SDP™ Software Defined Perimeter Working Group

Software Defined Perimeter

Internet-scale Security for the Internet2 Community

Junaid Islam
Co-Chair SDP Workgroup
Cloud Security Alliance

CSA cloud security alliance℠

The challenge:

How do you secure an open network?

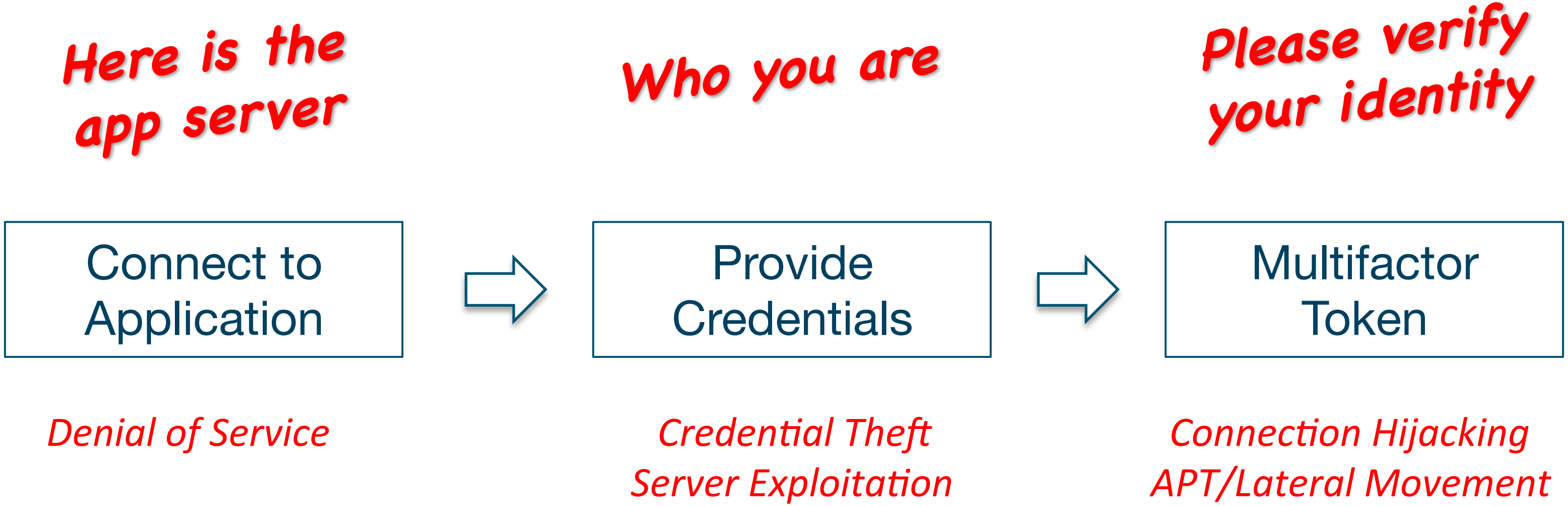
Solution Requirements for Internet2

Open ⇨ No secrets

Large ⇨ Highly scalable

Experimental ⇨ Any infrastructure

Current Perimeter Security Model



Here is the app server

Who you are

Please verify your identity

Connect to Application

Provide Credentials

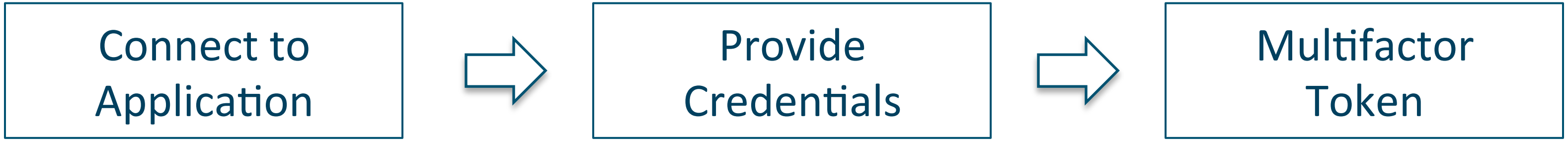
Multifactor Token

Denial of Service

Credential Theft
Server Exploitation

Connection Hijacking
APT/Lateral Movement

Software Defined Perimeter

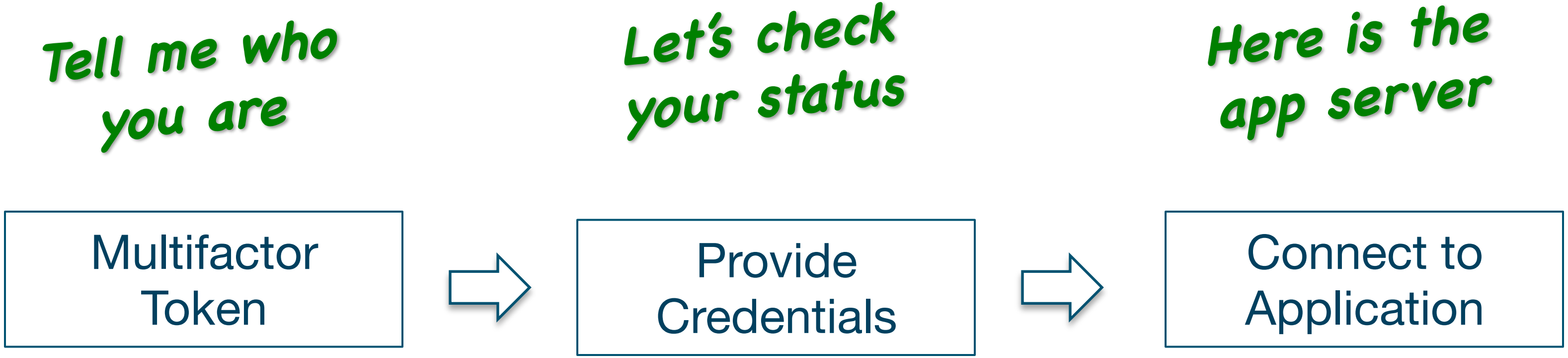


Connect to Application

Provide Credentials

Multifactor Token

Software Defined Perimeter Security Model



Tell me who you are

Let's check your status

Here is the app server

Multifactor Token

Provide Credentials

Connect to Application

SDP Changes The Connection Model for the Internet

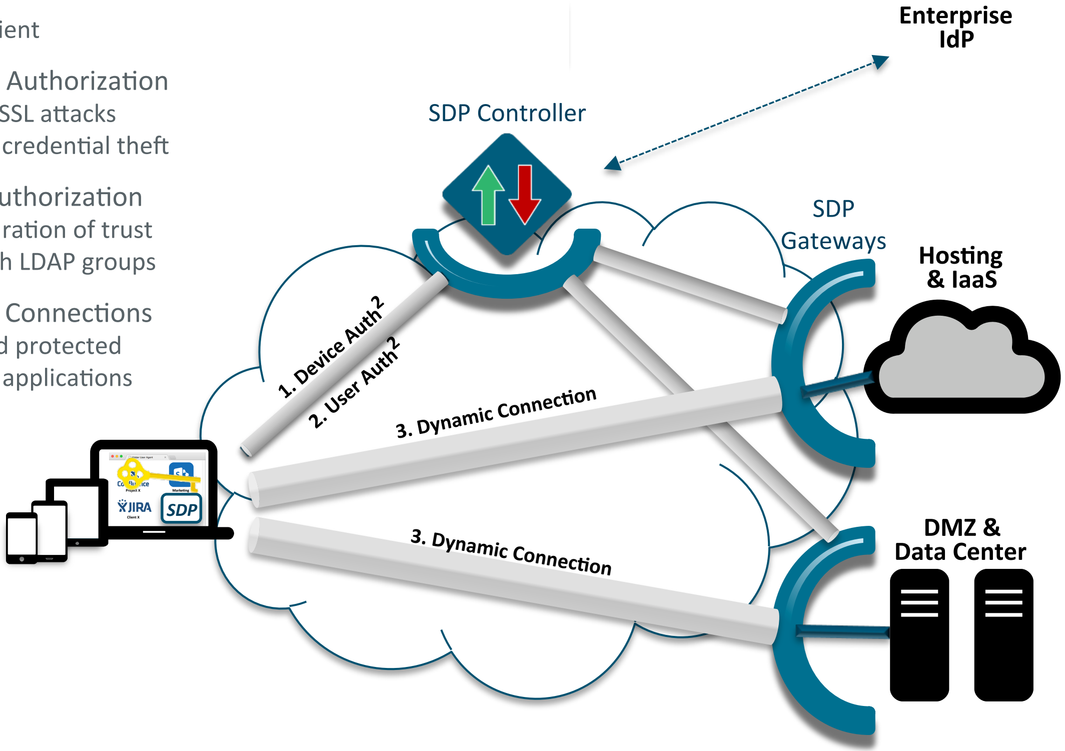
- TCP/IP still works as normal BUT connections are only established with known devices/users

- IP servers are “black” as there is no DNS or open ports to allow cyber attackers to find and connect to servers

- SDP supports SAML federation and can be scaled up leveraging public clouds to stop network attacks

SDP Architecture

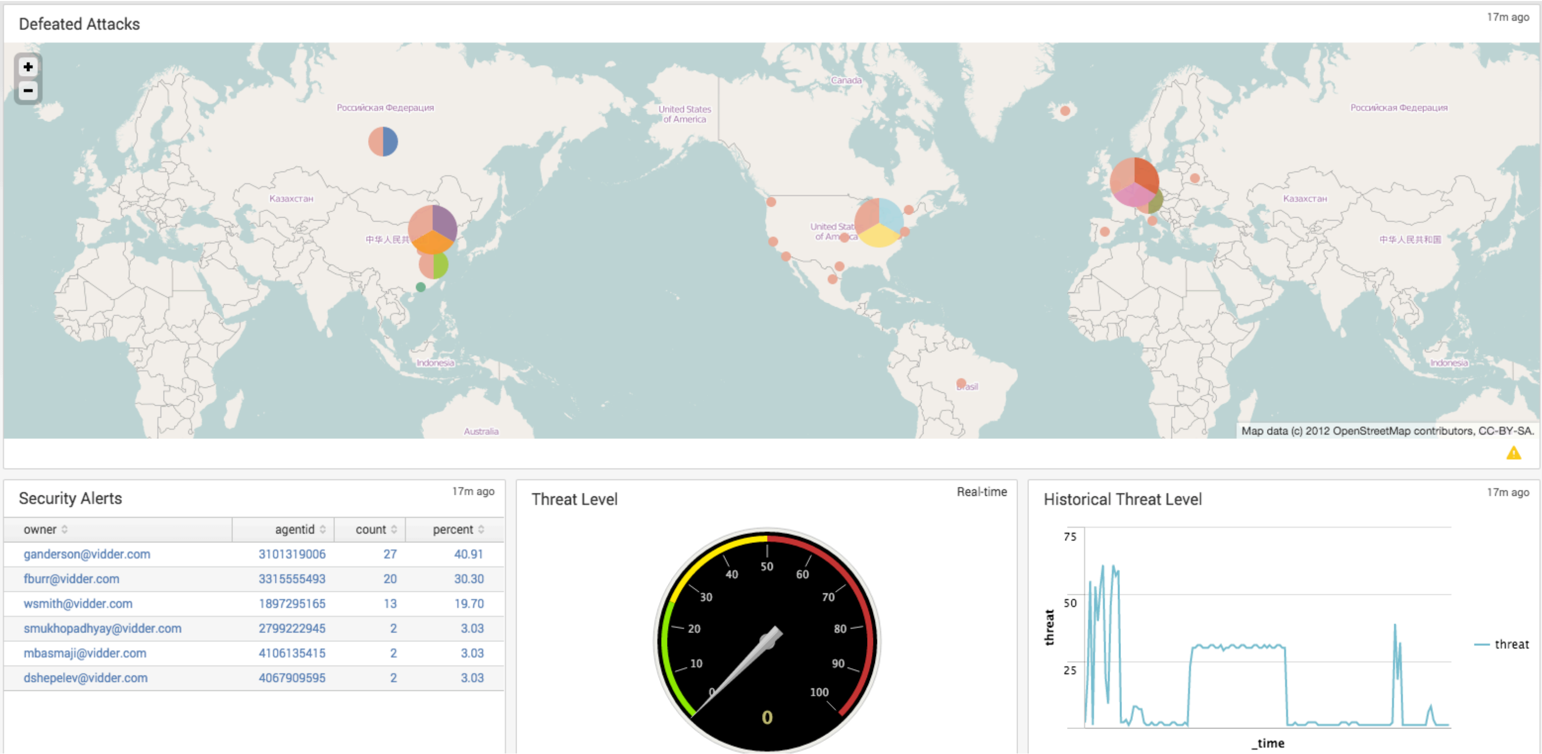
0. One time on-boarding
    - Client root of trust
    - Digital artifacts & thin client
1. Device Authentication & Authorization
    - SPA: anti DDoS, defeats SSL attacks
    - mTLS & fingerprint: anti credential theft
2. User Authentication & Authorization
    - Enterprise identity: separation of trust
    - SAML IdP integrated with LDAP groups
3. Dynamically Provisioned Connections
    - Applications isolated and protected
    - Usability: portal page of applications



Key SDP Features

- 64 bit id is not secret (can be listed)
- SPA can carry payload for Auto/IoT applications
- Attacks can be detected in the first packet

SDP Provides Real Time Threat Detection



Defeated Attacks

17m ago

Map data (c) 2012 OpenStreetMap contributors, CC-BY-SA.

Security Alerts

17m ago

owner	agentid	count	percent
ganderson@vidder.com	3101319006	27	40.91
fburr@vidder.com	3315555493	20	30.30
wsmith@vidder.com	1897295165	13	19.70
smukhopadhyay@vidder.com	2799222945	2	3.03
mbasmaji@vidder.com	4106135415	2	3.03
dshepelev@vidder.com	4067909595	2	3.03

Threat Level

Real-time

Historical Threat Level

17m ago

Attacks on SSL/TLS

Name	Date	Attack	SDP Mitigation
SSLstrip	Feb 2009	http to https	No http
DigiNotar	Sept 2011	MitM forged certs	Pinned certs
BEAST	Apr 2012	Java Applet oracle	Client-based
CRIME	Sept 2012	MitM SPDY compressing oracle	No compression
Lucky 13	Feb 2013	MitM CBC padding oracle	GCM
TIME	Mar 2013	Browser JavaScript timing oracle	Client-based
RC4 biases	Mar 2013	MitM RC4 oracle	No cypher negotiation
BREACH	Aug 2013	Website redirect, compression	No redirect or compression
Triple Handshake	Mar 2014	Server MitM on client cert	Pinned dedicated cert
Heartbleed	Apr 2014	OpenSSL bug	Not single-ended SSL
BERserk	Sept 2014	MitM PKCS#1.5 padding	Not Mozilla NSS
Poodle	Oct 2014	MitM SSLv3 oracle	No cypher negotiation
Poodle++	Dec 2014	MitM JavaScript timing oracle	Client-based
FREAK	Mar 2015	MitM negotiation 512 bit key	No key negotiation
Bar-mitzvah	Mar 2015	View RC4	No RC4
logjam	May 2015	MitM downgrade to 512 bit key	No suite negotiation

Attacks on Enterprises

- Server exploitation : constant attacks
  - Misconfigurations
  - Vulnerabilities
  - Injections
  - Denial of Service
- Credential theft
  - Phishing
  - Key loggers
  - Brute force
- Connection hijacking
  - Man-in-the-Middle
  - Certificate forgery
  - DNS poisoning

DigiNotar Internet Trust Services

500 digital certificates were forged from this Dutch certificate authority. The real-word effect of this attack is still unknown.

TÜRK TELEKOM

Turk Telekom was ordered to hijack Google's DNS servers at IP address 8.8.8.8 by the Turkish government.

SQL Injection **Adobe** on a public website used to gain access to a database of 150K customer password hashes.

Injection attack STRATFOR on the web admin interface resulted in the public dumping of PII of 60K government workers.

CHS Community Health Systems

Heartbleed enabled attackers to VPN into CHS and steal 4.5M patient records.

The New York Times

As a result of a spear phishing attack on Melbourne IT, the website of The New York Times was unavailable for two days.

CYBERVOR

A Russian cyber gang acquired 4.5B stolen credentials, cracked many of the passwords, and posted them online.

A phishing SOUTH CAROLINA DOR DEPARTMENT OF REVENUE attack on an employee of the South Carolina Dept. of Revenue and the resultant credential theft resulted in the loss of 75GB of data.

Hotmail

Chinese attackers performed a massive man-in-the-middle attack on U.S. ISPs stealing unknown amounts of emails and passwords.

Defeating Attacks on the Extended Enterprise

- Server exploitation: constant attacks

  ~~Misconfigurations~~

  ~~Vulnerabilities~~

  ~~Injections~~

  ~~Denial of Service~~

Server Isolation
SPA, Dynamic FW

- Credential theft: ⅔ of Verizon DBIR

  ~~Phishing~~

  ~~Keyloggers~~

  ~~Brute force~~

Transparent MFA
mTLS, Fingerprint

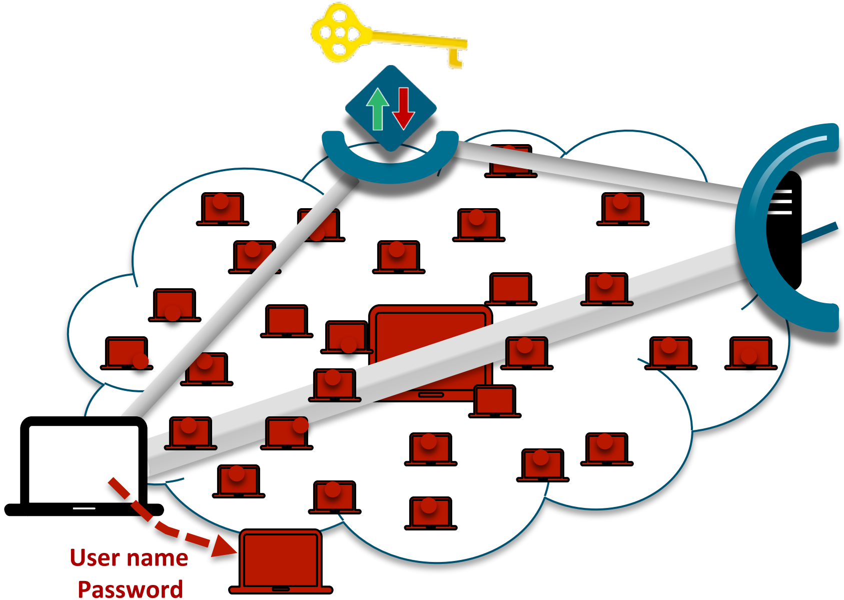
- Connection hijacking: stealthiest

  ~~Man-in-the-Middle~~

  ~~Certificate forgery~~

  ~~DNS poisoning~~

Encryption,
Pinned Certs,
No DNS

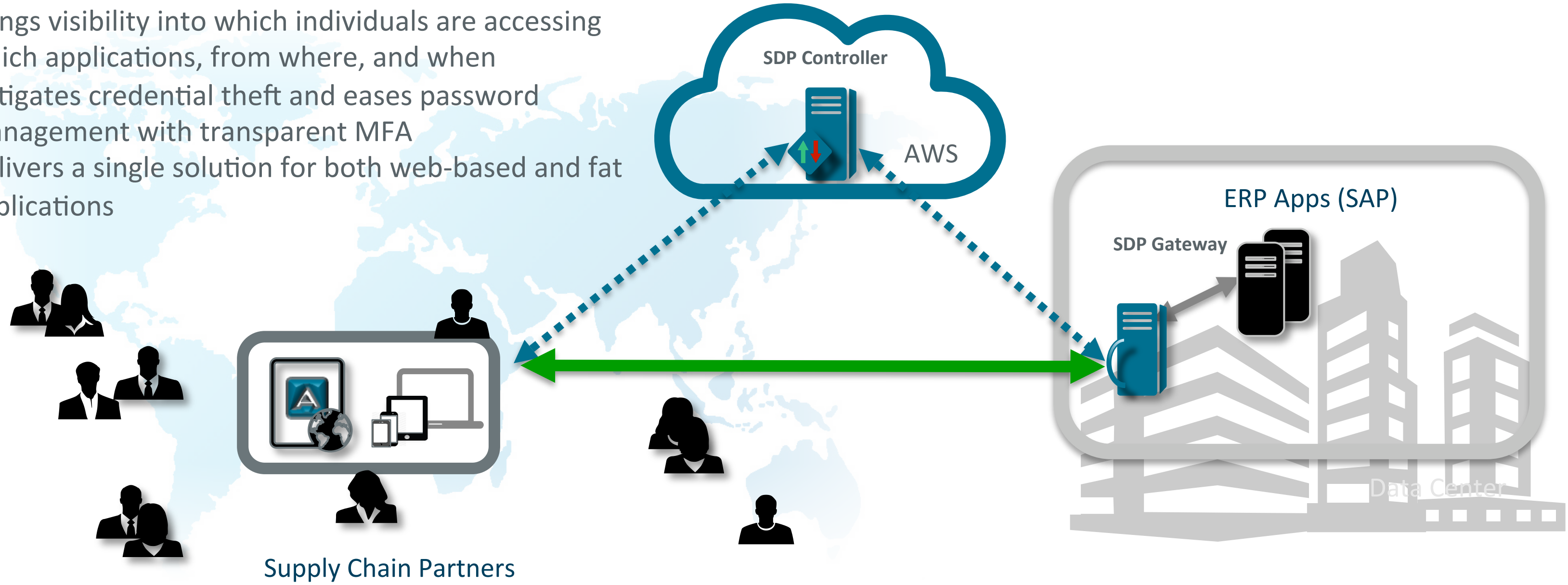


Global Beverage Company

Business Objective: Minimize operational costs and maximize flexibility

SDP Solution:

✓ Secures partner employee access to the required apps
✓ Protects against DDOS and server vulnerability attacks
✓ Brings visibility into which individuals are accessing which applications, from where, and when
✓ Mitigates credential theft and eases password management with transparent MFA
✓ Delivers a single solution for both web-based and fat applications

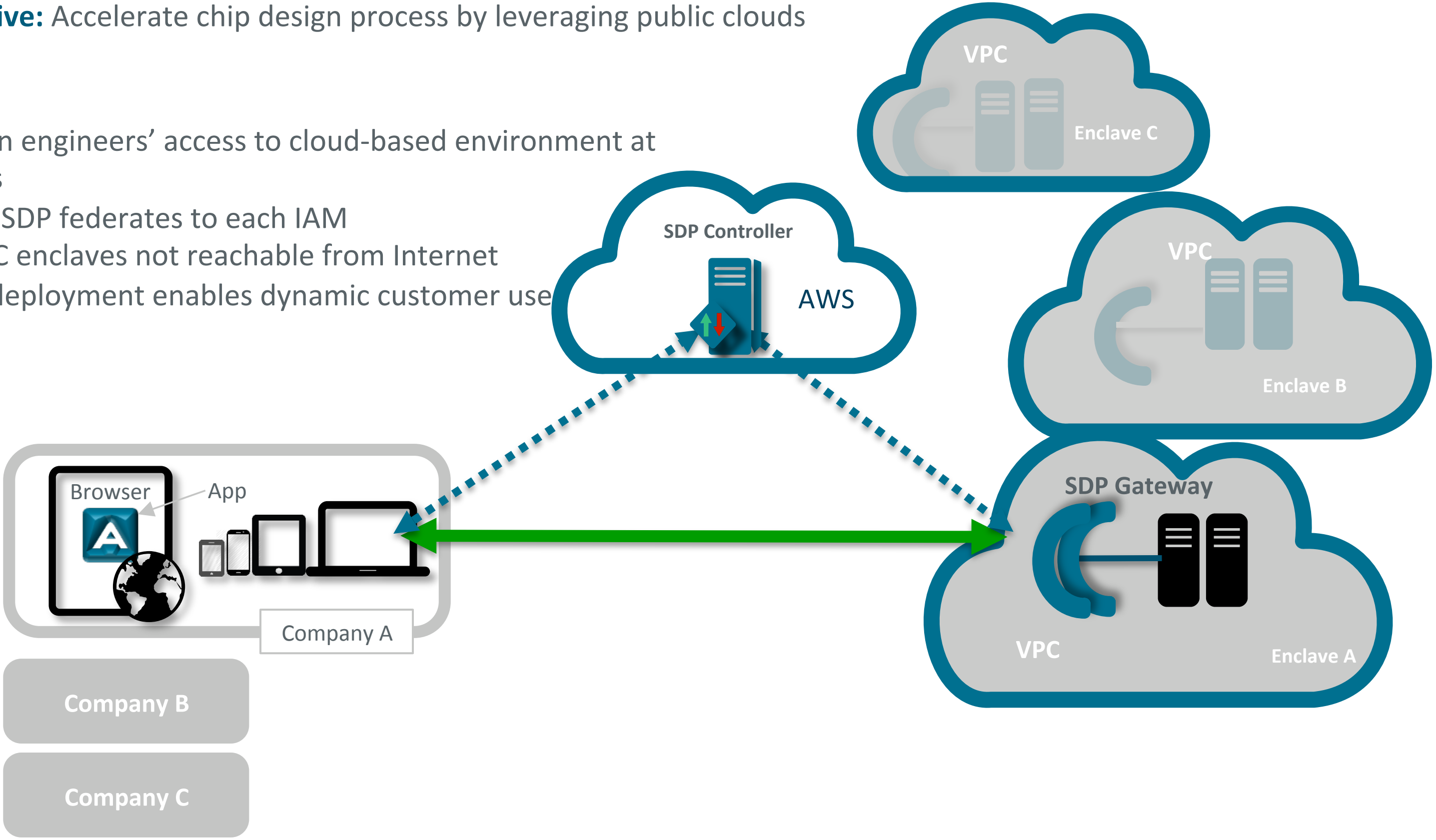


Chip Design Company

Business Objective: Accelerate chip design process by leveraging public clouds

SDP Solution:

- ✓ Secures design engineers' access to cloud-based environment at customer sites
- ✓ Single tenant SDP federates to each IAM
- ✓ Customer VPC enclaves not reachable from Internet
- ✓ Flexible SDP deployment enables dynamic customer use



Global Automotive Company

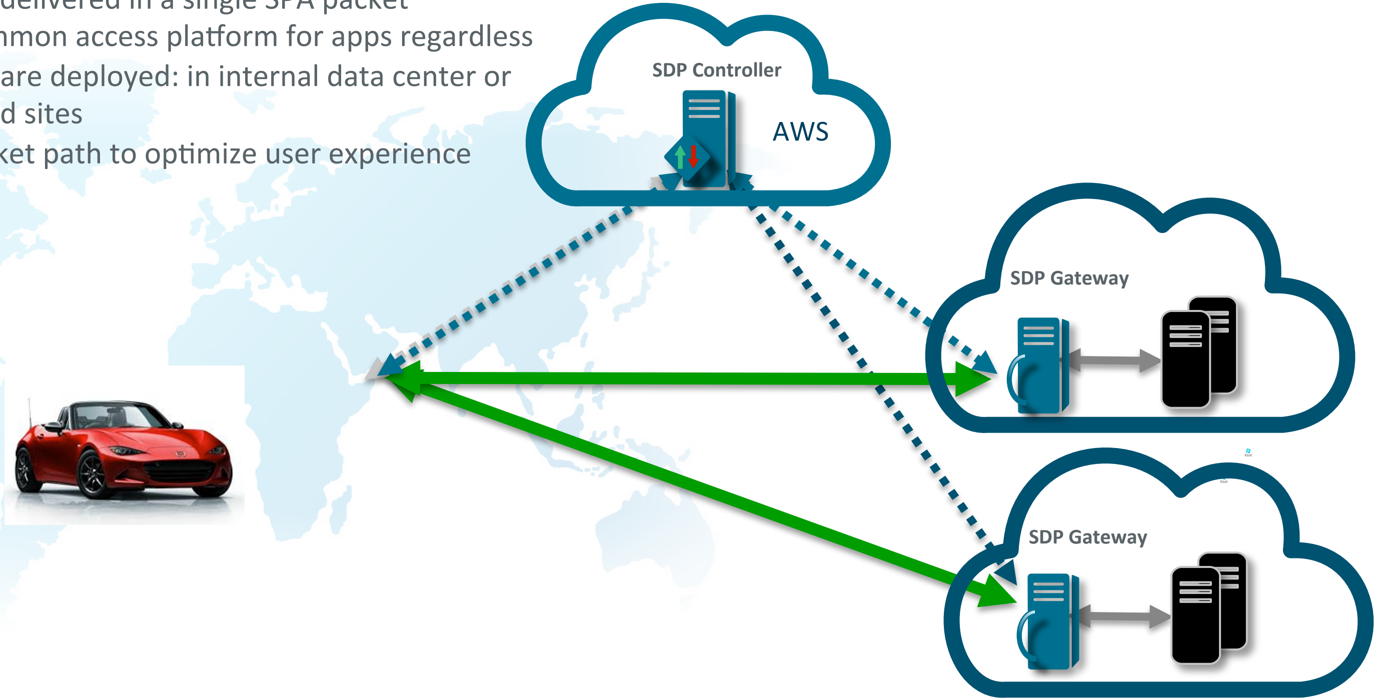
Business Objective: Enable in field vehicle upgrades to retain customers and "sell" new features

SDP Solution:

✓ Vehicle status delivered in a single SPA packet

✓ Provides a common access platform for apps regardless of where they are deployed: in internal data center or (multiple) cloud sites

✓ Optimizes packet path to optimize user experience



Closing comments

- SDP is really simple

- SDP supports a wide range of applications