The Next Generation CYBER Infrastructure

Scottie Ray
@H20nly
sray@vmware.com
Staff Systems Engineer
VMware Network & Security Team
Public Sector

© 2017 by presenter’s organization. Published by The Aerospace Corporation with permission.
“The Empire doesn't consider a small one-man fighter to be any threat, or they'd have a tighter defense. An analysis of the plans provided by Princess Leia has demonstrated a weakness in the battle station. ...The shaft leads directly to the reactor system. A precise hit will start a chain reaction which should destroy the station.”

--General Dodanna

A Long Time Ago...In a Galaxy Far Far Away...
Trading Off Context and Isolation

Any Application

Compute Abstraction Platform

Any x86

Any Storage

Any IP network

Application

OS

Hypervisor

High Context

Low Isolation

High Isolation

Low Context

Traditional Approach

No Ubiquitous Enforcement

High Context

Low Isolation

High Isolation

Low Context
We Need to Adapt Our Thinking to Leverage the Distributed Reality
Trusted Service Insertion to Go Beyond a Firewall

- **External Network**
- **Workload**
- **Trusted Service Partner**
- **Traffic Redirection Module**
- **Slot 2**
- **Slot 4**
- **Slot 5**
Trusted Service Insertion’s Role in a CYBER-Resilient Infrastructure

Policy Definition

**Standard VM Policy**
- Anti-Virus – Scan

**Quarantined VM Policy**
- Firewall – Block all except security tools
- Anti-Virus – Scan and remediate

Security Group = **Quarantine Zone**
Members = \{Tag = ‘ANTI_VIRUS.VirusFound’, L2 Isolated Network\}

Security Group = **EGS Mission “A”**
Leveraging the Inherent Value of Distribution

Confidentiality, Integrity, Authenticity
...for east/west traffic, applied to micro-segments

Operational Simplicity
...key management, service insertion, user experience

Any application topology
...private/public clouds, physical, containers
The Velocity of Change…
Thank You