PrecisionAccess™

Access Control Re-Invented

Josh Pollock
jpollock@vidder.com

VIDDER

Vidder Overview

- Headquartered in Campbell, CA (Silicon Valley).
- We protect some of the world's most sensitive applications.
- Exec team includes co-authors of Software-Defined Perimeter protocol.
- No product breaches including three hackathons (2 RSA; IAPP-CSA Congress)

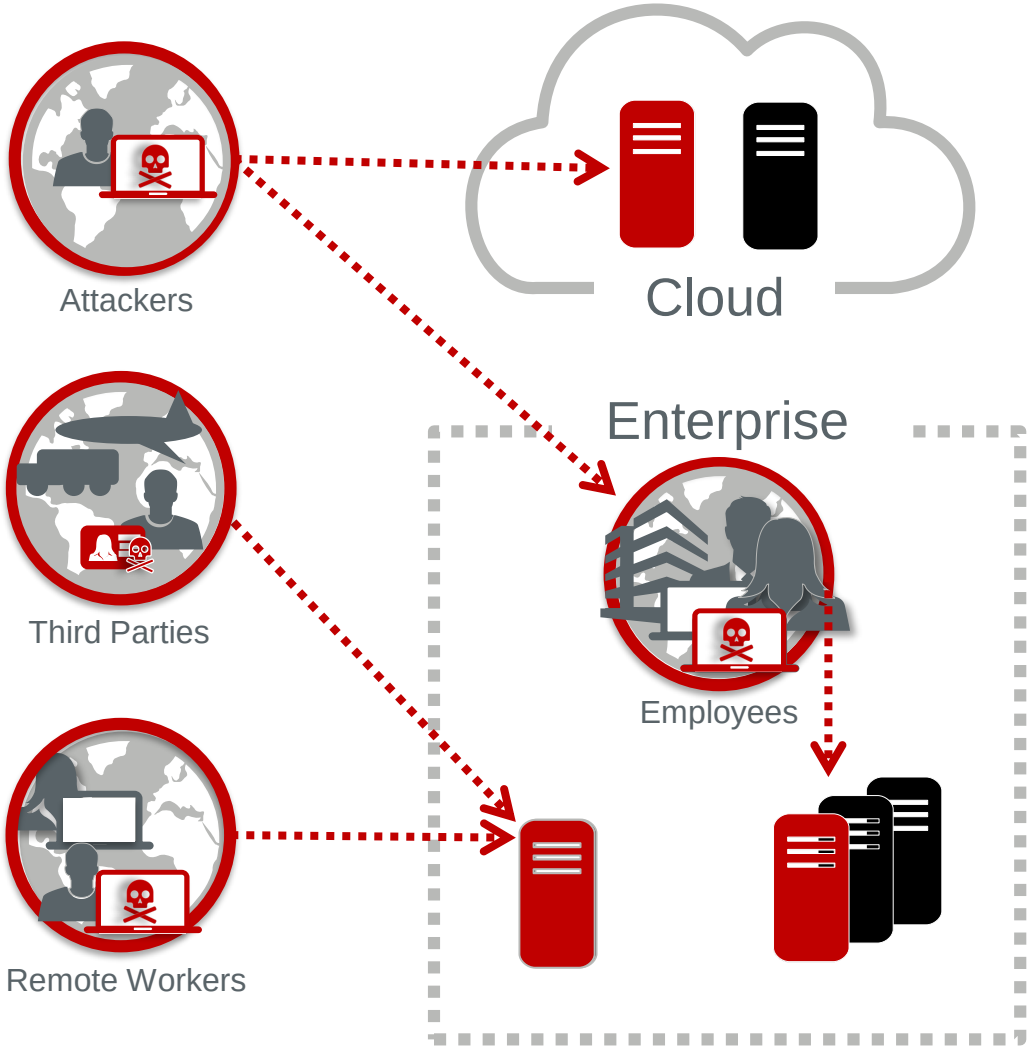
"Vidder enhanced security and allowed us to avoid a costly, time consuming infrastructure upgrade."

CISO- SGN

The Enterprise Perimeter is Dead

Problems with traditional perimeters

1. Sophisticated Attacks	Phishing attacks easily penetrate the perimeter
2. Increased Outsourcing	More untrusted third parties connecting to VPN
3. Cloud Migration	Applications are moving outside to the cloud



The Old-School Approach is Flawed.

VIDDER

Today:

Connect → Log in → MFA

Vulnerable to Server exploitation

Vulnerable to Credential theft

Defeats credential theft, but Painful to users

SDP:

MFA → Verify → Connect

Defeats

1. Credential theft, transparently
2. Server exploitation
3. Denial of Service
4. Infrastructure compromise
5. Connection hijacking
6. Compromised clients

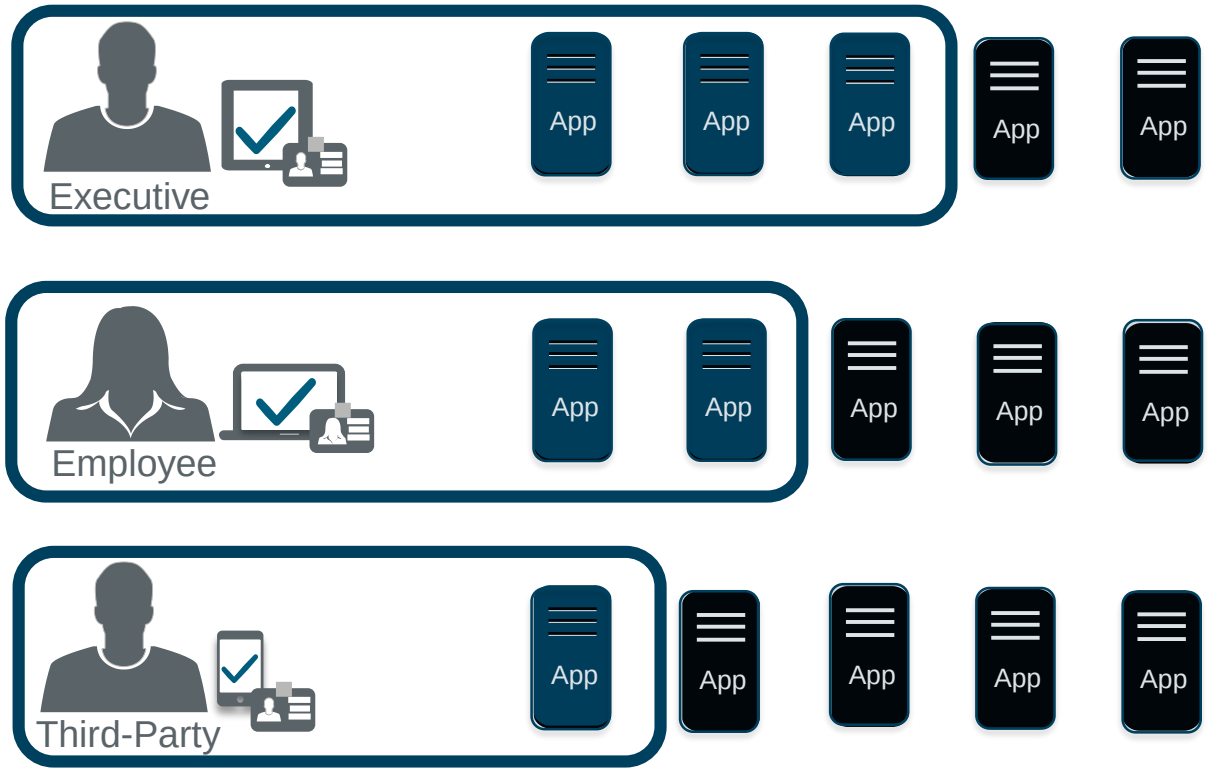
Software Defined Perimeter is the Solution

VIDDER

***Zero Attack Surface** until trust is proven*

Change the rules

1. Isolate	Isolate the Applications
2. Verify	Auth^2 Devices & Users Perform Trust Assessment
3. Connect	Connect Trusted Devices to Trusted Applications



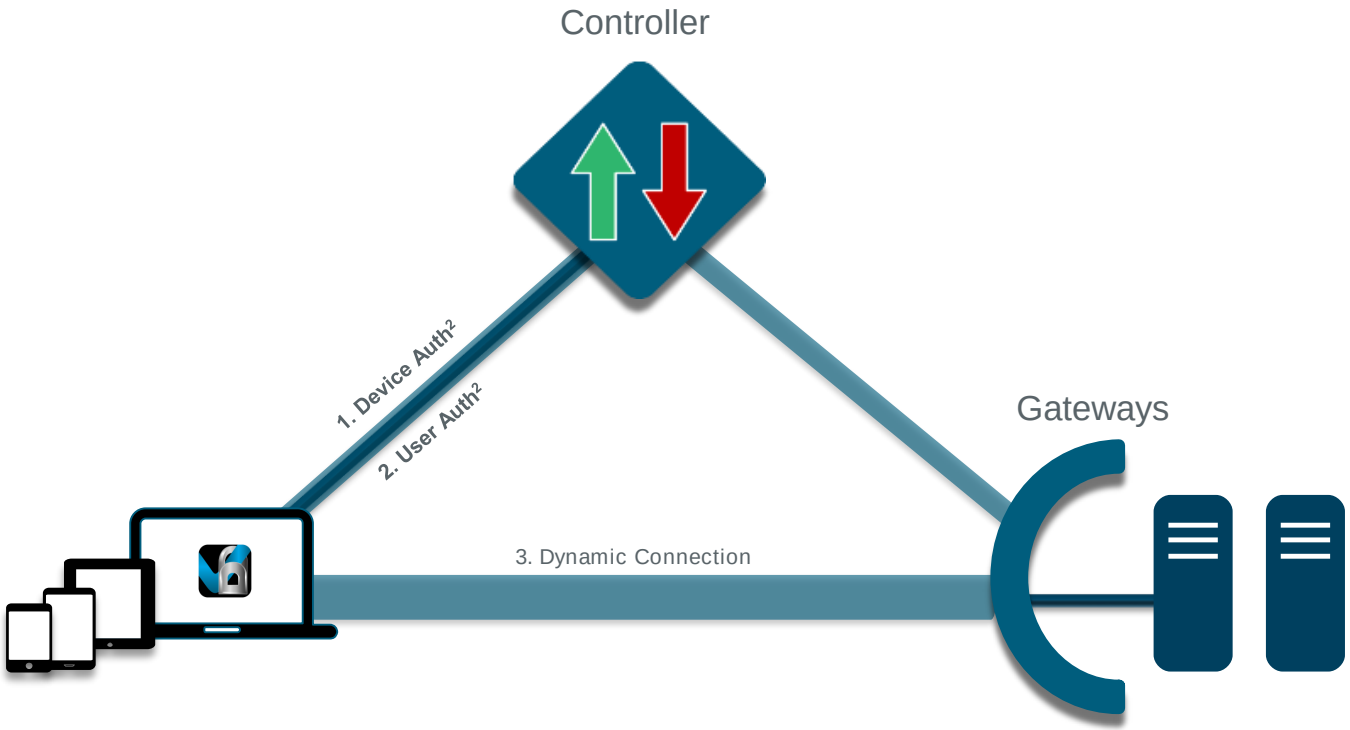
SDP Architecture

Requirements

1. Isolate the servers
2. Control plane for pre-attestation
3. Enable authorized users only

SDP implementation

1. Device authentication, security context
2. User authentication, authorization
3. Dynamically provision connections



SDP Protocol

0. One time on-boarding

Crypto Artifacts
Root of Trust
Thin Client

1. Device Authentication & Authorization

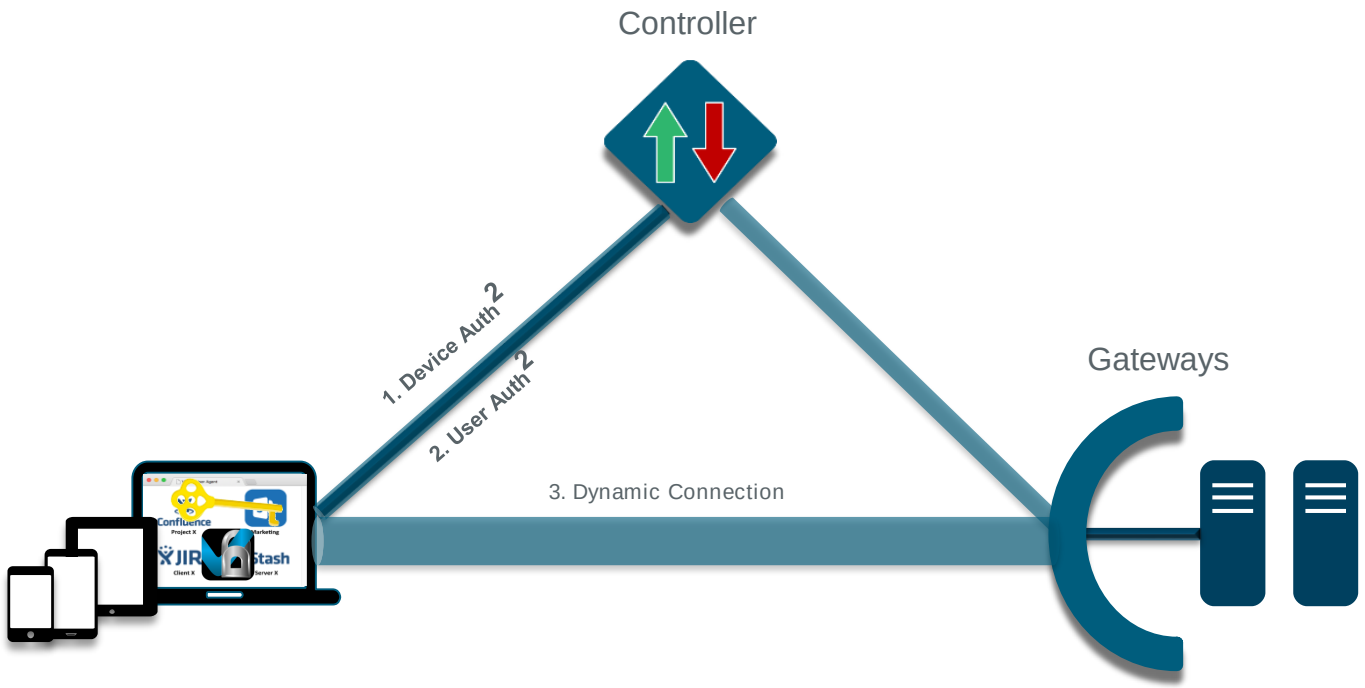
SPA: One-time Password
mTLS & Fingerprint: Device Authentication
Trust Assessor: Context-Aware Authorization

2. User Authentication & Authorization

Authentication: Integrated to Enterprise SSO
Authorization: Derived from AD/LDAP Groups

3. Dynamically Provisioned Connections

Trusted Access: Only enable access to trusted devices
Granular Access: No exposure of network



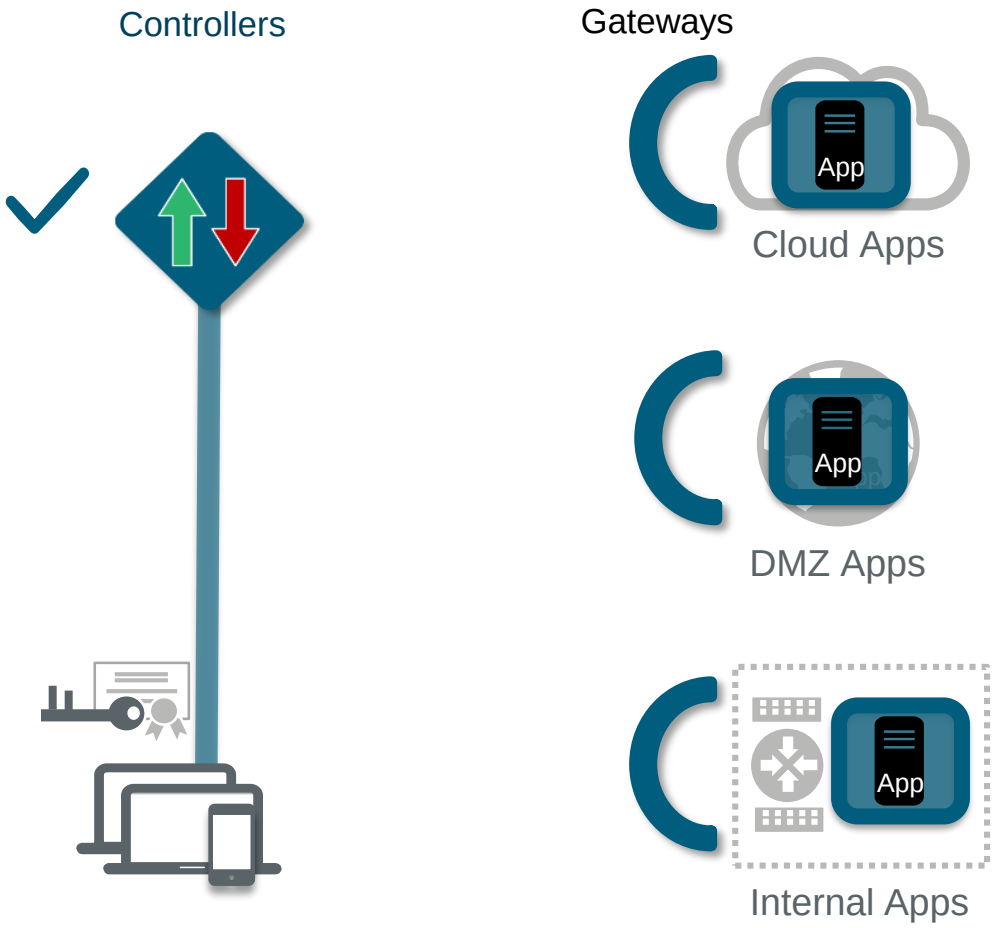
Defeats

1. Credential theft, transparently
2. Server exploitation
3. Denial of Service
4. Infrastructure compromise
5. Connection hijacking
6. Compromised clients

PrecisionAccess Features

Attack / Defense

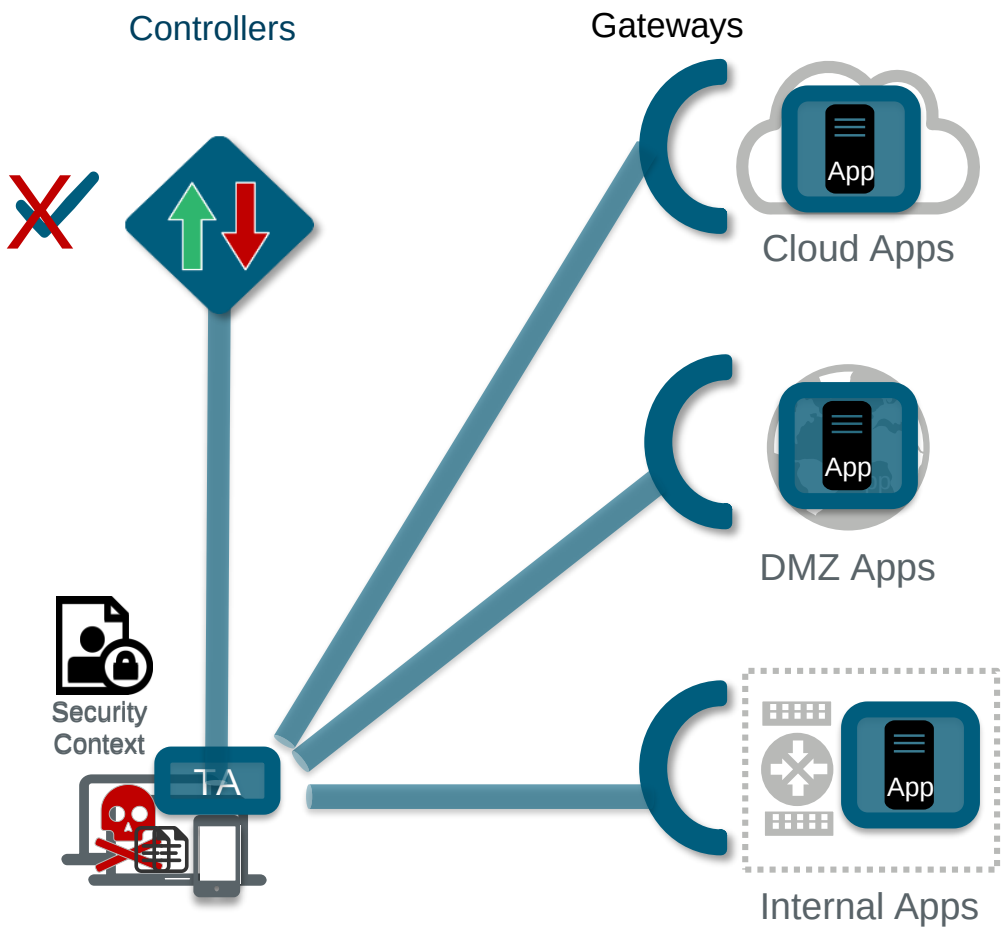
1. Credential Theft → Transparent MFA



PrecisionAccess Features

Attack / Defense

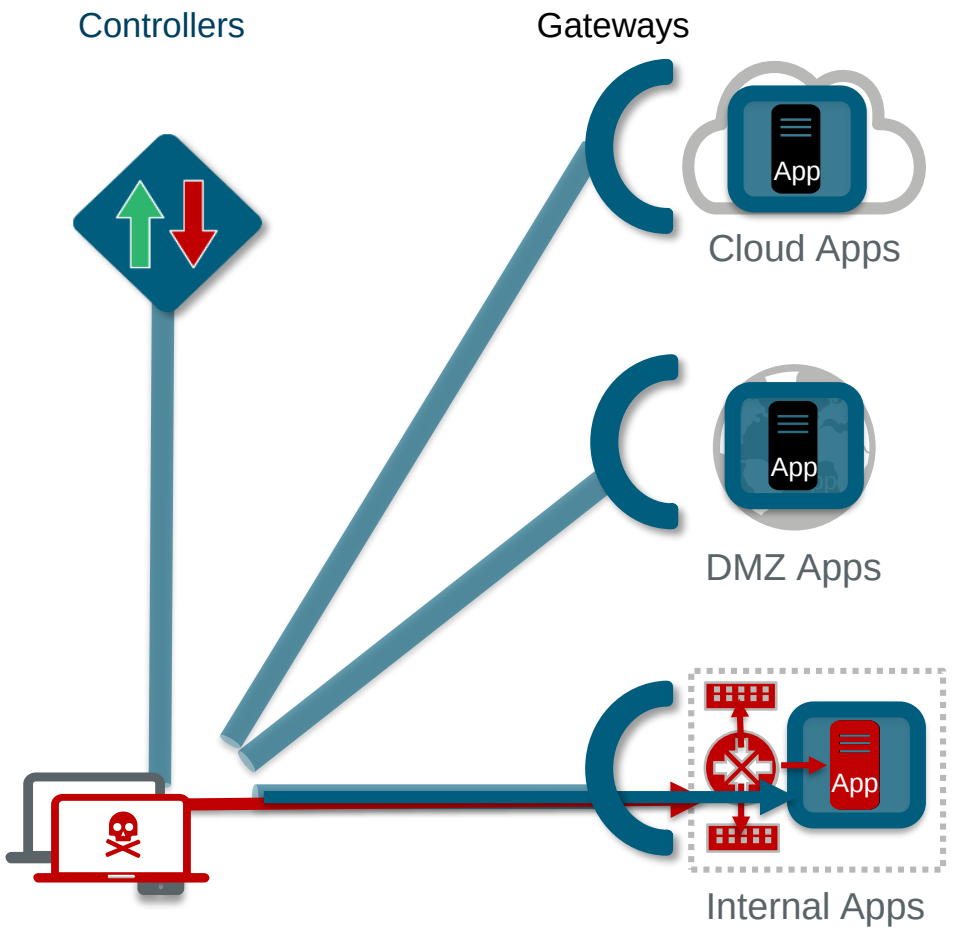
1. Credential Theft	Transparent MFA
2. Compromised Devices	Trust Assessor



PrecisionAccess Features

Attack / Defense

1. Credential Theft	Transparent MFA
2. Compromised Devices	Trust Assessor
3. Server Vulnerabilities	Server Isolation

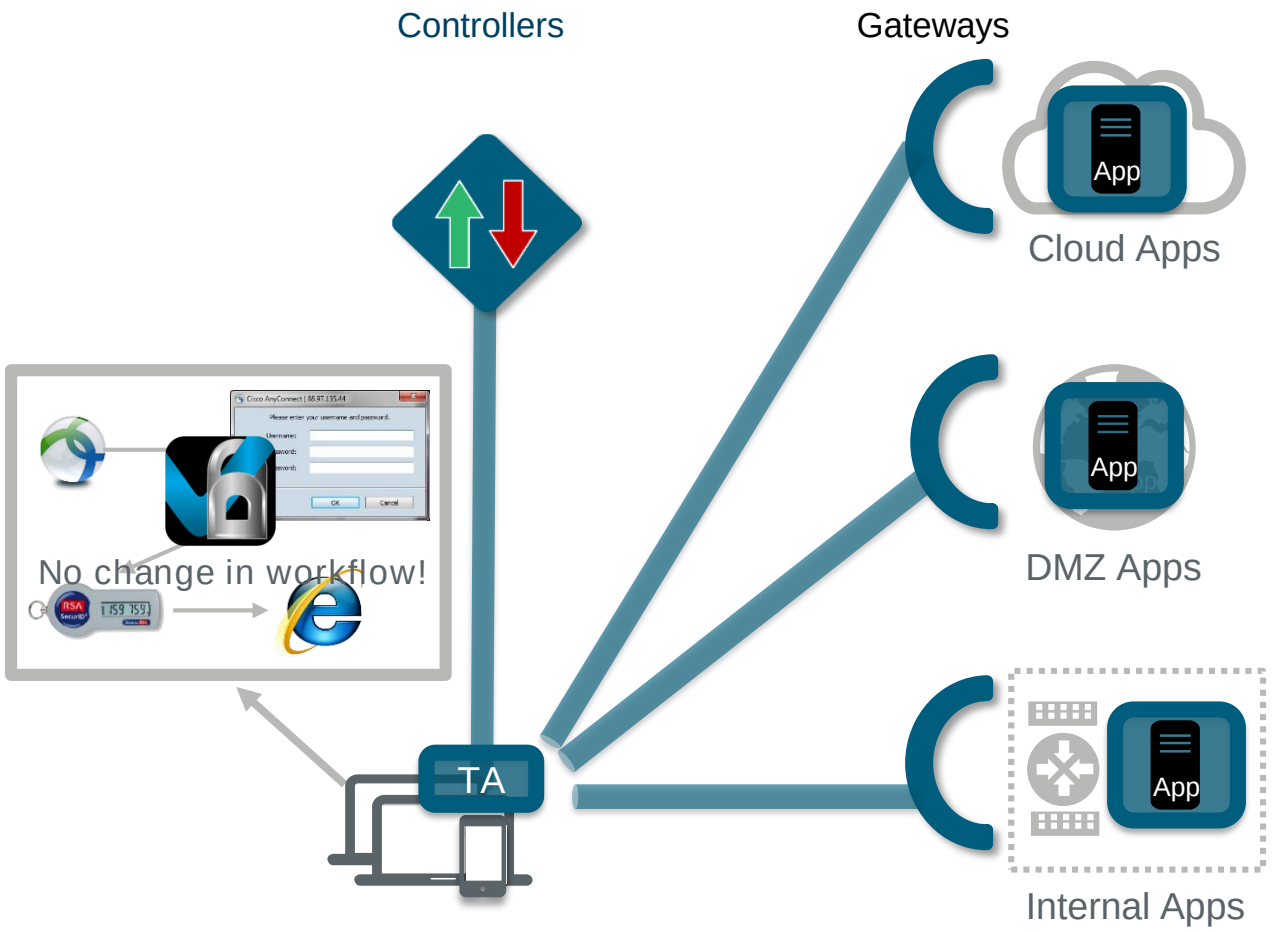


PrecisionAccess Features

VIDDER

Attack / Defense

1. Credential Theft	Transparent MFA
2. Compromised Devices	Trust Assessor
3. Server Vulnerabilities	Server Isolation
4. Interrupted Workflow	Transparent UX



PrecisionAccess Demo

VIDDER

One Tool for Access Control

VIDDER

Use Cases

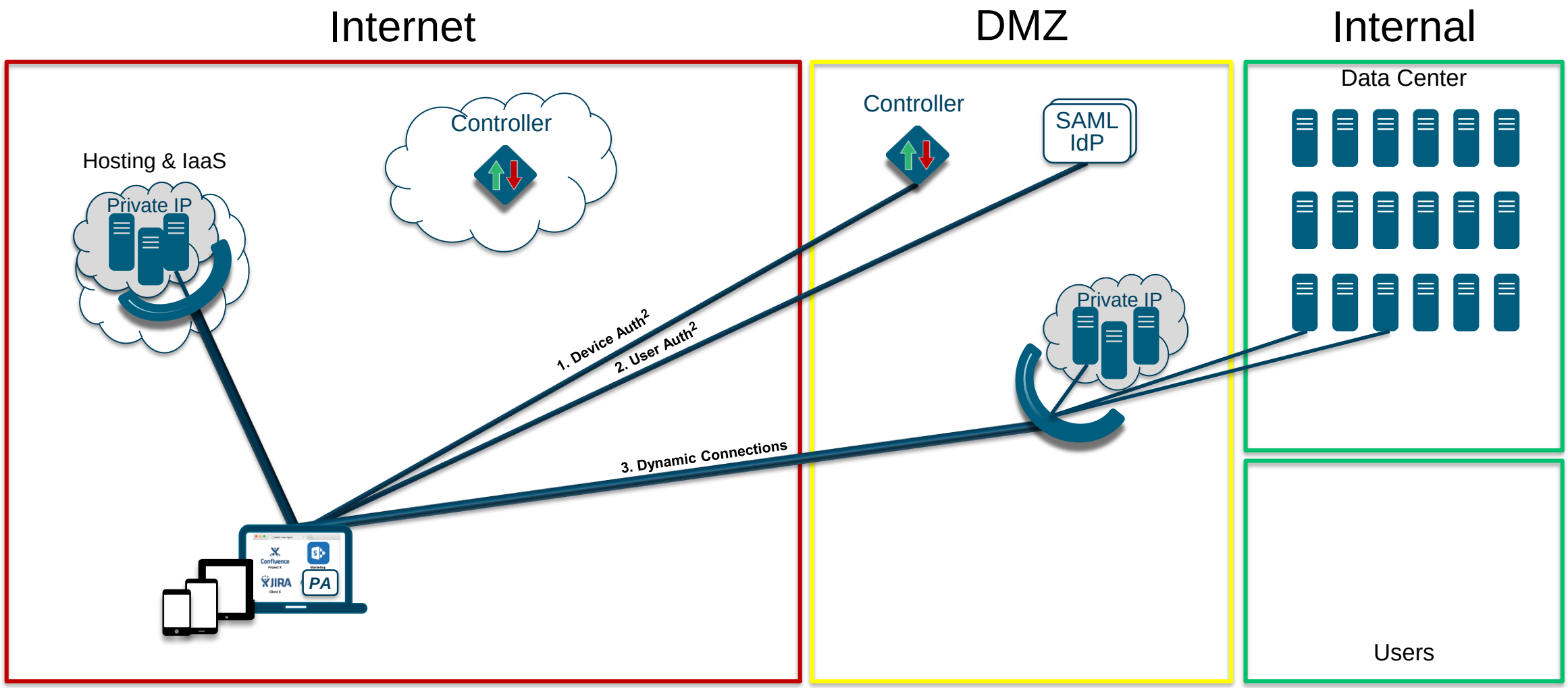
- Business-critical apps
  Secure intellectual property, PII, financial
- Data center isolation
  Secure the zero trust network
- Remote / 3rd party access, M&A
  App access, not network; transparent MFA
- Cloud migration
  Put the app on the Internet, then remove it
- Cloud Only Corp
  The vision of a simpler world

IT Projects

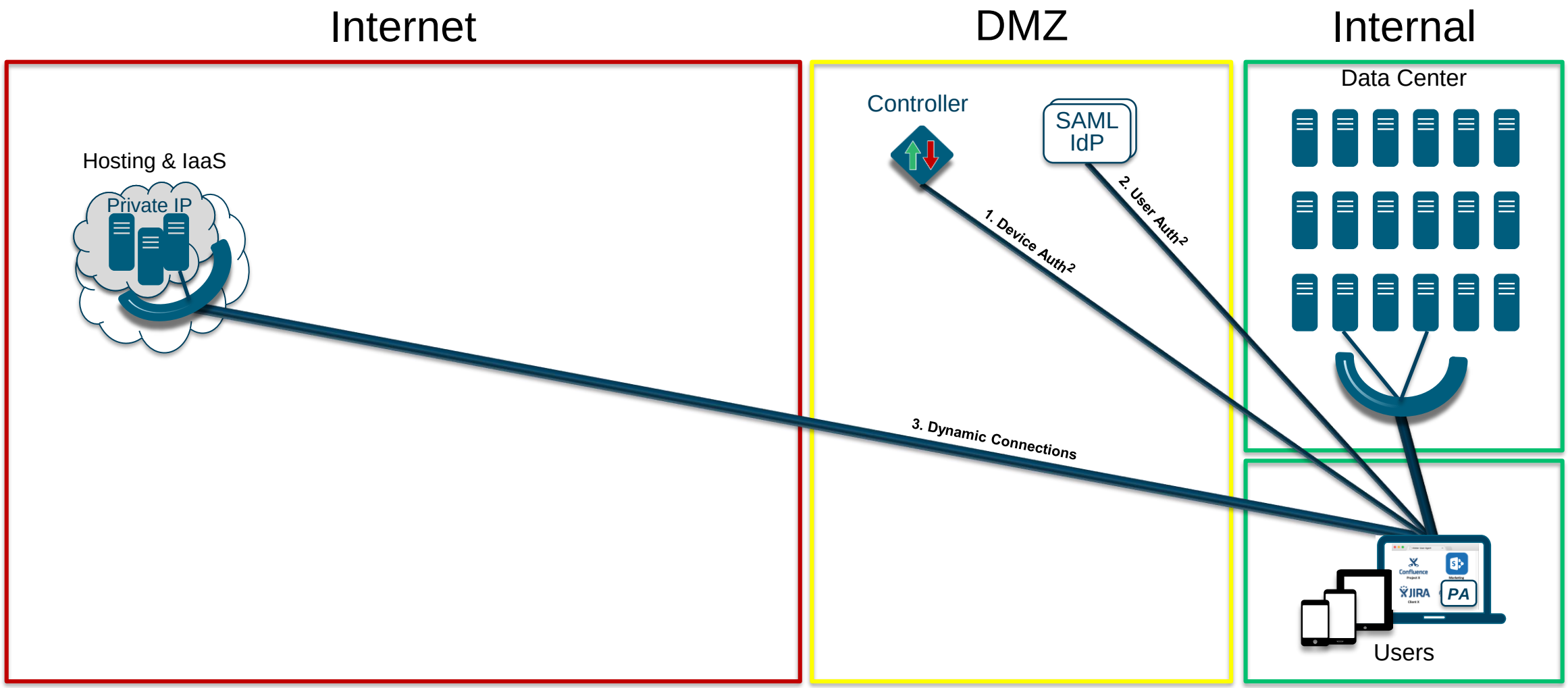
- Micro segmentation begins …
  … with user-to-server segmentation
- Fulfill the promise of NAC
  Fine-grained app access without VLANs
- Multi-Factor Authentication
  Easy to on-board, transparent to use
- Rationalize patch management
  Vulnerable servers isolated by default
- Zero trust network
  Interconnects trusted endpoints anywhere

PrecisionAccess Network Topologies

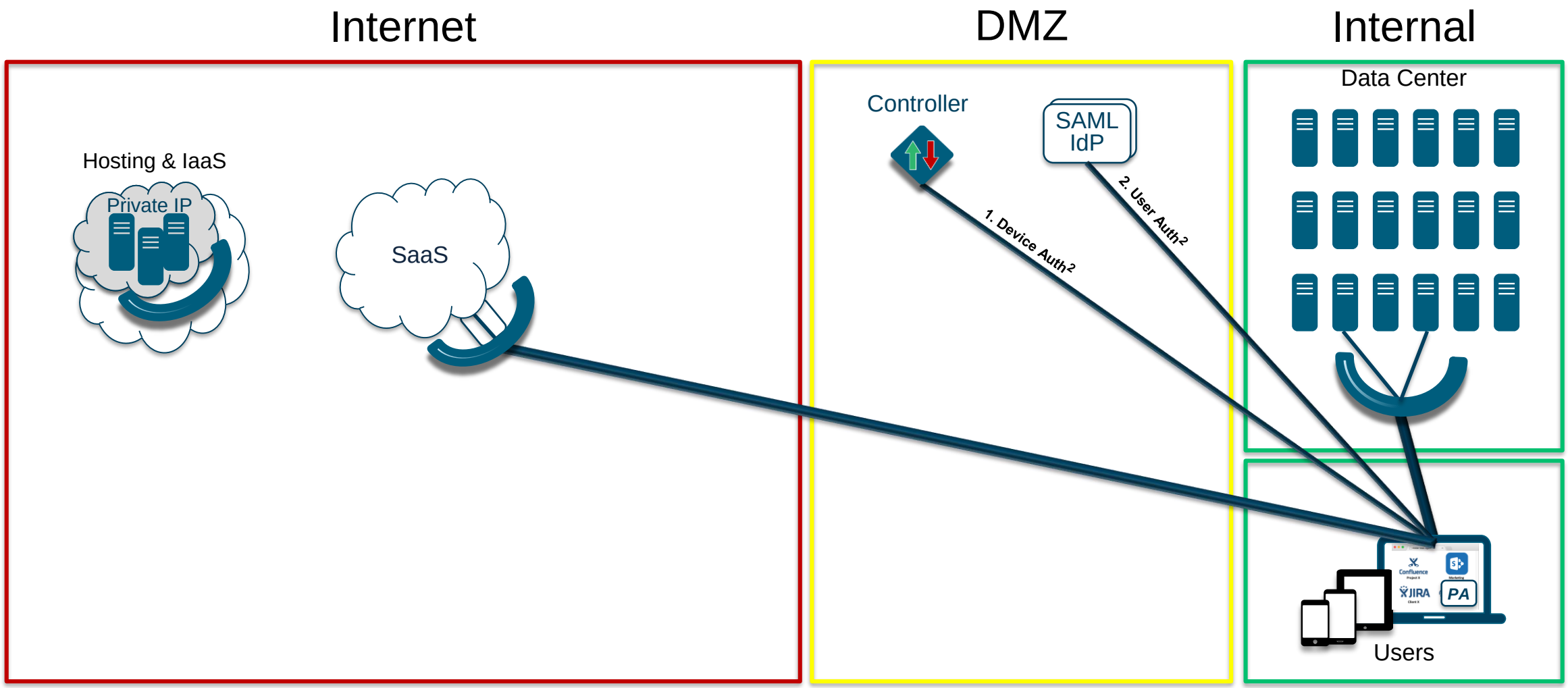
Integration with your Network



Integration with your Network



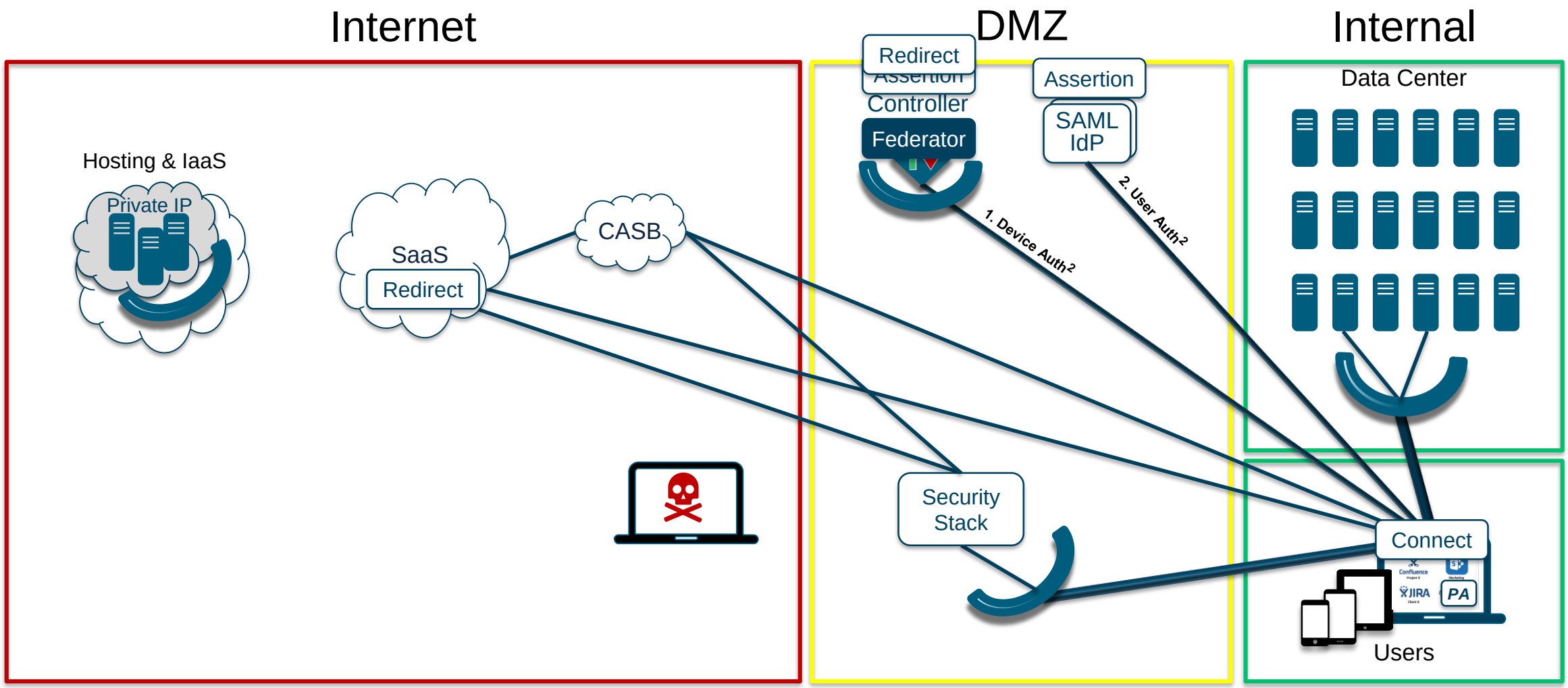
Adding SaaS to your Network



Defeat:

- Credential theft (transparently)
- Compromised device
- Man-in-the-Middle

Adding SaaS to your Network

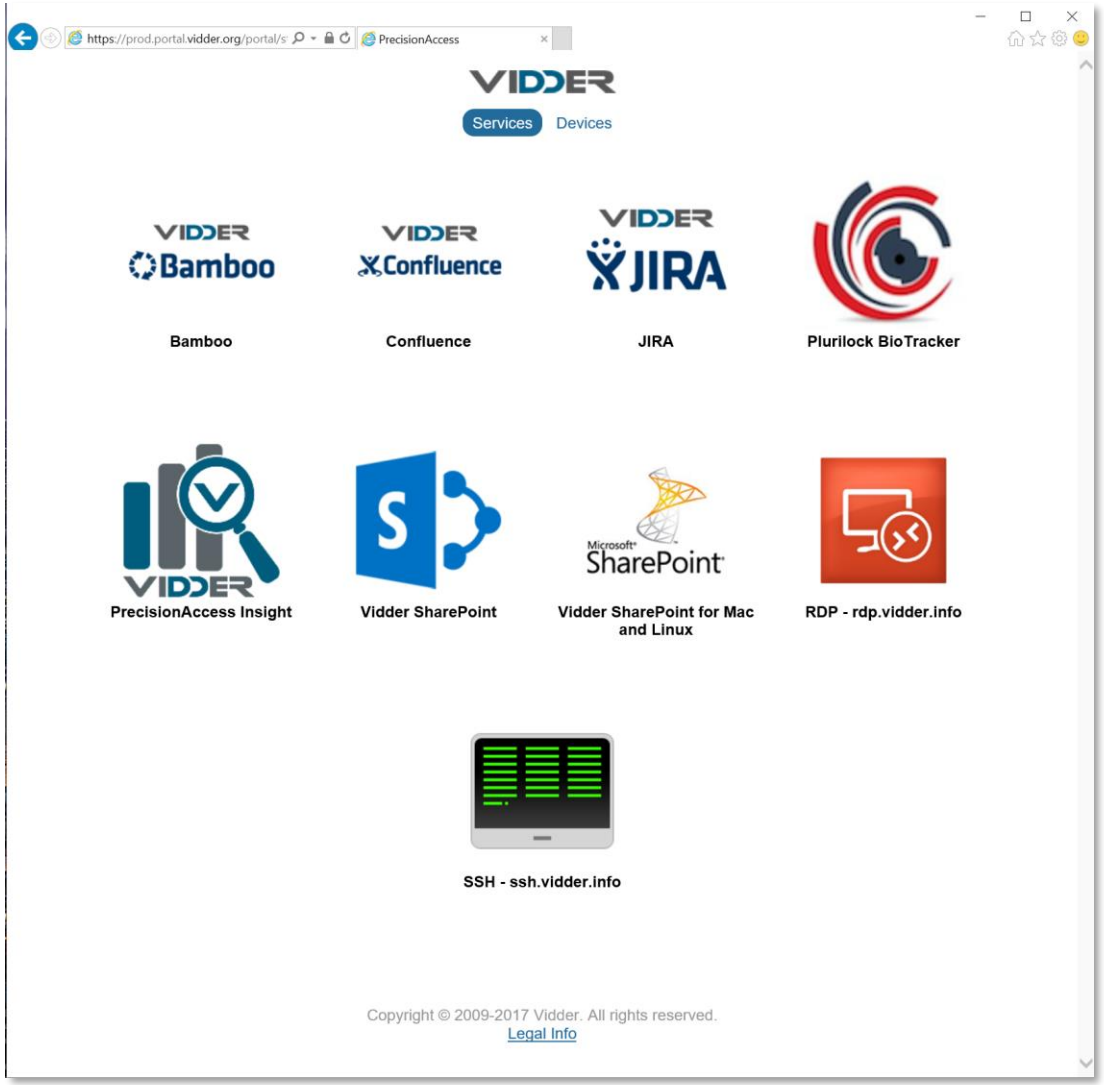


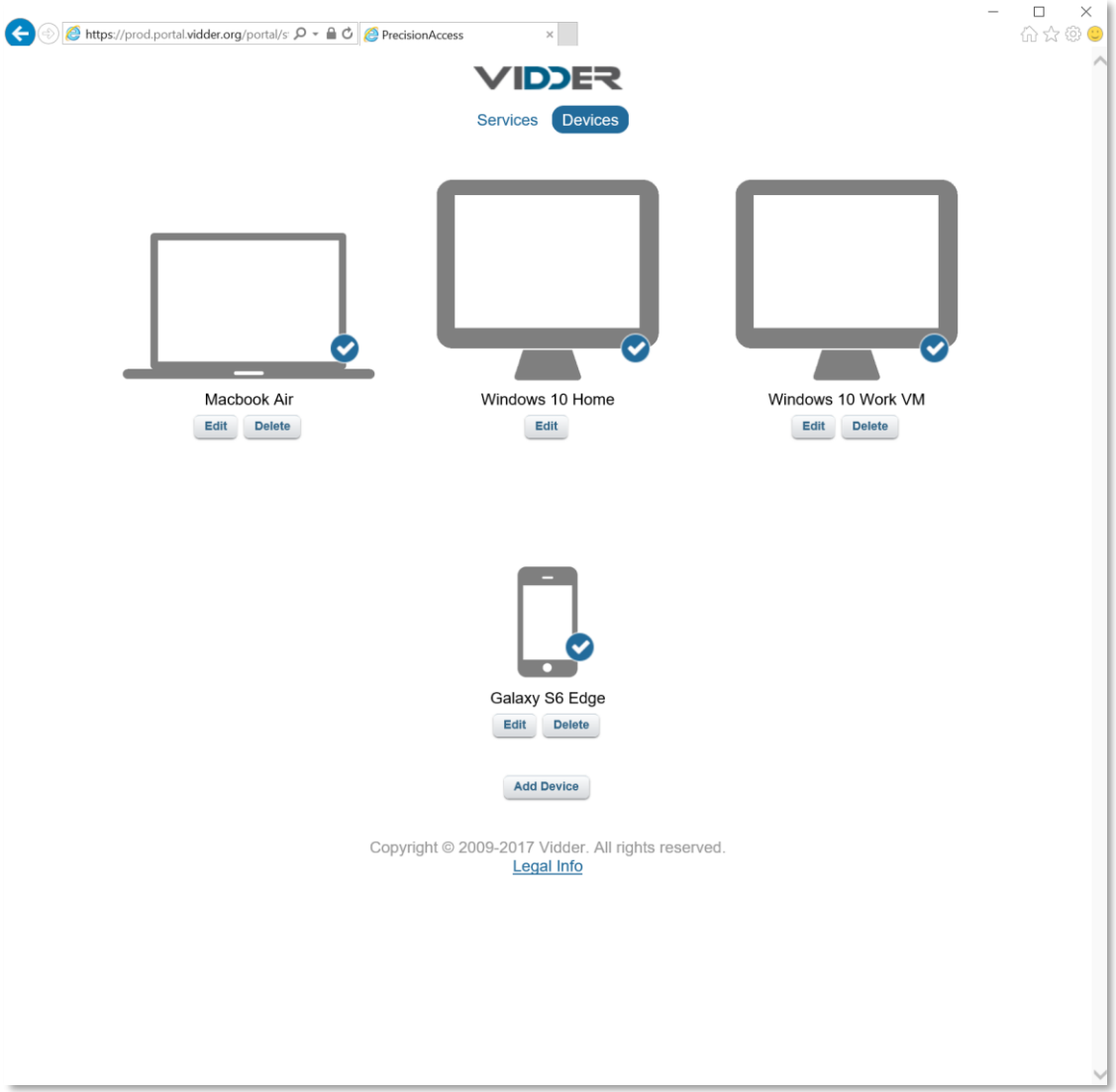
Defeat:

- Credential theft (transparently)
- Compromised device
- Man-in-the-Middle

PrecisionAccess - Screenshots

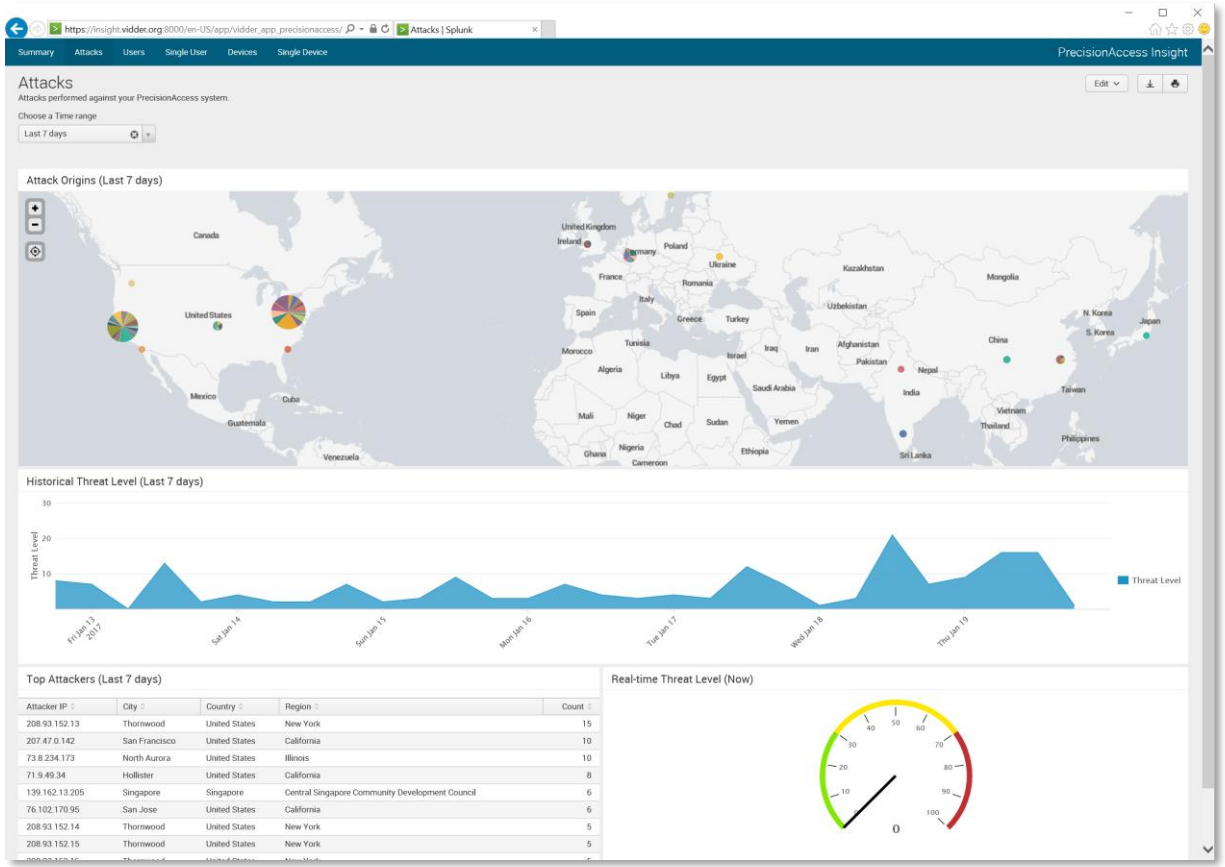
PrecisionAccess - Portal and Device





PA Insight


Summary
Attacks
Users
Single User
Devices
Single Device
PrecisionAccess Insight
Summary
A summary of key metrics on PrecisionAccess system.
Choose a Time range
Last 7 days
Attack Origins (Last 7 days)
Real-Time
0 Active Threats
Last 7 days
66 Attackers
Last 7 days
Attacks from 9 countries
All-Time
49 Onboarded Users
All-Time
116 Onboarded Devices


Summary
Attacks
Users
Single User
Devices
Single Device
PrecisionAccess Insight
Attacks
Attacks performed against your PrecisionAccess system.
Choose a Time range
Last 7 days
Attack Origins (Last 7 days)
Historical Threat Level (Last 7 days)
Threat Level
Top Attackers (Last 7 days)
Attacker IP
City
Country
Region
Count
Real-time Threat Level (Now)

PrecisionAccess - Roadmap

PrecisionAccess Roadmap 2017

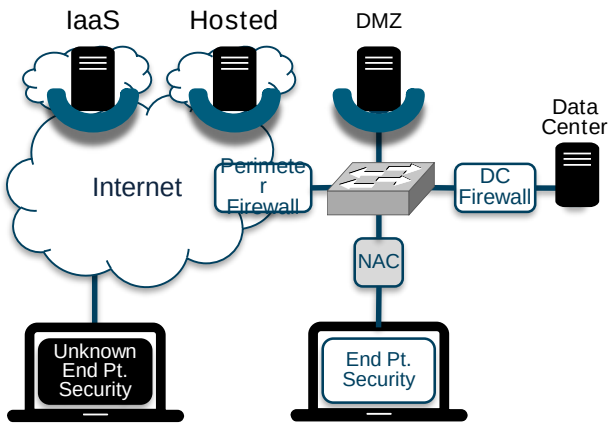
VIDDER

	Today	Q1 2017	Q2 2017	2H 2017
Client	Transparent MFA Transparent UX AD-Driven Auto Upgrade Automated Onboarding Windows, Mac, Linux, IOS	IOS Native App Support Android Browser	Android Native App Support	
Server	Dynamic Gateway Firewall Application-layer tunnel Context-aware Identity Integration via SAML / AD High Availability / DR Split Tunnel PKI Integration SIEM Integration	Wildcard DNS IP Ranges Port Ranges Number of Devices Policy Multiple Concurrent Devices	Increased Scale Geo-Clustering / Distribution SaaS Protection via SAML	
Insight	Users & Devices Attacks	Applications	Threat Detection Threat Hunting Enterprise-wide Searching Detailed Endpoint Visibility	Abnormal Behavior Detection
Trust Assessor	Managed vs Unmanaged Computer Domain User Groups		Alerting and Reporting Check for Processes, Network, User, Services, Registry, Patches Automated Endpoint Trust Assessment • Threat Intelligence Correlation • Indicators of Attack • Vulnerability Assessment • Malware Detection	Access Control Enforcement Revoke Access Per-App Risk-based Access Control ML/AI-Driven Detections 3rd Party Integrations

PrecisionAccess – Competition

NAC

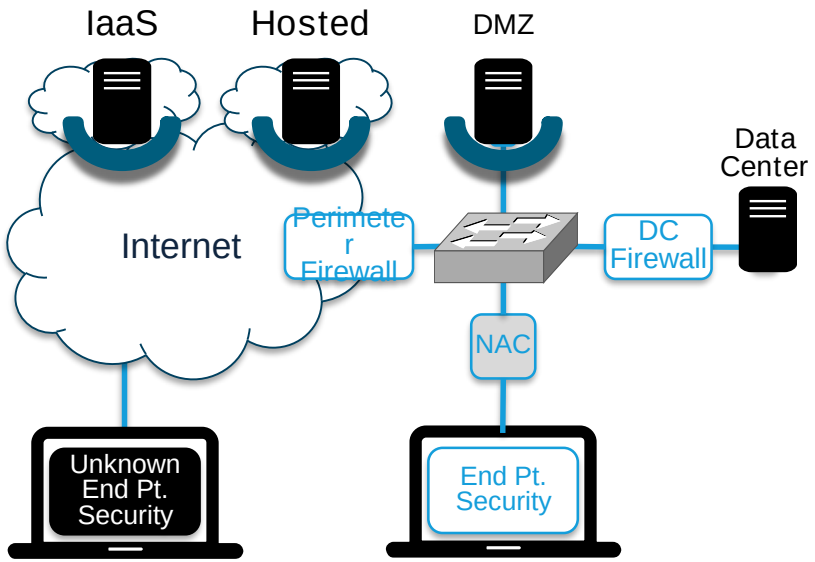
- Reduce / Complement
- Network Access Control (NAC):
  - Device pre-authentication for access to the LAN
  - In practice, non-granular assignment to 1 of 3 networks
    - Internal, untrusted (i.e., BYOD), guest
- PrecisionAccess:
  - Complements NAC
    - Extends it to cloud, non-employees
  - Reduces NAC
    - If eliminate full network access by remote offices
    - Huge cost reduction



Example vendors: HP(Aruba), Cisco, Forescout

Cisco ISE

- Reduce / Complement
- Cisco ISE:
  - Device pre-authentication for access to the LAN
  - In practice, non-granular assignment to 1 of 3 networks
    - Internal, untrusted (i.e., BYOD), guest
- PrecisionAccess:
  - Complements NAC
    - Extends it to cloud, non-employees
  - Reduces NAC
    - If eliminate full network access by remote offices
    - Huge cost reduction

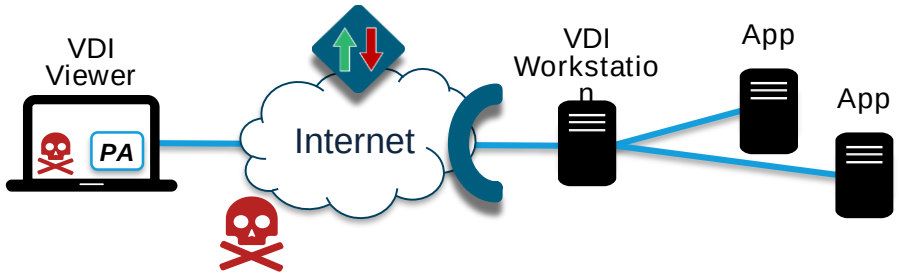


Example vendors: Cisco ISE

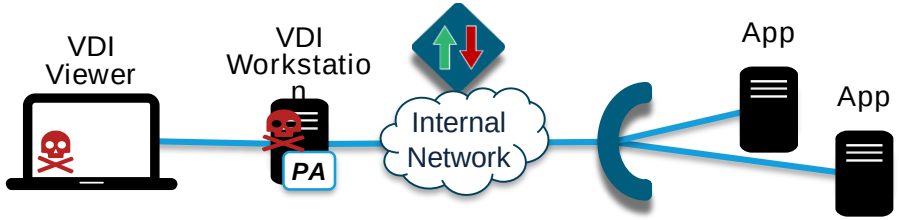
VDI

- Complement
- VDI:
  Mitigates attacks from ***compromised authorized*** users
- PrecisionAccess:
  Defeats access from ***all unauthorized*** users
- PrecisionAccess also:
  Defeats credential theft transparently
  Defeats server exploitation (e.g., 28 vulnerabilities in Citrix server)
  Is easy to install
  Is easy to use securely (tMFA vs. passwords or tokens)
  Works like users expect (without delay and jitter)
  Is virtual, elastic, and cloud friendly

Non-Persistent VDI & PrecisionAccess



Persistent VDI & PrecisionAccess



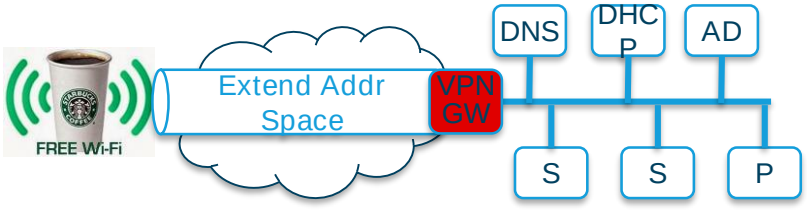
Example vendors: Citrix, VMware

Remote Access VPN

- Reduce
  - Eliminating non-employees, untrusted devices
- Remote Access VPN:
  - Useful to give broad access to remote employees
  - In practice, static configuration provides too much connectivity
- However, PrecisionAccess:
  - The solution for the enterprise ecosystem & untrusted devices
  - Fine grained access to authorized apps only (no DNS, DHCP, visibility, etc.)
  - Can be deployed anywhere (software vs. hardware, typically)
  - Is cloud friendly (virtual, elastic, no backhaul of traffic)
  - Is user friendly (transparent MFA vs. tokens)
  - Is client application specific (vs. all applications of client)
  - Scales immensely (separation of control plane vs. data plane)

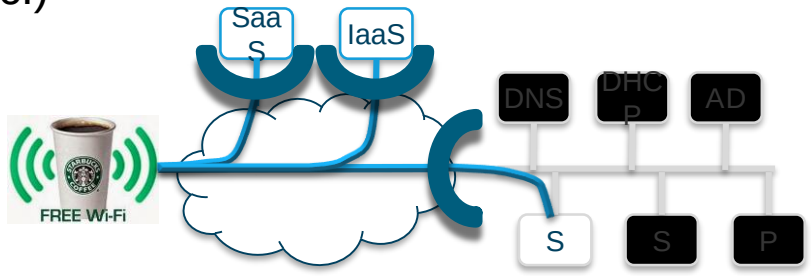
Example vendors: Cisco, Juniper, Checkpoint

Remote Access VPN



Common IP Addr Space

Software Defined Perimeter



Isolation of IP Addr

TCP TCP

Next Gen Firewalls

- Reduce complex firewall rules
- Both:
  - User and application aware
  - Visualize traffic by user and/or geographically
- PrecisionAccess:
  - Does not require 1,000's firewall rules (uses AD)
  - Defeats credential theft (transparent MFA)
  - Defeats connection hijacking (mutual TLS)
  - Can be deployed anywhere (dynamically configured)
  - Is cloud friendly (virtual, elastic, no backhaul of traffic)
  - Scales immensely (separation of control vs. data)
- Next gen firewalls:
  - Create the perimeter, add UTM functions
  - Data center east/west server separation
  - Example vendors: Palo Alto Networks, Cisco Sourcefire