Re-Think Security

Kirk House

Cloud Security Alliance - SDP Enterprise Working Group
Global Director, Enterprise Architecture - The Coca Cola Company
If Only I Could…

Reduce cyber risk
Traditional point products are not stopping malicious cyberattacks

Improve business agility
IT security needs to find a way to say “yes” to new business initiatives and secure business agility
Everything important is outside the enterprise perimeter but compliance models focus on the inside

Solutions Are Outside (SaaS – PaaS – IaaS)

Workers are Outside

The Enterprise Perimeter is quickly going away
We need to re-think security

Identify the biggest threats & focus on those

Stop utilizing compliance as a strategy

Find ways to pay for security thru cost efficiencies
It’s better for one house to be on fire than the entire city!!!

Cloud allows for much easier application isolation
Step #1: Trust No One

Identifying threats is the first step to having real security.

What is going on?

What am I doing?

Where is my risk?

How are attackers getting in?
Step #2: Trust Nothing

1. **Isolate** each application, so *it’s invisible to everyone*
2. **Verify** user authenticity and authorization, and device and software integrity
3. **Connect** the authorized user and trusted device to *only* the protected applications

**Identify devices & users before granting access to your applications**
Step #3: Get A Business Case

Any App, Anywhere
- Internal App Isolation
- Cloud App Protection

Any Device, Managed or Not
- Managed
- UnManaged

Any User, Anywhere
- Internal Employees
- Ecosystem Collaborators

Any Network
- Dedicated Network
- Internet
User Access – As Is

Common Attacks

• Cyber Attack Server exploitation: constant attacks
  Misconfigurations
  Vulnerabilities
  Injections
  Denial of Service

• Credential theft: ⅔ of Verizon DBIR
  Phishing
  Keyloggers
  Brute force

• Connection hijacking: stealthiest
  Man-in-the-Middle
  Certificate forgery
  DNS poisoning

RED Lines are Vulnerable
**Common Attacks**

- Cyber Attack Server exploitation: constant attacks
  - Misconfigurations
  - Vulnerabilities
  - Injections
  - Denial of Service

- Credential theft: ⅔ of Verizon DBIR
  - Phishing
  - Keyloggers
  - Brute force

- Connection hijacking: stealthiest
  - Man-in-the-Middle
  - Certificate forgery
  - DNS poisoning
SDP in a Nutshell

1. Device verification
   - SDP Controller

2. Identity & role verification
   - Identity System

3. Approved access

4. TLS Tunnel Config
   - SDP Gateway

5. Application Access
   - SDP Client

SDP Gateway

Business Solutions
Questions?