Can You Trust Your Eyes?
Using a Software-Defined Perimeter to Achieve Zero Trust

Jason Garbis

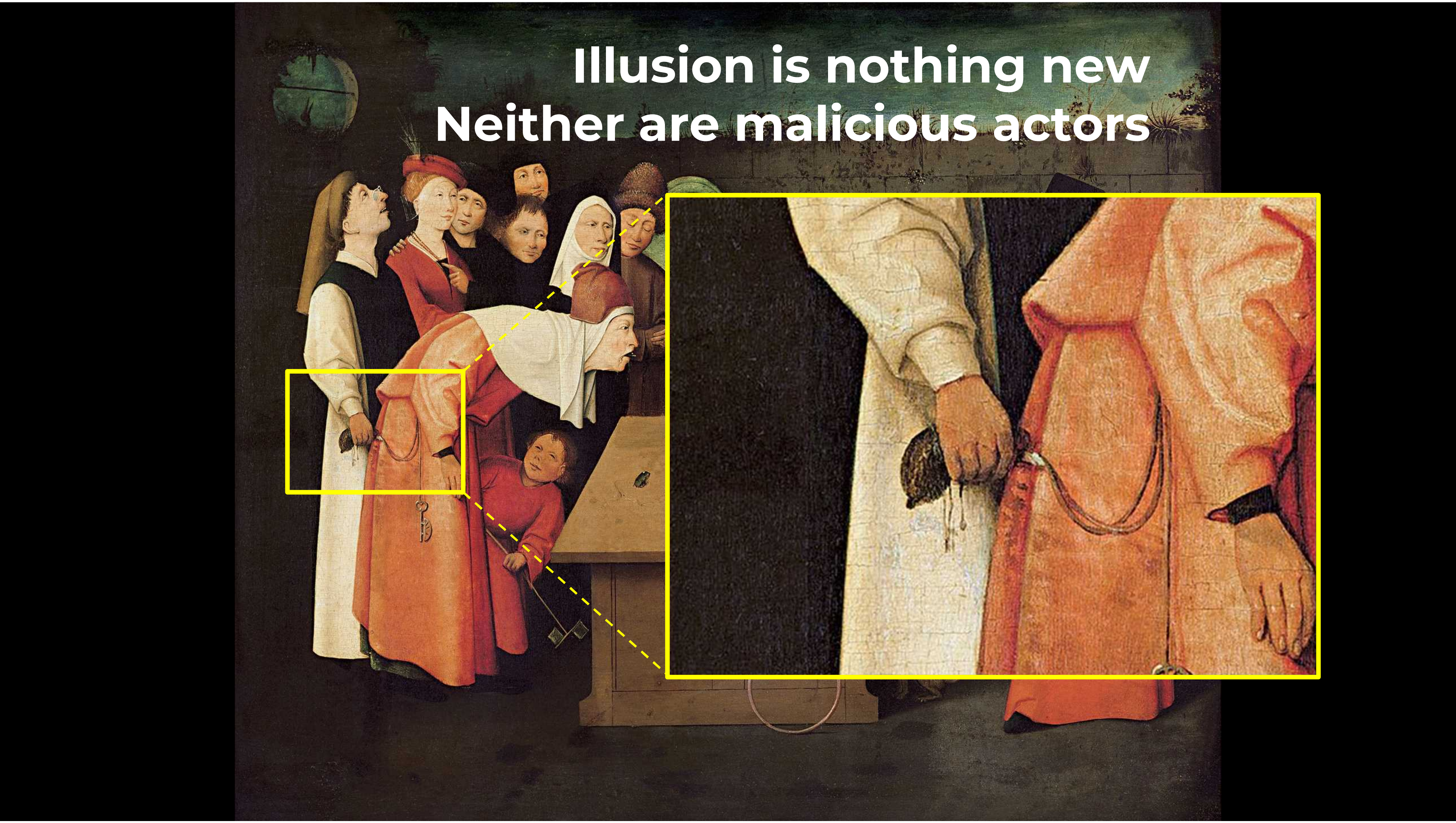
Vice President, Products – Cyxtera

Co-Chair, Software-Defined Perimeter Working Group, Cloud Security Alliance

Cyxtera™

Can we trust digital data?


Illusion is nothing new


Illusion is nothing new
Neither are malicious actors

No

Earning Trust

Passwords **Biometrics** **Tokens**

Authentication alone is insufficient

CVSS 10:
Critical

Remote Code Execution and Denial of Service Vulnerability

“A vulnerability in the XML parser...could allow an unauthenticated, remote attacker to remotely execute code”

CAUTION

DO NOT ENTER

AUTHORIZED
PERSONNEL ONLY

SmartSign.com • 800-952-1457 • S-7418

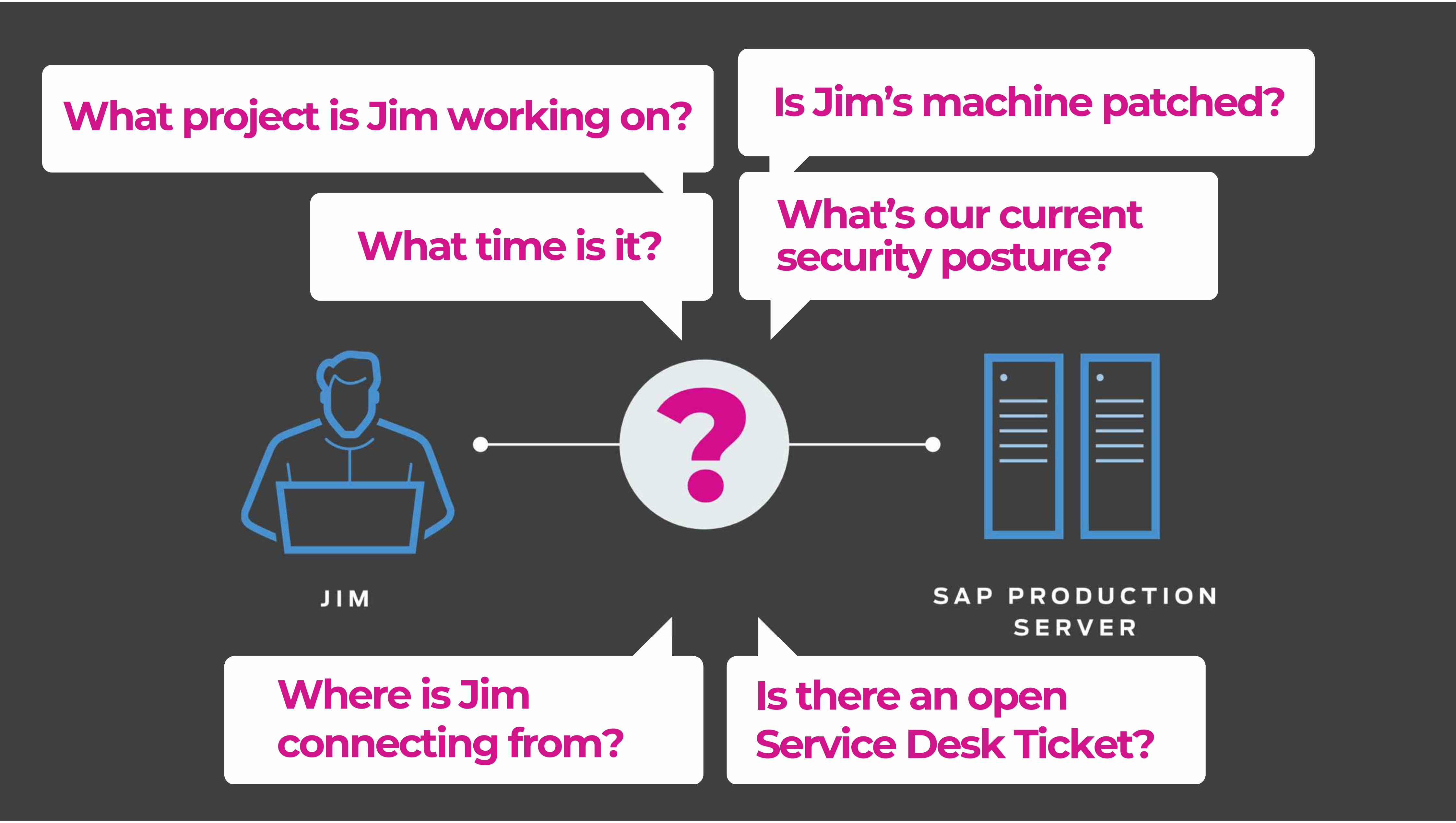

Come in We're
OPEN

Should 192.168.4.11 have access to 10.5.0.3?

Yes or No?

Should Jim have access to the production SAP® server?

It Depends


What project is Jim working on?
Is Jim’s machine patched?
What time is it?
What’s our current security posture?
JIM
SAP PRODUCTION SERVER
Where is Jim connecting from?
Is there an open Service Desk Ticket?

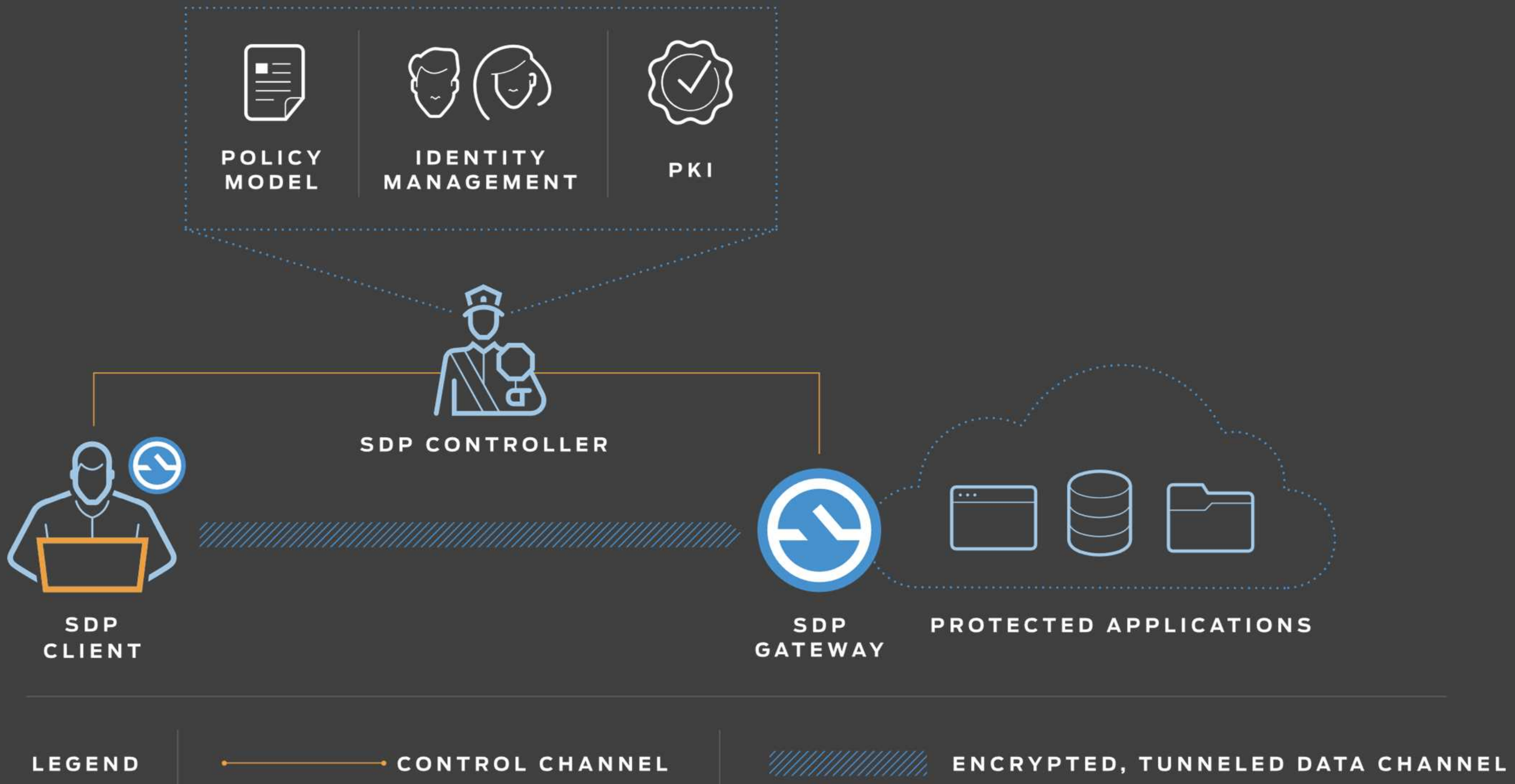
Access Control Requirements

Users, Servers, Microservices, and IoT Devices

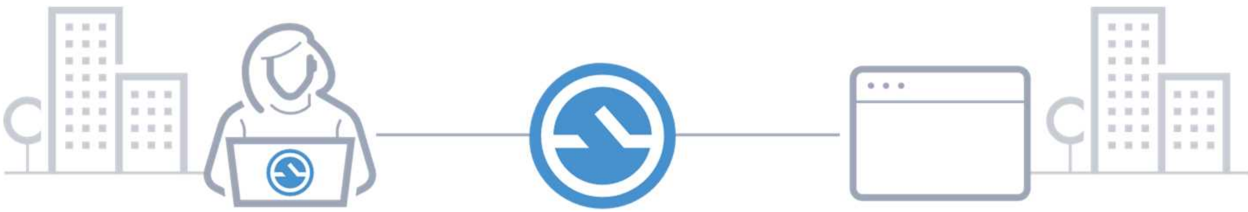
- **ALL** Users, **ALL** Services, **ALL** Environments
- Dynamically Adjusts Based on Context
- Software-Defined

The Software-Defined Perimeter

cloud security alliance®



On-Premises User Access



- Zero Trust Network
- Simple Authentication

Transparent User Experience	Sally turns on her computer and gets immediate access
Principle of Least Privilege	No network access except for applications she needs

Policy:

Allow employees in the Finance Department to access the Finance Reporting Server if using a company device
Authentication: Require password only if on corporate network

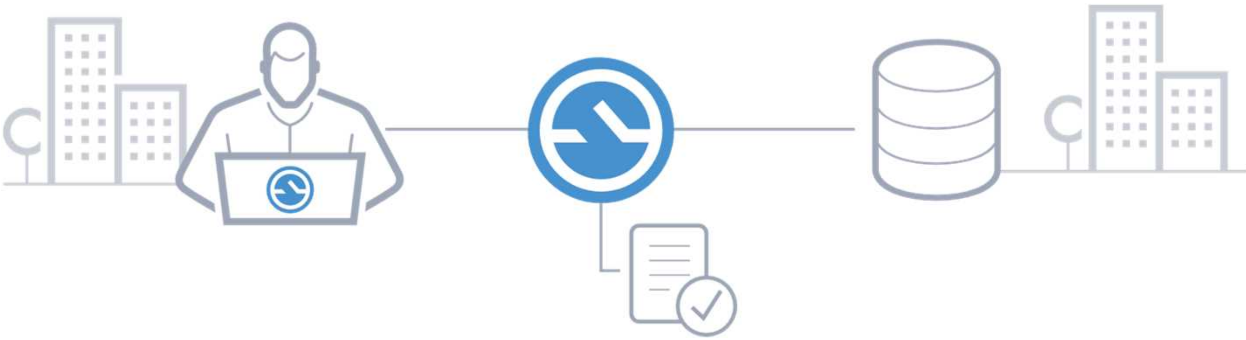
Remote User Access

- Secure Remote Connection
- Multifactor Authentication
- Client Ringfenced

Policy:

Allow employees in the Finance Department to access the Finance Reporting Server.
Authentication: Require MFA if remote
Security: Ringfence remote devices

Privileged User Access

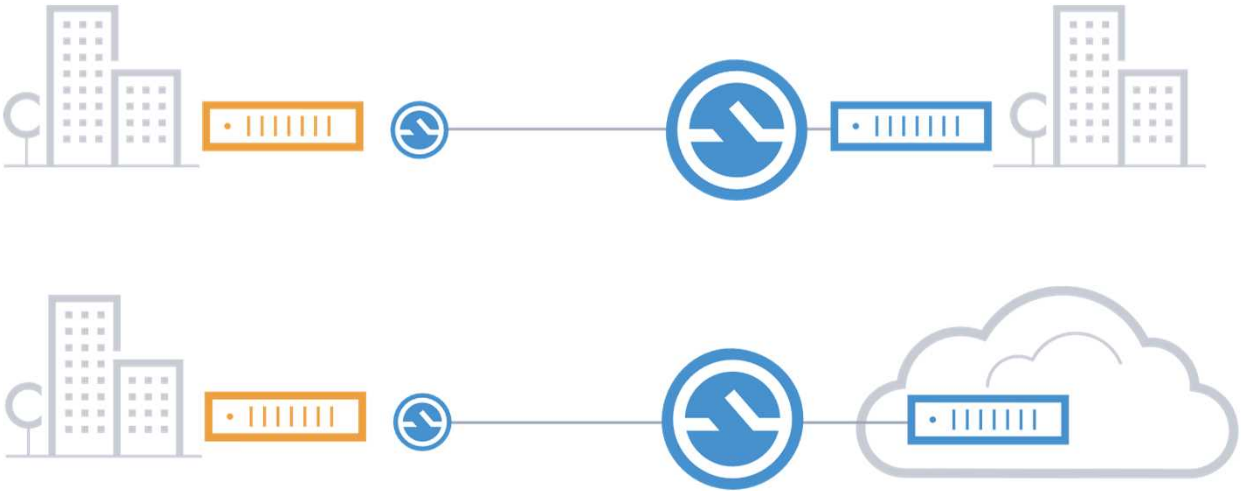


- IT Admin Access
- Multifactor Authentication
- Service Desk Ticket Check

Policy:

Allow IT admin access only if a Service Desk ticket is OPEN and names the user and the server.
Authentication: Always require MFA access

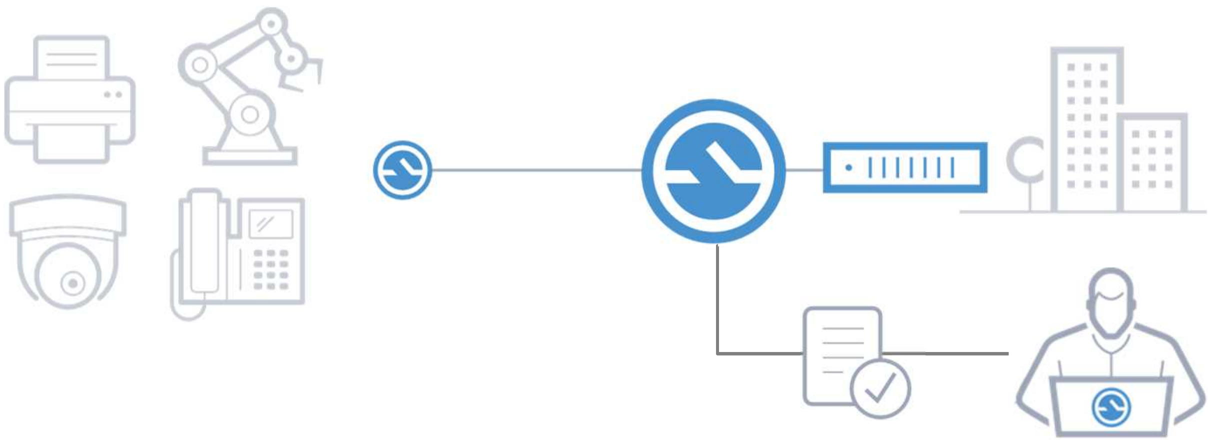
Server-to-Server Access



- Server-to-Server Access
- Within or Between Locations
- Cloud or On-Premises
- Identity-Centric and Policy-Based

Policy: Allow server-to-server access only for defined services, based on server identity.
Authentication: User server certificate store

IOT Device Access



- IoT Device to Server
- User/Server to IoT Device
- Fine-Grained Access Control
- IoT Device Identification

Policy:

Allow IoT Devices to **only** access their defined services, based on device type.
Authentication: Require Multifactor and Service Desk Ticket for all User Access

Summary

- Zero Trust is Achievable Today
- Requires a new approach to network security – the Software-Defined Perimeter

Take the first step in your journey to Zero Trust

Twitter: @JasonGarbis

テクマトリックス企業概要

商号	テクマトリックス株式会社
設立年月日	1984年8月30日
本社所在地	東京都港区三田3-11-24
代表取締役社長	由利 孝
資本金	12億9,812万円
従業員数	1,079名 (連結)
決算期	3月
一次店製品	

本社

Thank You

Cyxtera™

www.cyxtera.com