant</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td>Partitioned&lt;br&gt;Performance Interrelated</td>
<td>Unified&lt;br&gt;Performance Isolated</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>Separated&lt;br&gt;Manual</td>
<td>Centralized Full Control&lt;br&gt;With Automation</td>
</tr>
<tr>
<td><strong>Scheduling</strong></td>
<td>Plan Ahead&lt;br&gt;Overprovisioning</td>
<td>Flexible&lt;br&gt;Scalable</td>
</tr>
<tr>
<td><strong>Renting</strong></td>
<td>Per Physical Machines</td>
<td>Per Logical Usage</td>
</tr>
<tr>
<td><strong>Application / Services</strong></td>
<td>Fixes on Designated Servers</td>
<td>Runs and Moves across All VMs</td>
</tr>
</tbody>
</table>

### Cloud Computing:
- **End Device / Client**
- **Common App. Platform**
- **Cloud Data Center**

### Cloud DC Requirements:
- On-Demand Self-Service
- Resource Pooling
- Rapid Elasticity

- Measured Usage
- Broad Network Access
- Network Dependent
And now for my favorite topic... Security!
Traditional Data Center Security

- Zoning
- Manual Patching and Patch Management
- Physical Security
- Usually requires 3rd party scanning software (Nessus, Nexpose, Nikto, etc)
- You maintain trained Ops and Sec teams
- Many third-party monitoring/sec tools
Cloud Native

Applications and services that automate and integrate the concepts of DevOps, continuous integration/deployment/delivery, microservices, serverless and containers.

It is NOT copying everything from your traditional datacenter directly into someone else’s datacenter.
You're pretty new to cloud storage, aren't you?
Cloud Native Security

- Zero Trust
- Just in Time access control
- Automation for Patching & Patch Management
- Total visibility and threat monitoring
- Automation of security during the SDLC
- Monitoring of everything, with automated responses
- Better resilience means the ‘A’ in CIA
- Security as Code
Cloud Native Security

- DevSecOps
- Using serverless & logic apps to protect yourself
- Writing playbooks for automated security responses
- Using Cloud Native Security tools, such as Native SIEM, Native Threat Detection/Protection and Native Firewalls.
- Less Heroics = Happier Staff
- Happier Staff = Less Turnover
Trust
Resources: OWASP DevSlop Has Your Back!

DevSlop.co https://aka.ms/DevSlopShow
Resources: Mentoring

#Mentoring Monday

EVERY MONDAY!
Resources: Open Web Application Security Project

#OWASPlove
https://owasp.org
Women of Security welcomes you!

WoSEC

Paris, Ottawa, San Francisco, Singapore, Dallas, Houston, Austin, Vancouver, Portland, Ottawa, Chicago, Bangalore, Boise, Montréal, Zurich, Nairobi, Johannesburg, Stockholm, Victoria, Milwaukee, Detroit, Denver, Barcelona, Madrid

Canada, France, USA, India, Switzerland, Kenya, South Africa, Sweden, Spain

@WoSECTweets
Resources: Hands-On Workshop!

Online Workshop Invite

aka.ms/Cloud-Workshop-Video

FREE!
Follow me?

Twitter: @SheHacksPurple

https://medium.com/@SheHacksPurple
https://dev.to/SheHacksPurple
https://YouTube.com/SheHacksPurple
https://mailchi.mp/e2ab45528831/shehackspurple
THANK YOU

Tanya Janca
Security Sidekick
CEO and Co-Founder

FOR BEING FABULOUS

@SheHacksPurple