



# A New Approach to Securing the Smart Grid with Identity Networking

John Hayes, Founder and CTO

# The Secure DGM LDRD Project at NREL

Distribution Grid Management, Laboratory Directed R&D

- The Secure DGM LDRD project testbed addressed the cybersecurity and resilience requirements of distribution grid management
- The function of the testbed is to emulate and demonstrate—as realistically as possible, real world environment
- Penetration testing performed by a 3<sup>rd</sup> party

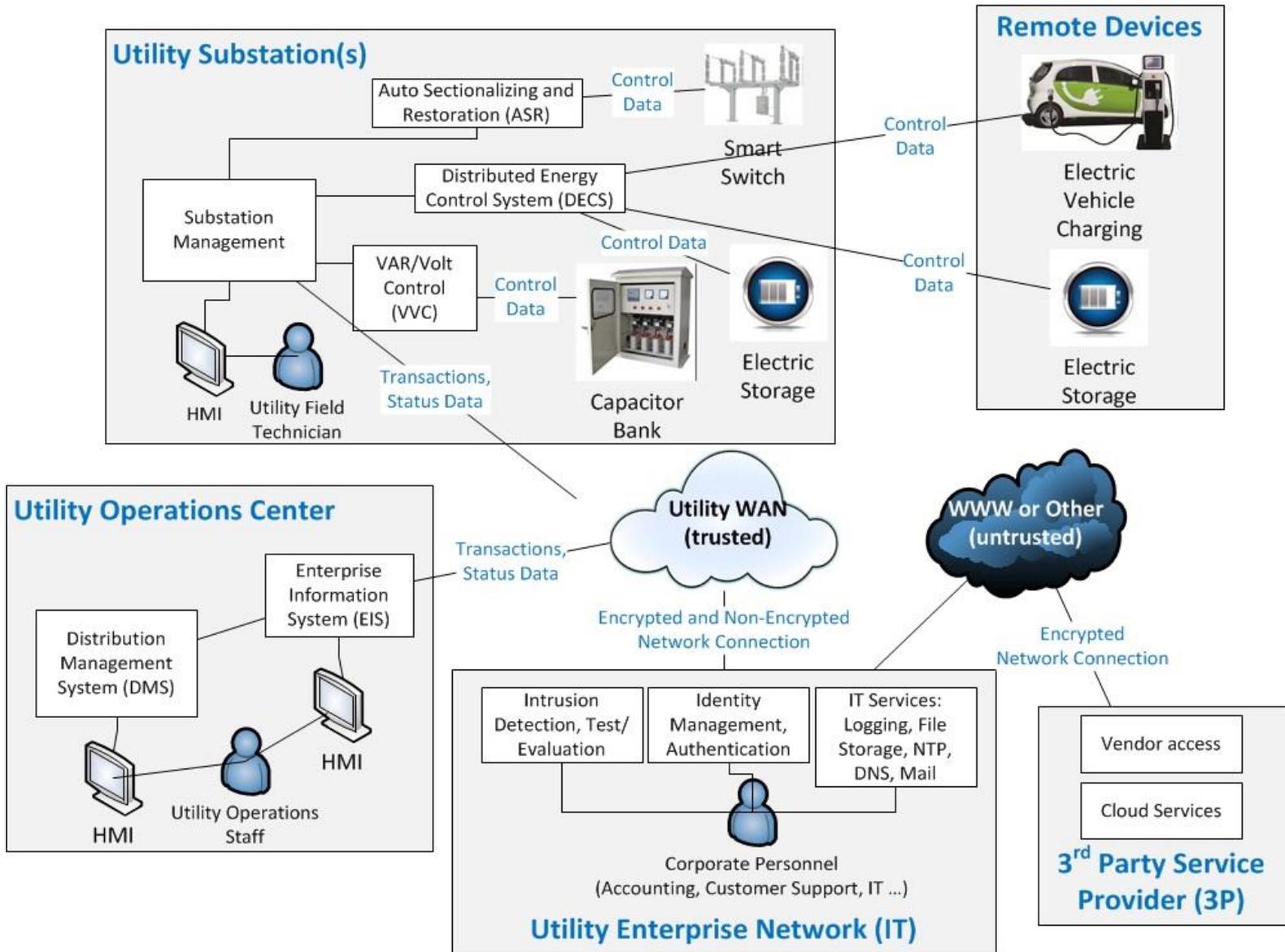
# BlackRidge Participation

- BlackRidge Transport Access Control (TAC) devices provide in-line blocking to protect the Enterprise Information System and the two Advanced Substation Platforms
- BlackRidge TAC inserts authenticated tokens into the first packet of a TCP session to ensure that only legitimate users access these nodes

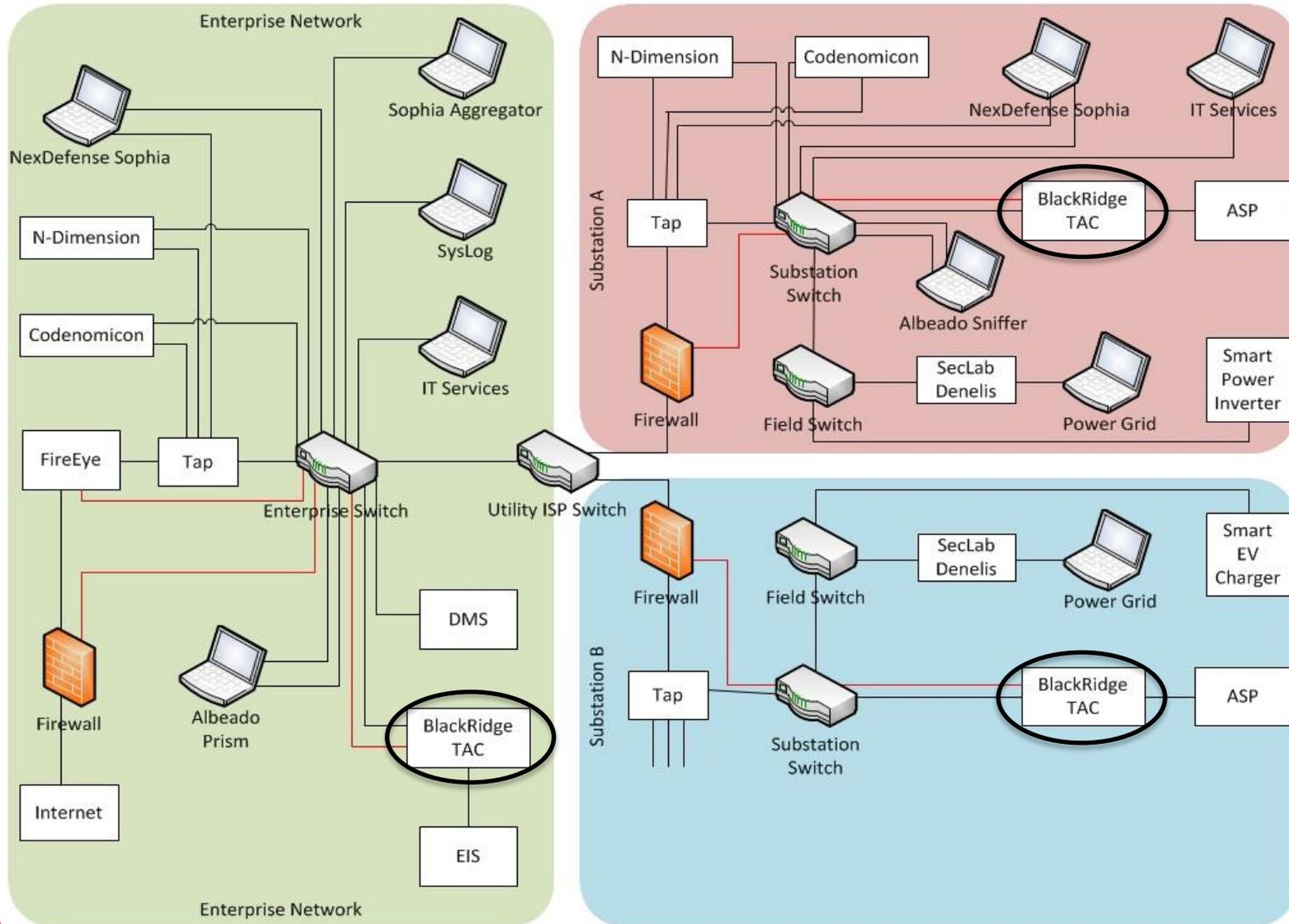
# Pen testers reported:

“all of the **external vulnerabilities identified** in the initial test were **completely mitigated**. The network hardening and installation of new hardware and software all contributed to an impenetrable outer layer of defense. The new architecture included an **industry-recognized layered defense** that would require multiple exploits to penetrate successive layers to reach the critical assets of the SCADA systems.”

# Logical Architecture of the Test Bed



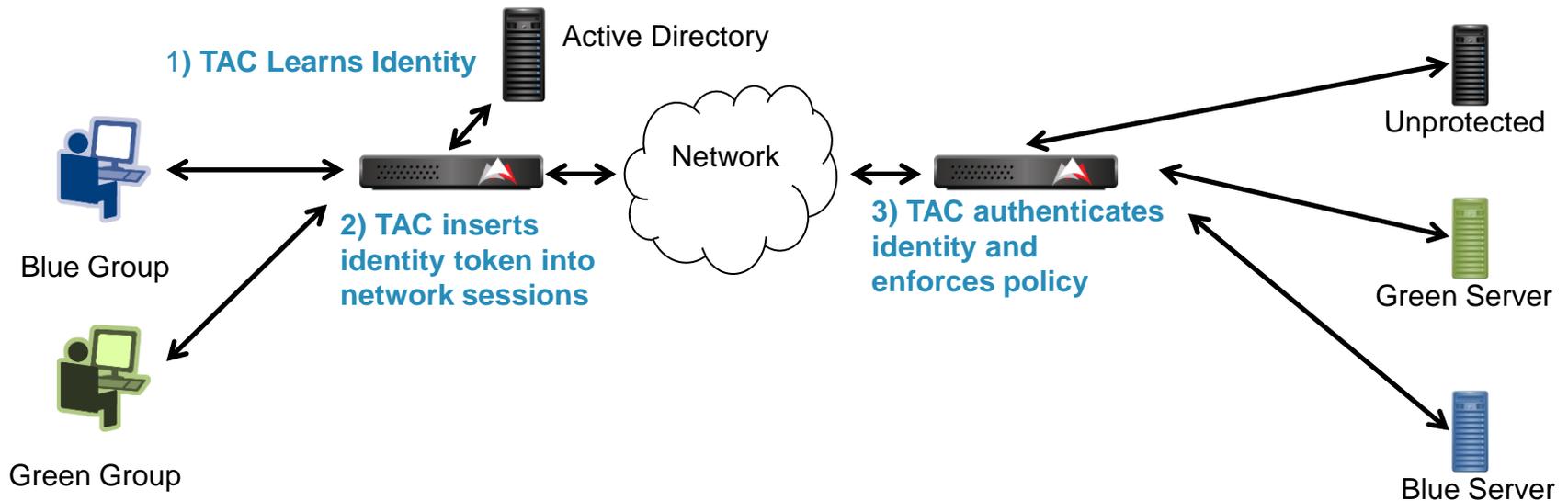
# Test Bed Configuration



# More BlackRidge Use Cases

# Securing Legacy Resources: No Application Changes

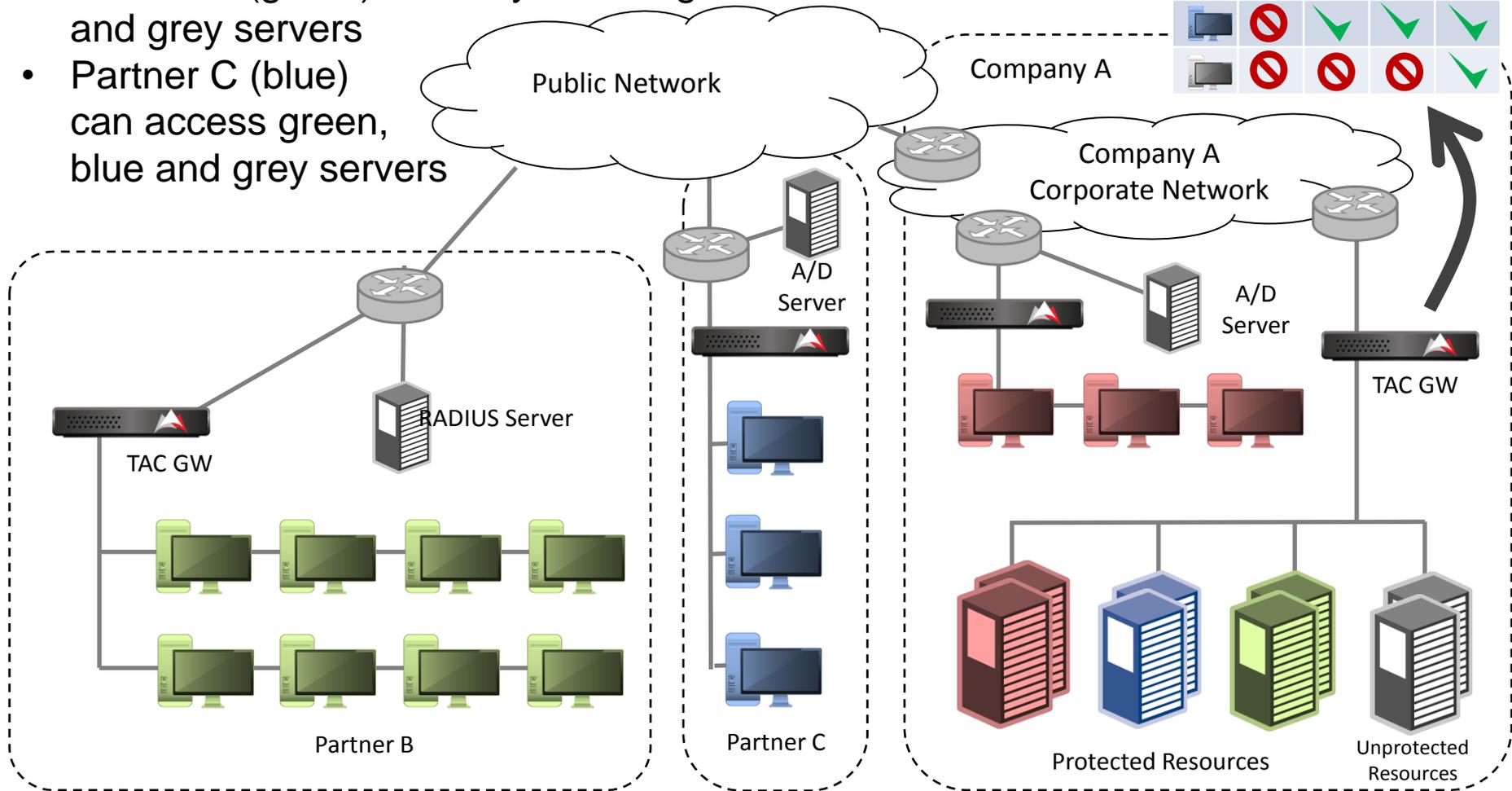
- Transport Access Control (TAC) uses existing identity infrastructure to protect network and key internal resources
- High throughput, low latency, turn-key physical or virtual operates transparently to networks and users
- Compatible with existing infrastructure, topology independent, and incrementally deployable



# Financial Deployment: Partner and 3<sup>rd</sup> Party Access

- Company A (red) can access all servers
- Partner B (green) can only access green and grey servers
- Partner C (blue) can access green, blue and grey servers

	Red Server	Blue Server	Green Server	Grey Server
Company A (Red)	✓	✓	✓	✓
Partner B (Green)	✗	✗	✓	✓
Partner C (Blue)	✗	✓	✓	✓
Company A (Grey)	✗	✗	✗	✓



# Live Test Results: Blocking 100% of Unauthorized Traffic

Firewall IPS Protection					Adding BlackRidge Protection				
Hosts protected by an Intrusion Protection System					Time Frame				
<u>erhp Educational Site, Protected By a Juniper SRX 3600</u>					Number of Days				
Time Frame	Number of Days	Total SSH attempts	Average Per Day	Std. Dev.	Total SSH attempts				
					Average Per Day				
					Std. Dev.				
All Hosts Combined									
erhp So Far Today	1	12	N/A	N/A	ALL Hosts So Far Today	1	68,246	N/A	N/A
erhp This Month	24	605	25.21	39.39	ALL Hosts This Month	24	2,593,017	108,042.38	27,977.56
erhp Last Month	31	13,828	446.06	1,289.94	ALL Hosts Last Month	31	3,233,934	104,320.45	36,333.54
erhp This Year	115	15,001	130.44	696.98	ALL Hosts This Year	115	10,404,482	90,473.76	37,445.92
erhp Since Logging Started	437	46,278	105.90	514.36	ALL Hosts Since Logging Started	480	62,837,633	130,903.40	78,322.18
erhp Normalized Since Logging Started			0.00	0.00	ALL Hosts Normalized Since Logging Started	1,784	30,777,390	17,027.68	25,442.11
<u>erhp2 Educational Site, Protected By a Juniper SRX 3600</u>					Hosts protected by BlackRidge Technologies				
Time Frame	Number of Days	Total SSH attempts	Average Per Day	Std. Dev.	<u>blackridge Educational Site, Protected By a BlackRidge Technology Eclipse</u>				
					Time Frame				
					Number of Days				
					Total SSH attempts				
					Average Per Day				
					Std. Dev.				
erhp2 So Far Today	1	2	N/A	N/A	blackridge So Far Today	1	0	N/A	N/A
erhp2 This Month	24	241	10.04	18.25	blackridge This Month	24	0	0.00	0.00
erhp2 Last Month	31	10,166	327.94	997.09	blackridge Last Month	31	0	0.00	0.00
erhp2 This Year	115	10,744	93.43	537.05	blackridge This Year	115	0	0.00	0.00
erhp2 Since Logging Started	405	21,047	51.96	302.17	blackridge Since Logging Started	350	0	0.00	0.00
					blackridge Normalized Since Logging Started				
					0.00				
					0.00				

Firewall with IPS allows large number of TCP connection attempts through and information to leak to scans.

BlackRidge does not allow any unauthorized connection attempts or scans (information leakage) to occur.

# BlackRidge Provides A New Network Security Element:

## Identity

# Identity

Who or What is responsible for an action or event

Provides Trust and Accountability

Identity is widely used by applications today...

... but not by the network

# Identity Networking Benefits

Session authentication before allowing access and response

- Policy based on requestor's Identity, requested resource
- Separates Identified and Authenticated traffic from unidentified traffic

Blocks Network Scanning and Reconnaissance

- Protected services are cloaked from unauthorized access
- No response to unidentified or unauthenticated traffic

Separates Security Policy from Network Design

- Supports dynamic addresses and NAT
- Network can change without requiring changes in security policy

# What is Transport Access Control?

Transport Access Control (TAC) inserts and authenticates Identity on each and every TCP/IP session

Every TCP session is individually authenticated using First Packet Authentication

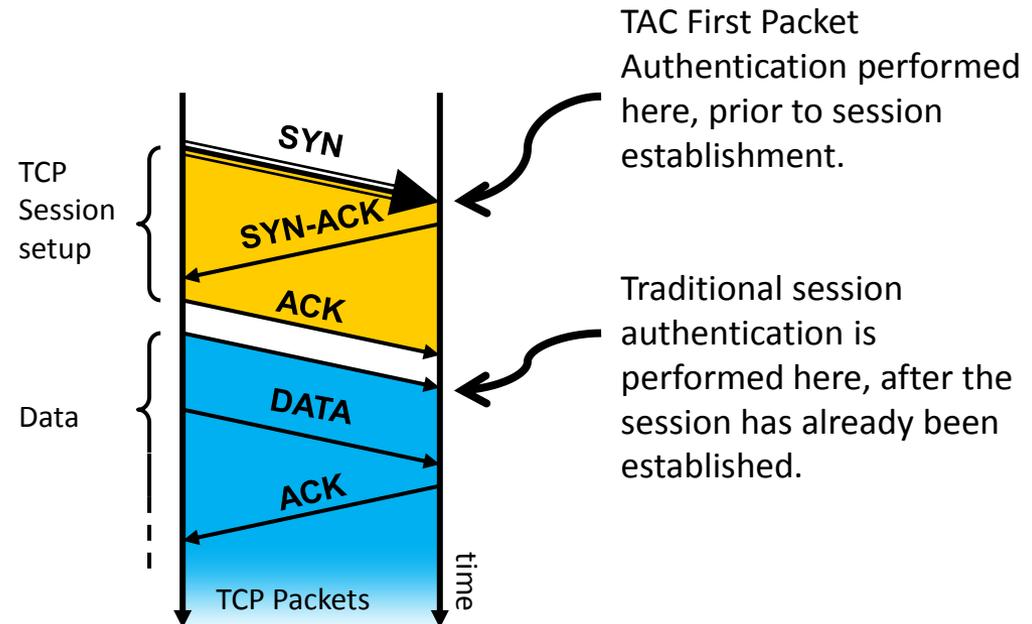
Works with legacy network, security, identity and application infrastructure



# Transport Access Control

Transport Access Control (TAC) Authenticates every TCP session request before responding and establishing the session

TAC is **Simple**,  
Efficient, End-to-End,  
NAT tolerant, Highly  
Scalable & Topology  
Independent



# Analytics and Feedback

- Provides session attribution information to analytics systems at earliest possible time
  - Enables better, more efficient analytics
- Analytics detect behavioral changes undetectable by Identity based systems
- Analytics provide feedback to Network Identity based security systems
  - Policy feedback via Trust level – efficient, deterministic
  - Independent of network topology

# Identity Networking - Summary

- Identity – A new network security element
- Blocks scanning, reconnaissance, DDoS and unauthorized access with non-interactive authentication protocol
- Horizontal applicability- protects SCADA, Enterprise and Cloud Resources
- Works with legacy network, security, identity and application infrastructure
- Network topology and address independent – Supports dynamic addresses and NAT
- Provides attribution information to analytics systems at earliest possible time



# Overview Presentation

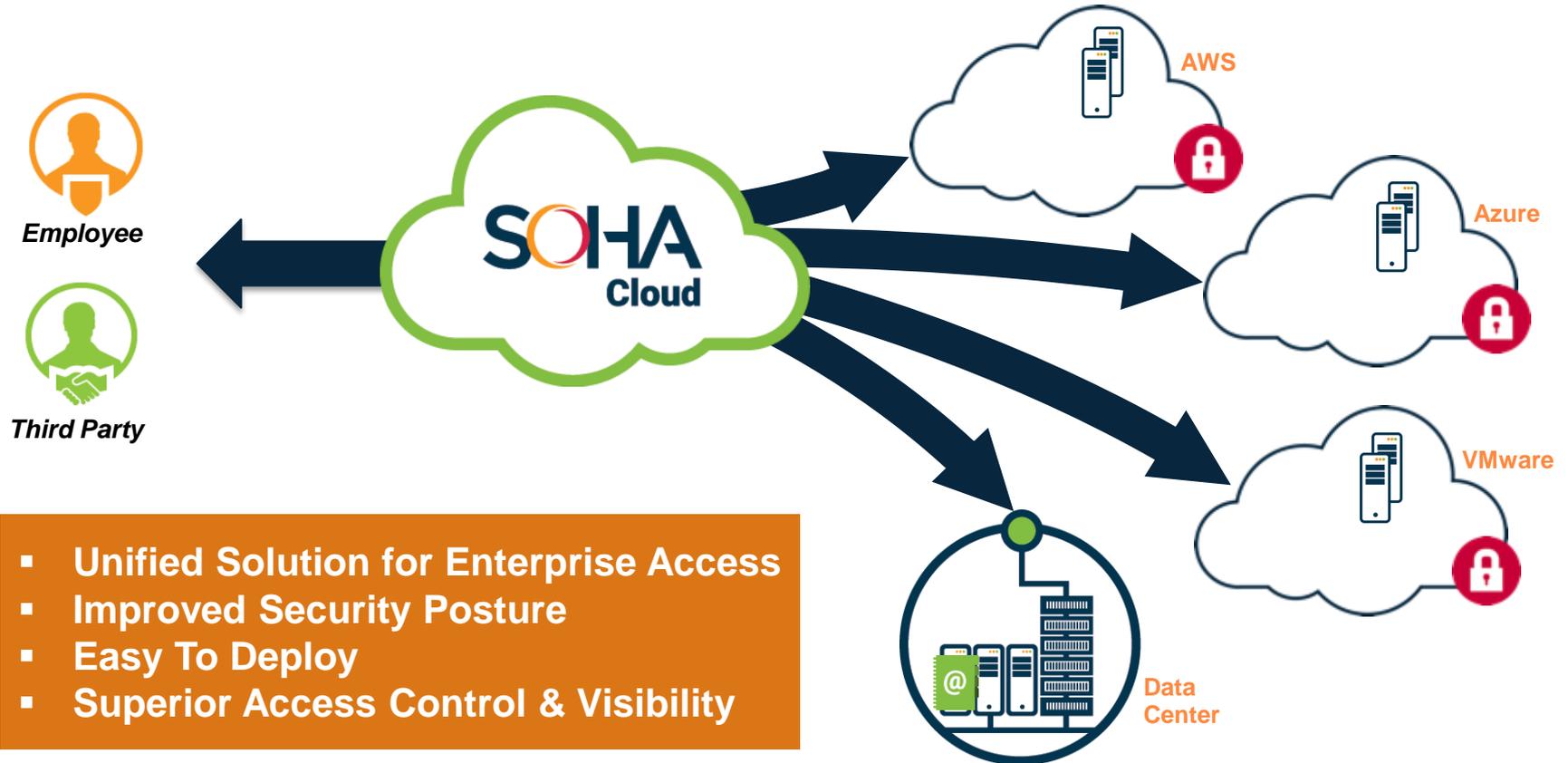
Haseeb Budhani | Haseeb@Soha.IO

June 2016

# Company Facts

- Founded in Q3 2013
- ~\$14 million in total funding
- Team strength: 38
- DNA:      
- Company launch: H2-2015
- Patents: 7 Filed

# Soha: Enterprise Secure Access; Delivered As A Service



# Companies Say Building A Secure Access Stack Is Hard!

## Lots of Moving Parts



agree they have to touch **5 to 14 network and application components** when adding new external user groups

## Expect More Breaches



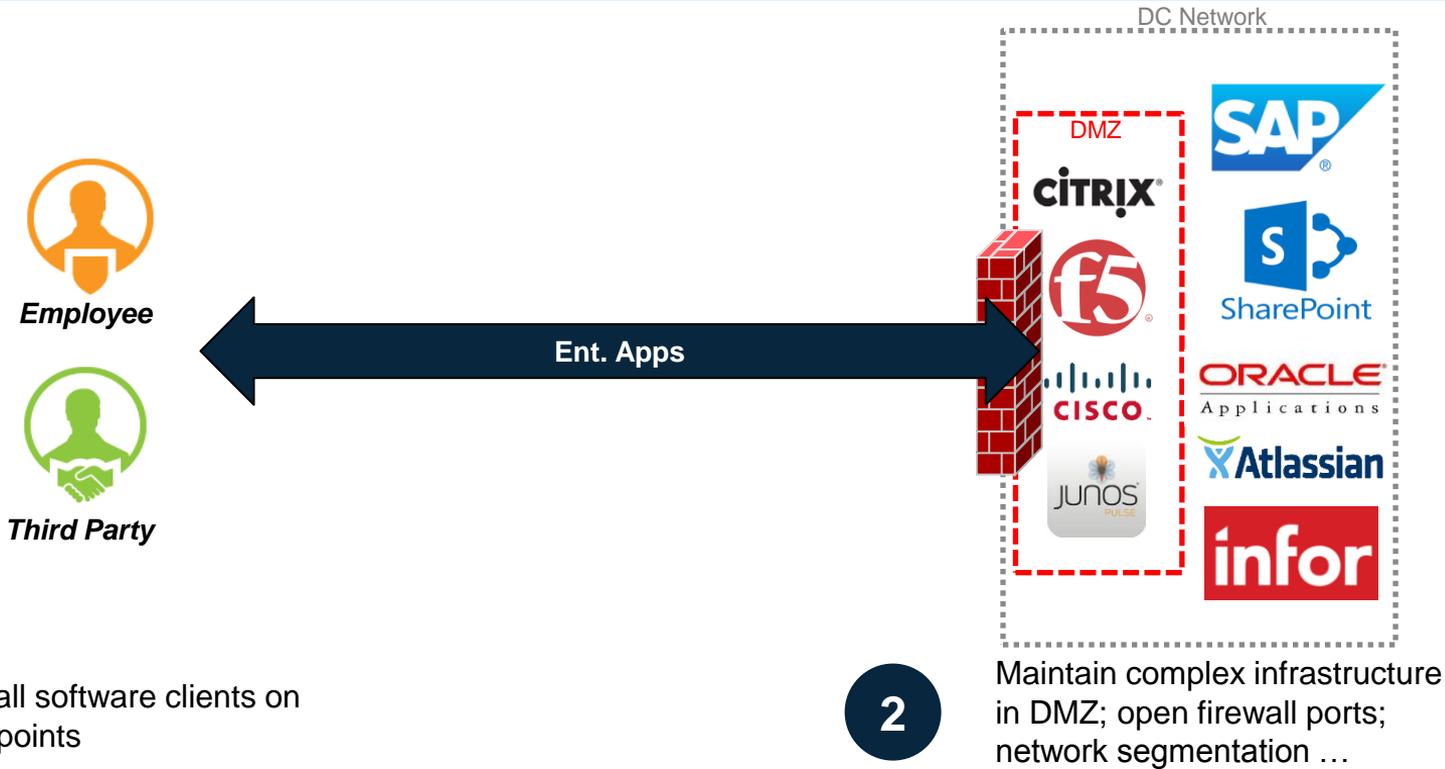
while 62% of respondents didn't believe their organization was vulnerable to an attack from their parties, **79% expect their competitors have or will suffer a serious data breach in the future**

## Third Parties are Prime Suspects

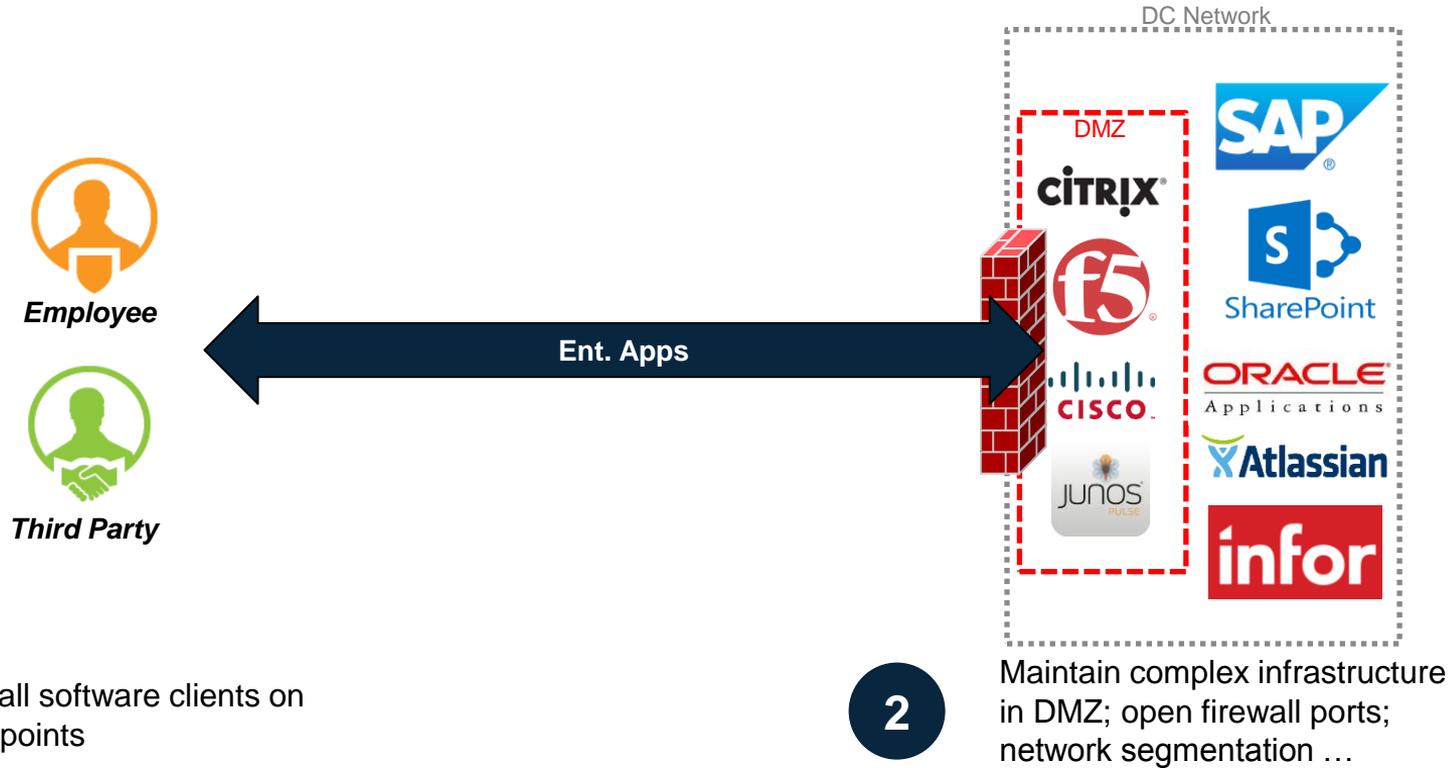


**of all data breaches are linked to third parties, and will likely get worse as enterprises grow their use of outside resources**

# Traditional Secure Access Stack



# Traditional Secure Access Stack



*... But Enterprises Networks Continue To Get Breached ...*

# Building Out App Security Infrastructure Is Complex

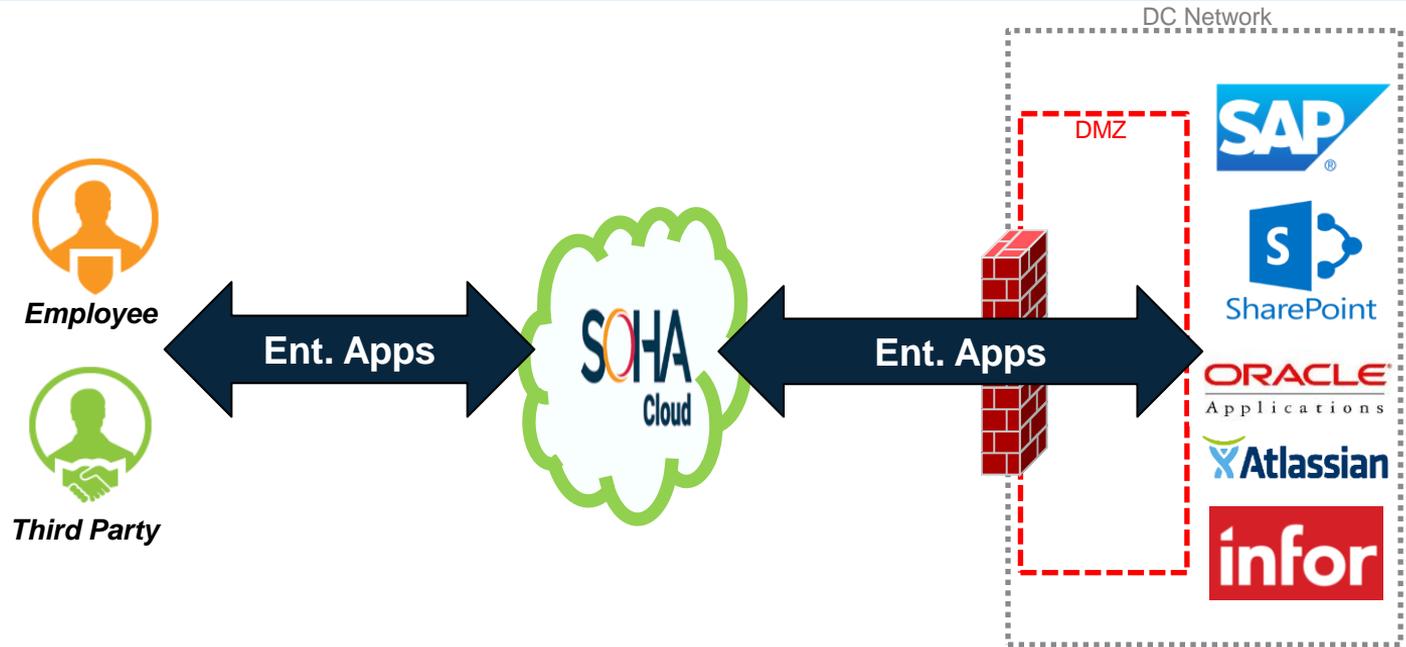
## Operational Challenges

- Deploy/manage complex appliances (physical or virtual) in DMZ
  - High (CapEx + OpEx) undertaking
- Manage network segments spanning DMZ, internal network, etc.
  - Time to deploy new app measured in weeks, not hours/minutes

## Security Challenges

- Inbound firewall ports opened up per app
  - Attack surface grows with each new app deployed in network
- Users granted access to the network, not just to needed apps
  - Network access is an easy path for malware proliferation
  - Risk even greater with 3<sup>rd</sup> parties

# Soha Cloud: Enterprise Secure Access As A Service



# Soha Cloud Is Different

- Inline solution that enterprises consume as a service
- Radically new security approach: Shut down inbound firewall ports
- Works in any (private or cloud) network env
- No software on endpoints



# Soha Cloud vs. Traditional L4-7 Solutions

---

## Faster Deployment

Delivered as a service - no more appliances to deploy in the DMZ

No need for network segmentation in the data center

Up and running with strong app security in <30mins

## Lower OpEx

Enable secure access in minutes and save 100s of man hours per app

One-time deployment works for any number of apps - eliminate projects for additional apps

Do all this at a fraction of the cost of competitive, appliance-based solutions

## Better Security

Zero open ports on your edge firewall

Attack surface moved to Soha Cloud

Application infrastructure "hidden" from bad guys

# Soha Cloud Is Most Suitable For ...

---

- ✓ Companies providing 3<sup>rd</sup> parties with enterprise application access
- ✓ Companies deploying apps in new environments, e.g. AWS or Azure
- ✓ Companies suffering from IT slowdowns due to access related complexity

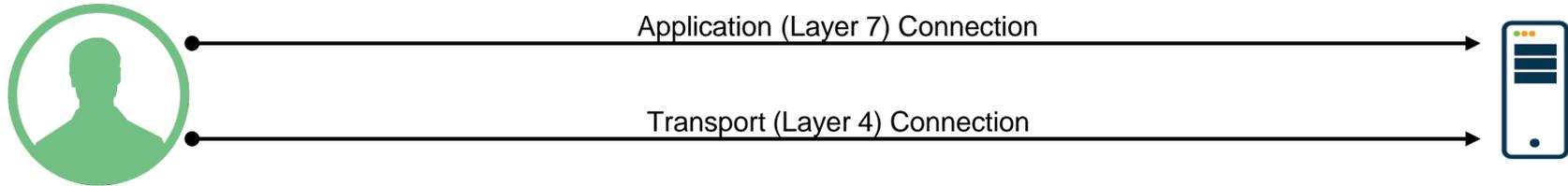
Learn more at <http://soha.io>

Thank you

# Backup

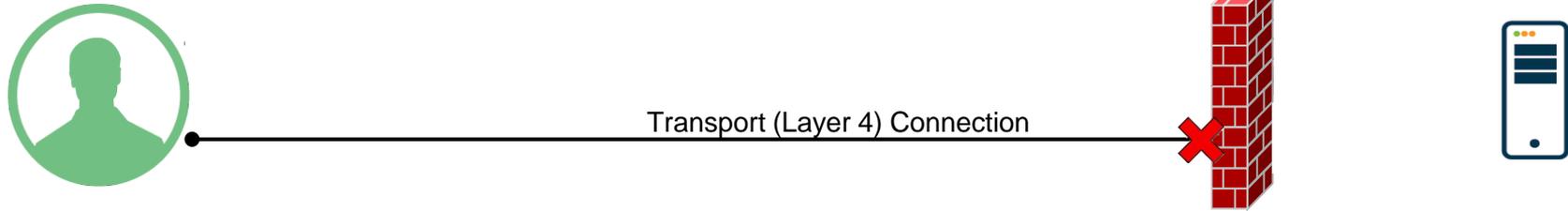
# Connectivity 101

## The Traditional Way



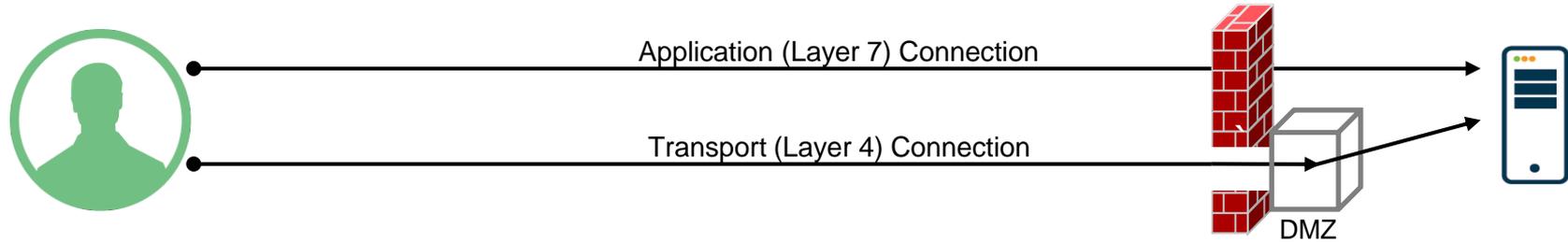
# Connectivity 101

## The Traditional Way



# Connectivity 101

## The Traditional Way



# A Whole New Way Of Thinking About Connectivity

## A New Way

