OWASP Meetup

Zero Trust in API Security

James Jinwon Lee / Security Solution Architect, F5 APCJ

What Problems Are We Trying to Solve in Zero Trust?

Enter Zero Trust

ELIMINATES THE IDEA OF A TRUSTED NETWORK INSIDE A DEFINED PERIMETER

"A way to think about cyberthreats is to assume you have already been compromised; you simply don't know it yet."

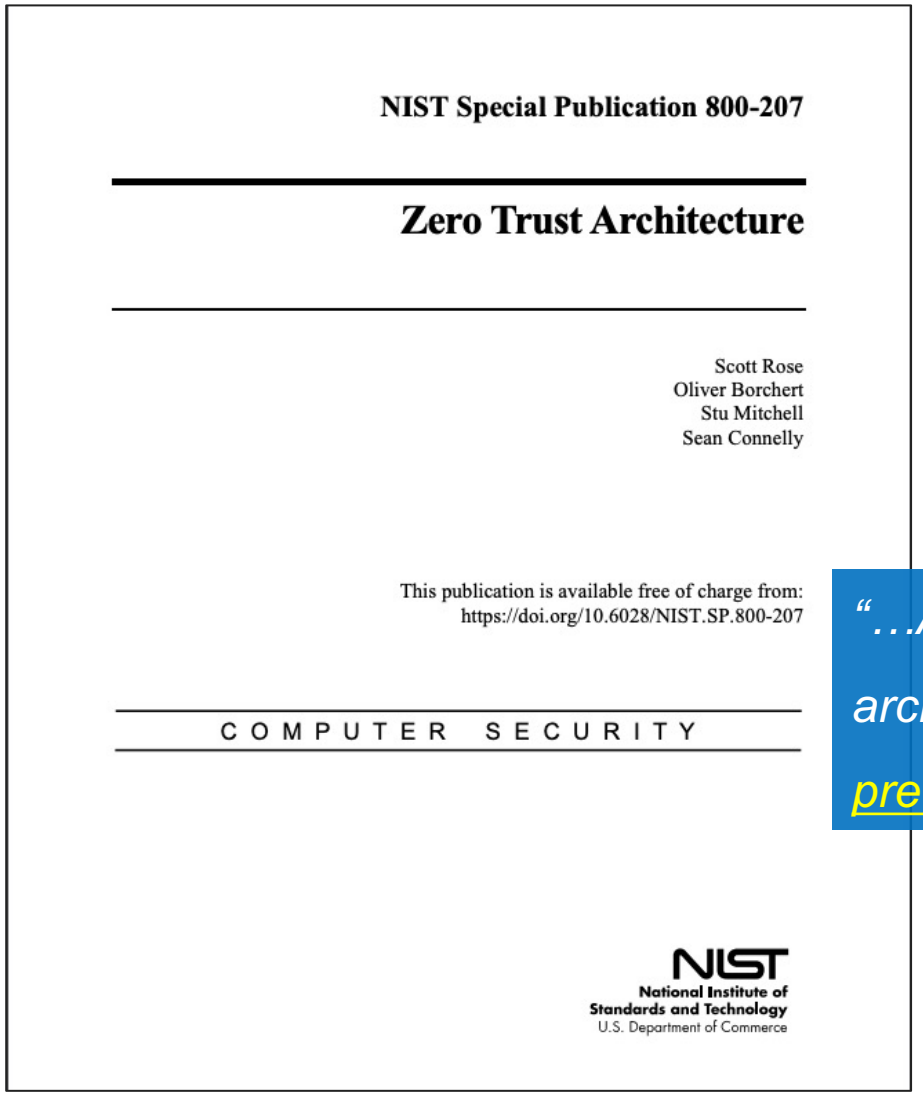
— FORRESTER®

THE ZERO TRUST PARADIGM

- Assume attackers are already on the network and lurking
- No environment is any more trustworthy than any other
- Assume no implicit trust
- Continually analyze and evaluate risks
- Mitigate risks

US NIST Technical Requirements of Zero Trust

Preventing Lateral Movement



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

"…A zero trust architecture (ZTA) is an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement…"

NIST 800-207 Report (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf)

Singapore Government Zero Trust - GovZTA

Scope

The GovZTA provides an overarching Enterprise Security Architecture to guide the coherent development of applications, infrastructure, and cybersecurity controls. It covers all aspects of an agency's digital estate (identity, infrastructure, systems, and applications) to ensure that trust is enforced and established under appropriate perimeters.

Users to Services (and vice versa)

ENFORCE & ESTABLISH TRUST:

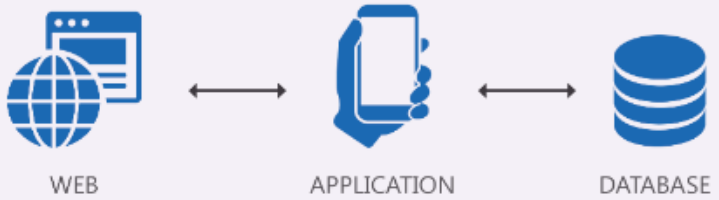
Only the **right people** have the **right access** to the **right services** from the **right devices**, under the **right circumstances**.

User-To-App or N/S Traffic

Services to Services

ENFORCE & ESTABLISH TRUST:

Only the **right service identity** has the **right access** to the **right services and data** using the **right secret key**, under the **right circumstances**.



App-To-App or EW Traffic

https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/government-zero-trust-architecture

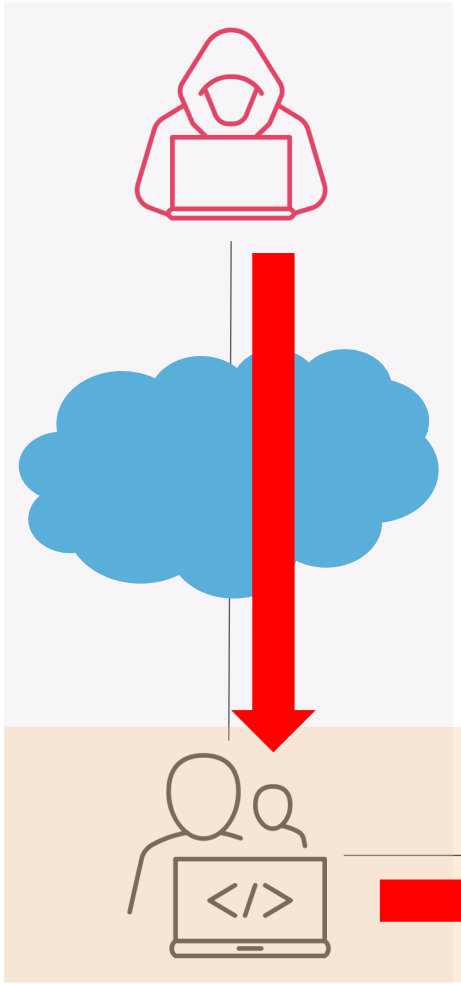
Singapore Government Zero Trust Best Practice

Control Points	GovZTA Principles	Desired Outcomes
STRENGTHENING ARCHITECTURE ACCESS	Apply Least Privilege and Enforce Access Control	**Users, devices, and applications** are assigned groupings and specific permissions, enforcing the principle of least privilege within an identity-based trust system. Trust is actively verified using a **standardised enforcement point** as well as **dynamic access policies** to authenticate and authorise access to resources on a per-request basis.
SECURING APPLICATION SERVICES	Limit Lateral Movement	**Blast radiuses of breaches are minimised** by micro-segmenting the network, isolating applications, and logically segregating data.
ENHANCING OPERATIONAL READINESS	Integrate Security Automation & Orchestration	**Automated process** workflows are used to achieve the **continuous integration and continuous delivery** of services, which are built on repeatable baselines.
	Enhance Detection & Response	**Aggregate logs across the platform**, host, network, application, and data layers to **analyse security information and application performance**.

https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/government-zero-trust-architecture

Technical Requirements of Zero Trust

Preventing Lateral Movement

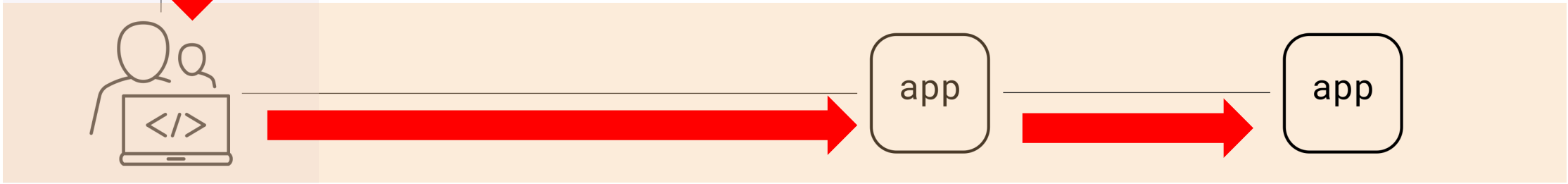


Initial compromise (Malware attack)

- **Pass-the-hash:** In this technique, an attacker steals the password hash from a system and then uses that hash to authenticate to other systems on the network.
- **Pass-the-ticket:** The attacker steals a Kerberos ticket from a system and then uses that ticket to authenticate to other systems on the network, like active directories. Pass-The-Ticket attacks, such as a Golden Ticket attack or a Silver Ticket Attack, are powerful techniques adversaries employ for post-exploitation lateral movements and privilege escalation. Using these techniques, attackers can gain unlimited access to any endpoint on the network or service, potentially causing catastrophic consequences.
- **Exploiting vulnerabilities:** An attacker exploits vulnerabilities in systems to gain access and then uses that access to move laterally within the network.
- **Using stolen credentials:** The attacker steals valid credentials from a system and then uses those credentials to authenticate to other systems on the network.

Source: SentinelOne Website

Lateral movement attack



What are the solutions?

Common Mi

Is it easy to detect usi

PROFILE

Chanam Park

Seoul, South Korea

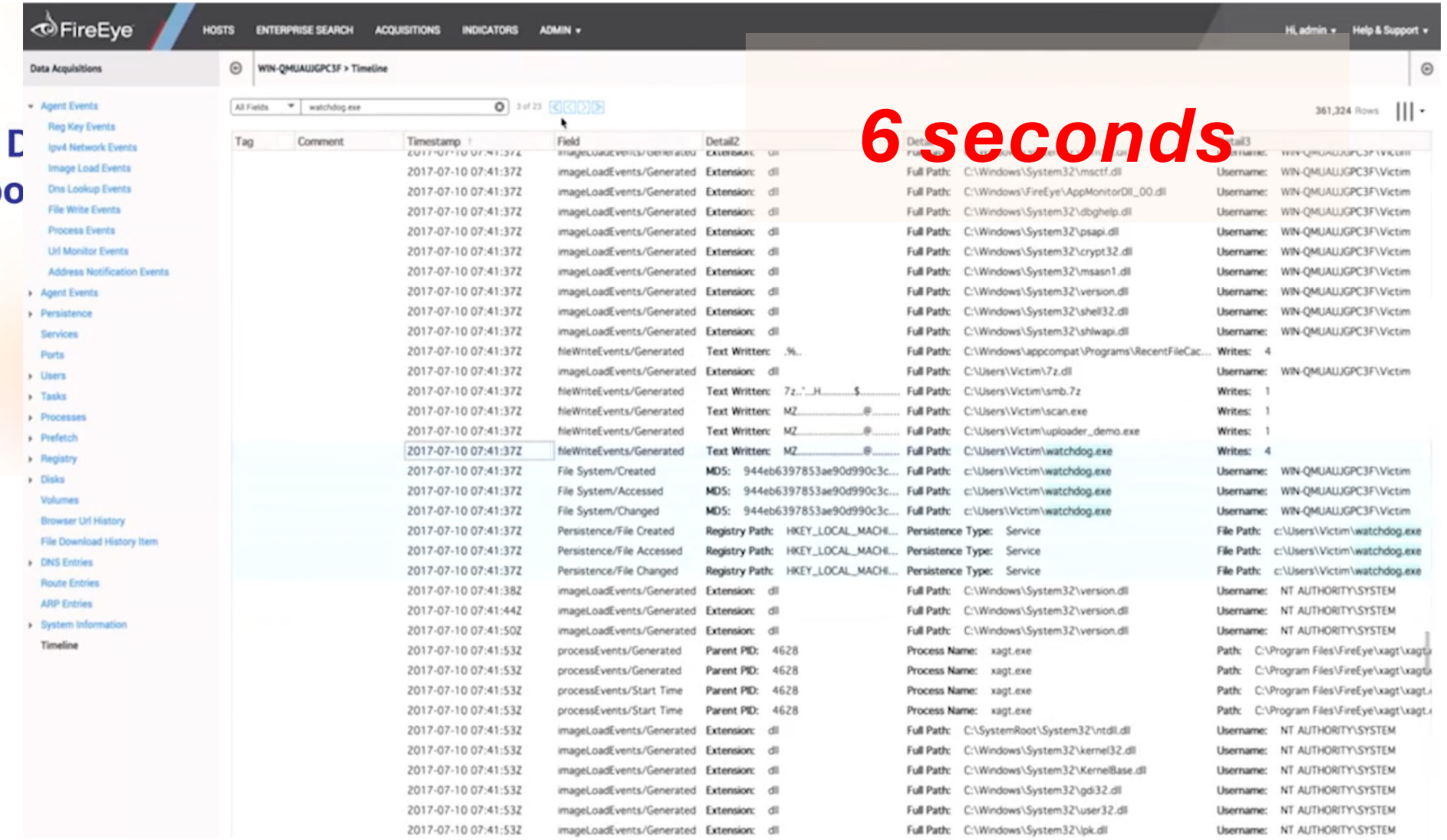
"...Once you access the internal network, you need to explore the inside of an organization's network to perform the lateral movement attack. Then, you can find many interesting things from the enterprise network. SOC normally thinks they already have many security solutions to prevent lateral movement attacks, but in reality, the internal network is much more vulnerable than you think..."

Chanam Park - Whitehacker

Common Misunderstandings

Is it easy to detect using the latest technologies?

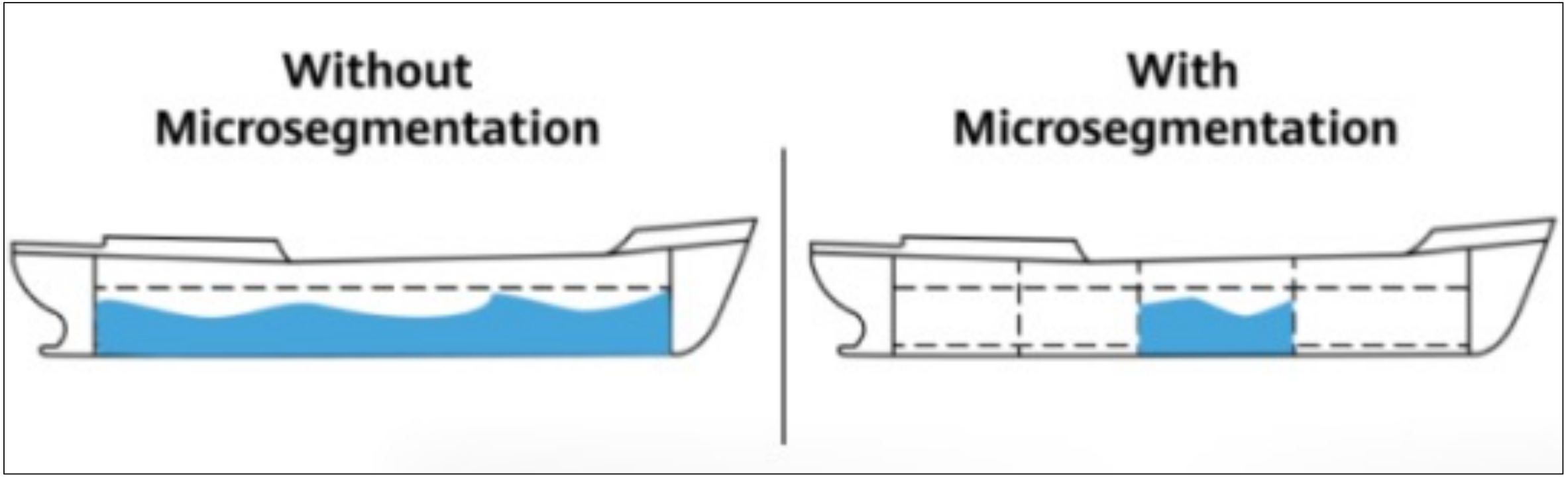
Endpoint D
and Respo



6 seconds

X-Segmentation

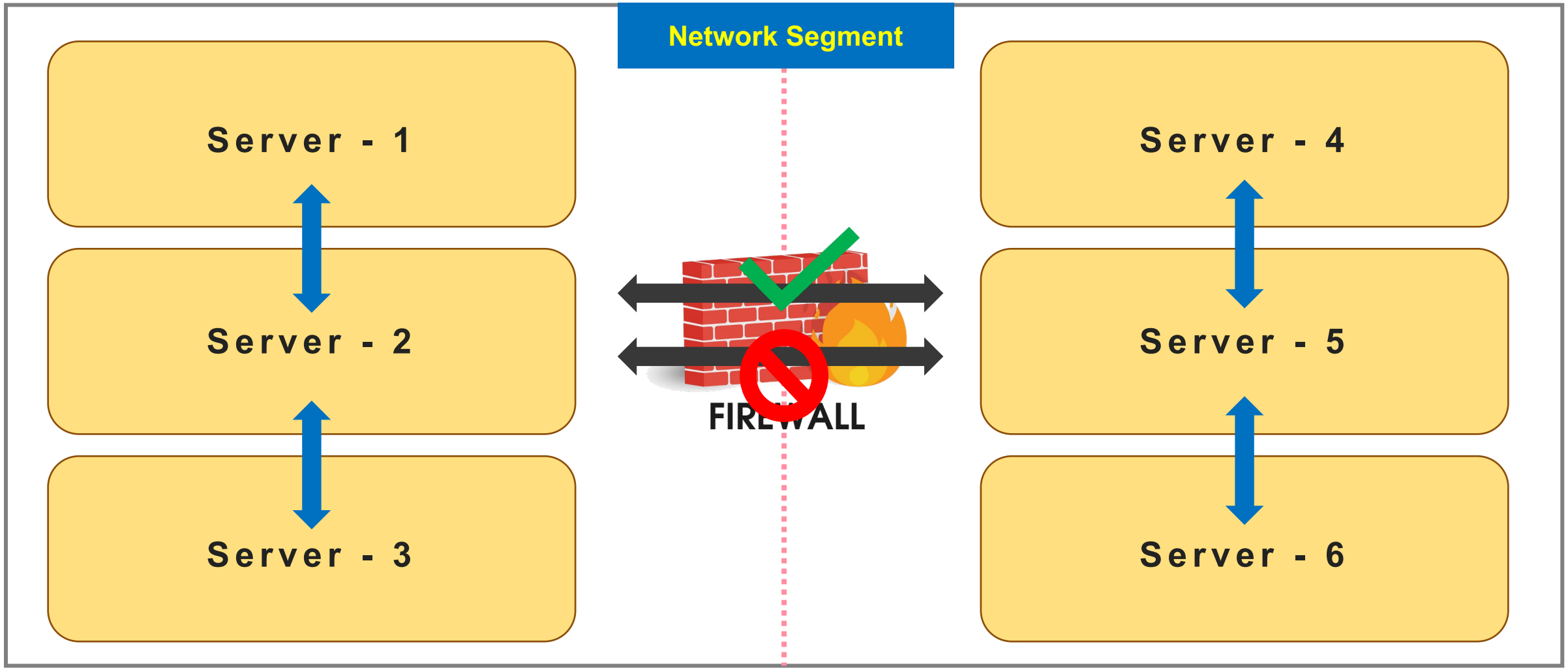
Rise of Micro-Segmentation



Source: https://support.huawei.com/enterprise/fr/doc/EDOC1100196735

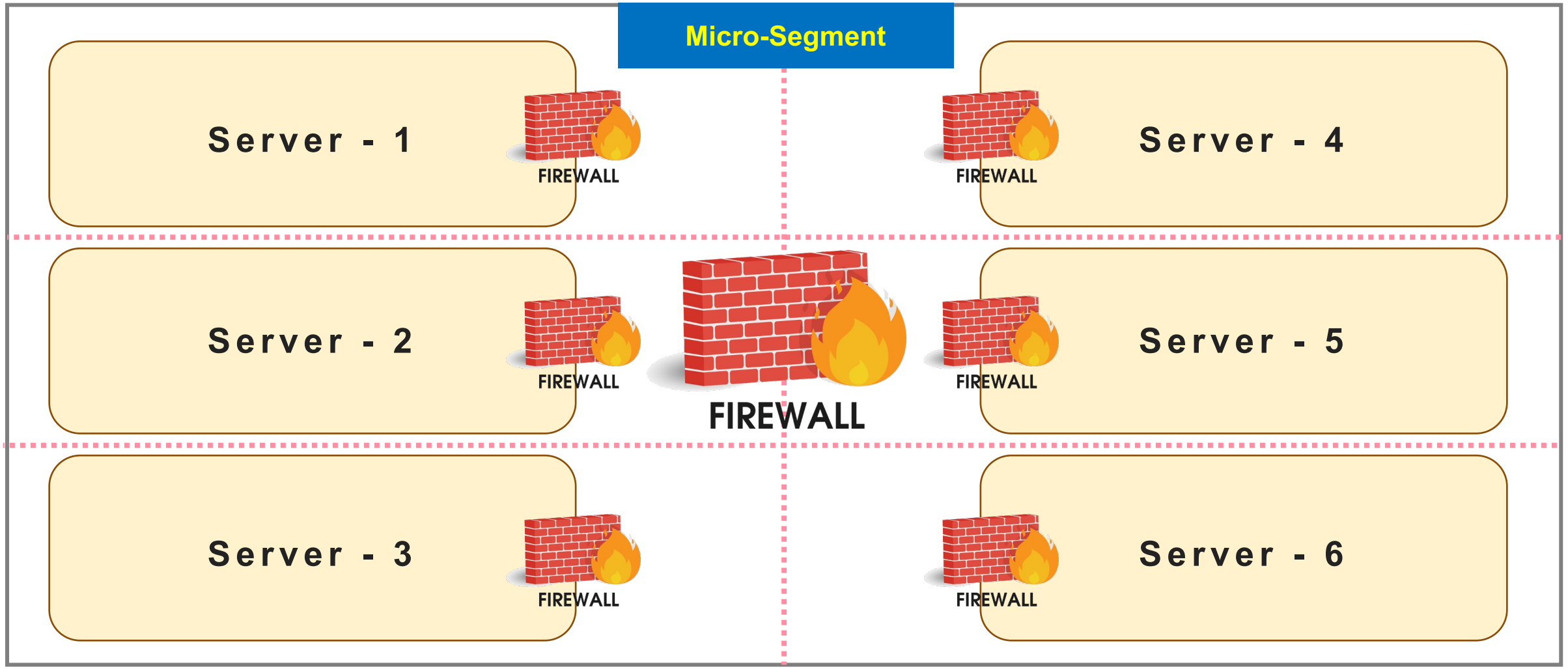
Current Product Offering of X-Segmentation for Zero Trust

Network Segmentation



Current Product Offering of X-Segmentation for Zero Trust

Micro-Segmentation



Micro-segmentation

Different Segmentations for Zero Trust App Access

Network Fabric

- Requires SDN controller (e.g. Cisco ACI, Arista CloudVision, etc)
- Not supported on public clouds
- Requires specific network implementation
- It may increase the latency or cause a bottleneck.

Agent-based

- Most effective technical option for the micro-segmentation
- Agent fatigue in many organizations
- Increase the operational costs

Hypervisor

- Considered easy to implement
- Not supported on public clouds and traditional DC
- Supported for VMs only
- It may increase the latency or cause a bottleneck.

Network-based

- Easy to implement
- Supported all deployment models
- Requires small IP-based subnets
- Increase the complexity of the network design

Challenges of Current Product Offering of Micro Segmentation

Challenges of Micro Segmentation in Real World

Complexity	• Requires deep knowledge of networks, applications, and risk level of enterprise assets. • Need to manage all different security policies on a ‘micro-segment' basis.
Dependency	• It sometimes has a dependency on the solution of the ‘Micro Segmentation’. • For example, the ‘Network fabric’ method is normally not supported in a public cloud.
Limited Access Control	• Most micro-segmentation security policy uses layer-4 level attributes. (Except the agent-basis method.) • Requires SSL/TLS termination(or decryption) to inspect the encrypted traffic. (Agent-basis naturally can inspect this types of traffic)
Agent fatigue	• While the agent-basis method provides much more benefits than other methods, it introduces operational complexity. • Many organizations have an ‘agent-fatigue’ issue.

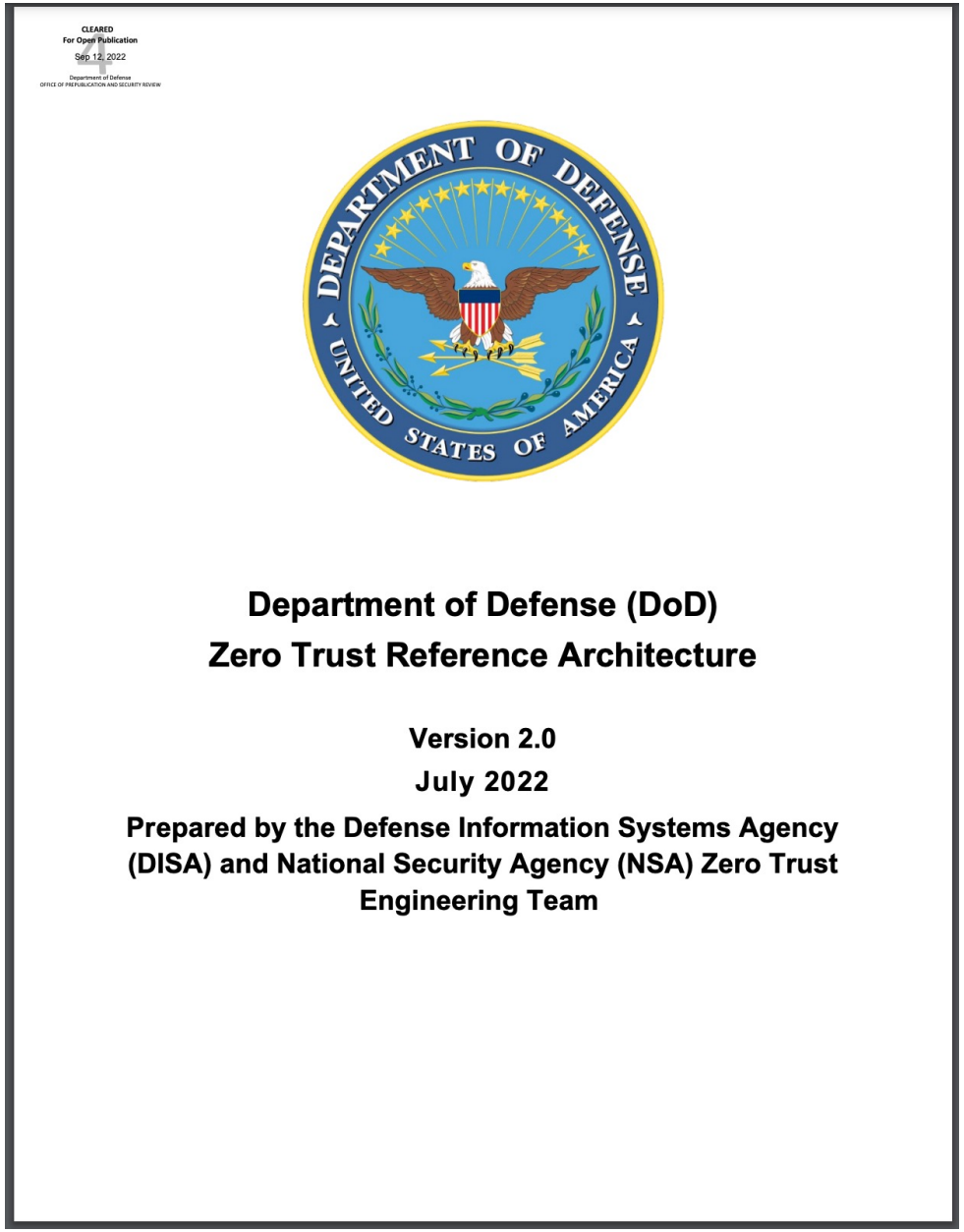
API Micro Segmentation

US DoD:

Zero Trust

Reference

Architecture



datacenter resources and cloud services accessible via the Internet. All requests for access will be highly scrutinized using continuous multi-factor authentication and the concept of least-

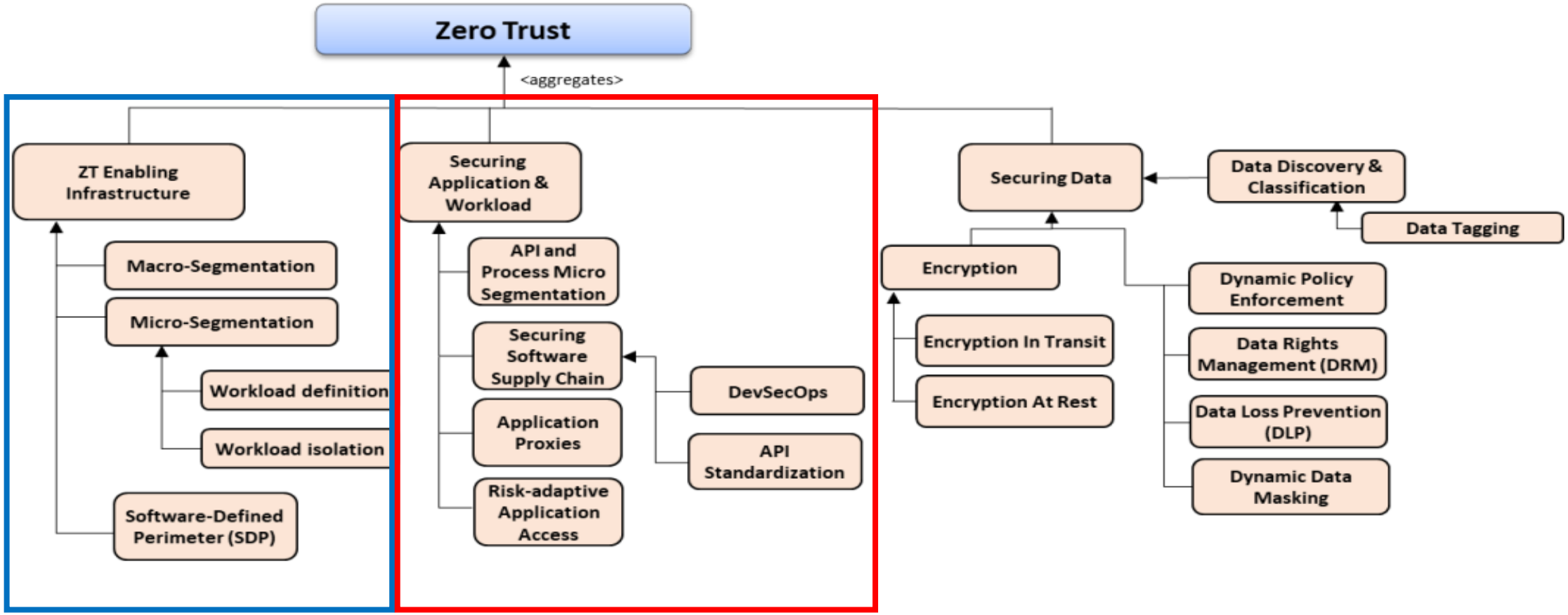


Figure 8 Zero Trust Infrastructure, Workload and Data Capability Taxonomy (CV-2)

Network-based Segmentation

Application-based Segmentation

- Prevent and Curtail Lateral Movement
- Explicitly Allow Authorizations (Deny by Default)

Figure 22 East-West Segmentation (OV-1)

The ZT-enabling Infrastructur aggregate capability includes all the capabilities that impact the Network and Environments resources Pillar nodes of travel among the enterprise. This also cloud resources. Controls built around capabilities. A macro and micro segmentati isolating specific workloads as long as the wo for not only interconnection between req requirements of connection for Software Def

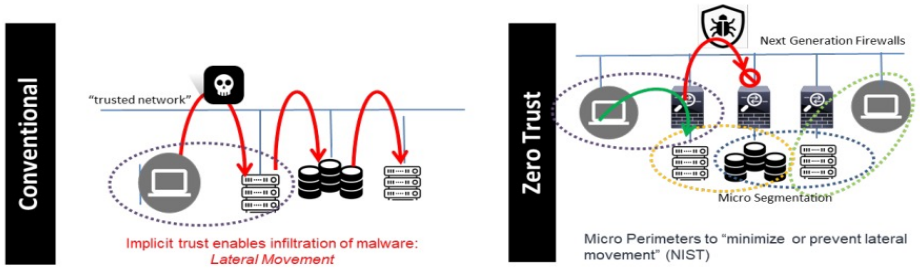
The Securing Application and Workload ag surround the Workloads Pillar. These capab data to end users. These capabilities aim t practices, and segment the application into d into this zone are highly scrutinized and bro convergence to a standardization of applica changes and updates.

The Securing Data aggregate capability incl These capabilities are the closest to the d securing data whether it be tagged data, encrypting of sensitive data. Securing Data information regardless of the effectiveness o

July 2022

datacenter resources and cloud services accessible via the Internet. All requests for access will be highly scrutinized using continuous multi-factor authentication and the concept of least-privilege. In this model, formerly external users do not incur additional latency by hair-pinning through a VPN.

4.11 East-West Segmentation (OV-1)



- Prevent and Curtail Lateral Movement
- Explicitly Allow Authorizations (Deny by Default)

Security states of previous deployments of application and server stacks have had issues involving implicit trust in communication between systems. This trust has allowed malicious users and devices the ability to traverse through the environment with relative ease. Once through the perimeter controls malicious users and software can move laterally across to infect or attack systems and data within the area of influence. ZT aims to enhance the security posture of static DMZ network configuration by only allowing the specific communication that is required for the applications to work and implement ever evolving controls. Micro-segmentation will require communication between devices to be limited with just enough access to complete the intended task of communication between servers, devices and applications. Communication will be controlled not only at the network level between hosts, but also from process to process and in the application stack through API Micro-segmentation. Additional Authentication and Authorization will be part of each step of the process towards the data layer.

Micro Firewall vs Micro Proxy Approach

The Cybersecurity Domain Controller directs the agents/Micro Firewalls on the virtual machines. The Micro Firewalls are the PEP
The Micro segment is realized by the policy statements to the micro firewalls by the ZT policy controller.

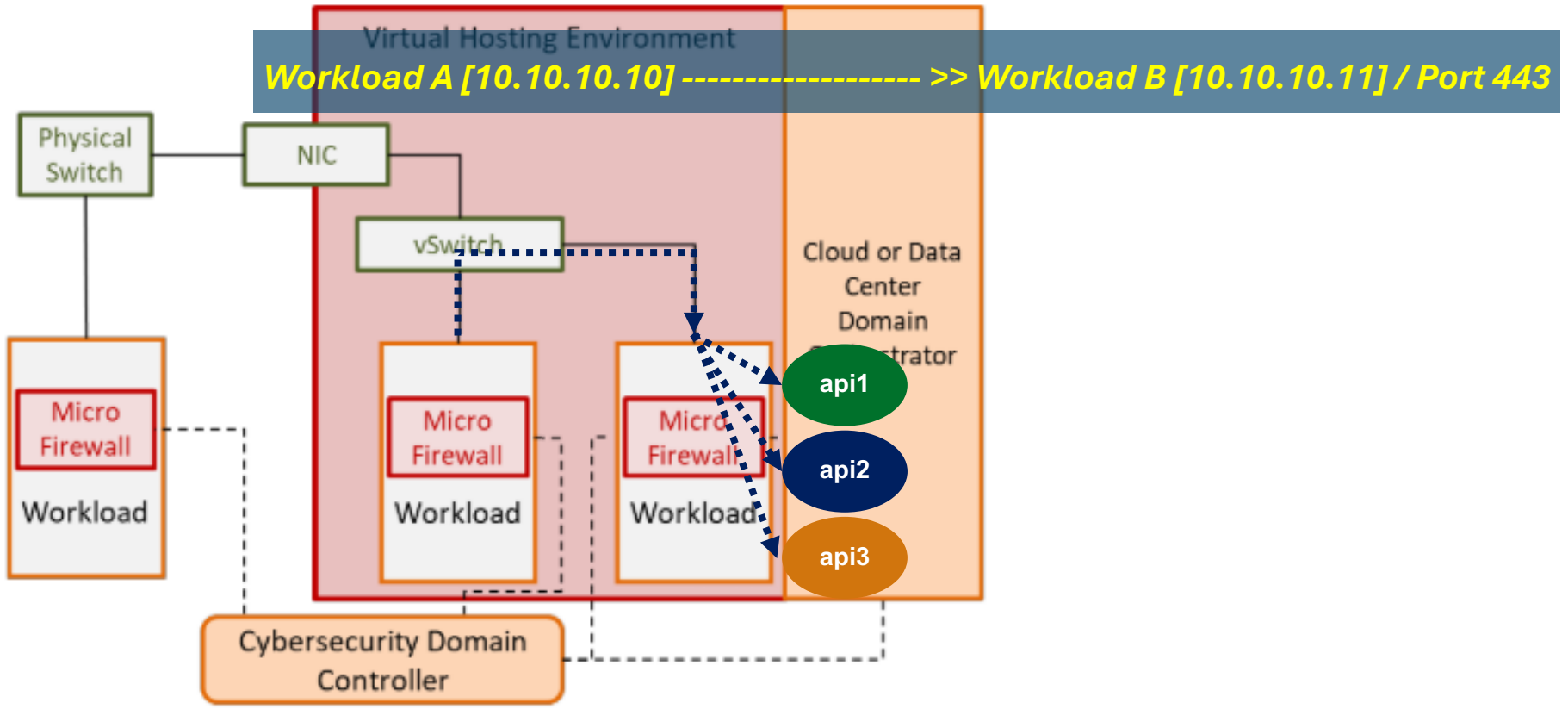


Figure 36 SoS Micro Segmentation (SV-1)

Micro Firewall vs Micro Proxy Approach

- *Workload A must obtain the 'OAuth token' first before accessing Workload B.*
- *Workload A can access APIs in Workload B but with different privileges.*
- *Access API#01 with 'Read privilege.'*
- *Access API#02 with 'Read/Write privilege.'*
- *But can NOT access API#03.*

The Cybersecurity Domain Controller directs the agents/Micro Firewalls on the virtual machines. The Micro Firewalls are the PEP
The Micro segment is realized by the policy statements to the micro firewalls by the ZT policy controller.

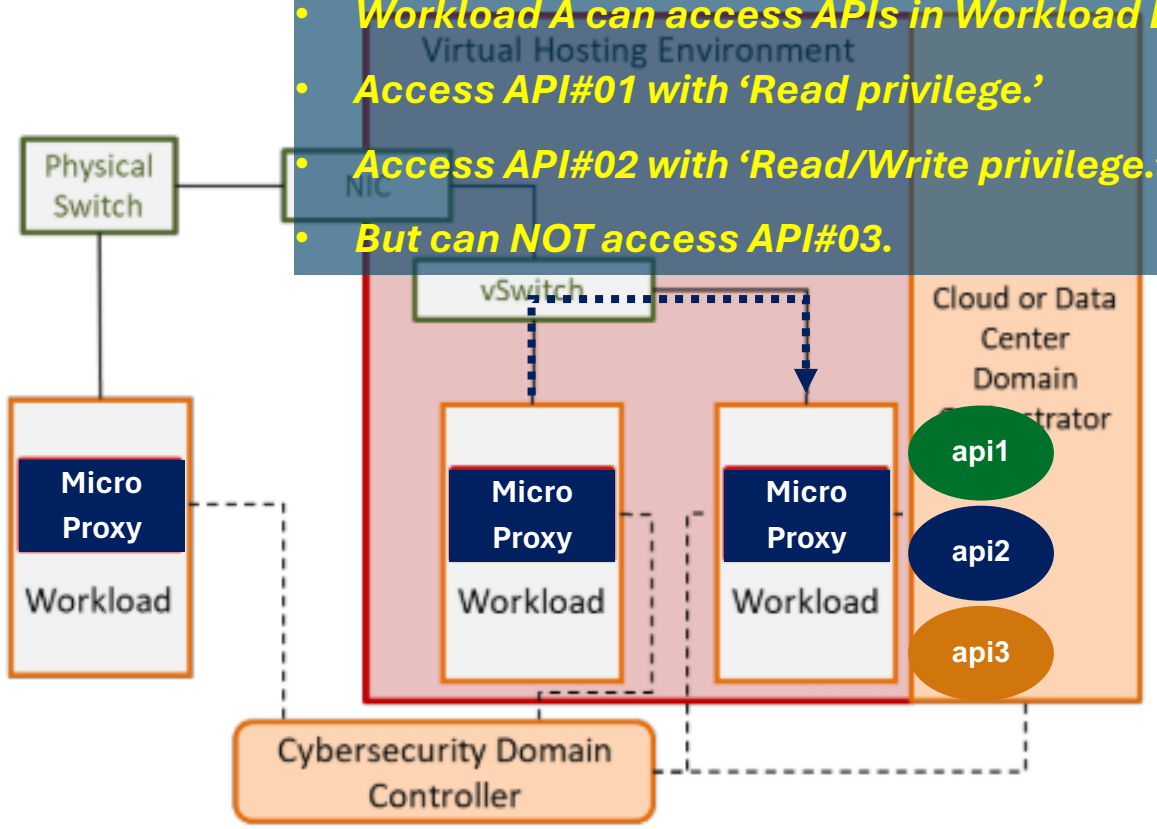


Figure 36 SoS Micro Segmentation (SV-1)

Learning from Real-World Case

Data Breach happens in Cloudflare

Brief Analysis of the Breach

Nation-state actor used recent Okta compromises to hack into Cloudflare systems

News

05 Feb 2024 • 4 mins

Data Breach | Hacking

The hack, which used stolen tokens and credentials, was able to acces
amount of source code" before being thwarted.

CLOUDFLARE

The Cloudflare Blog

Email Addr

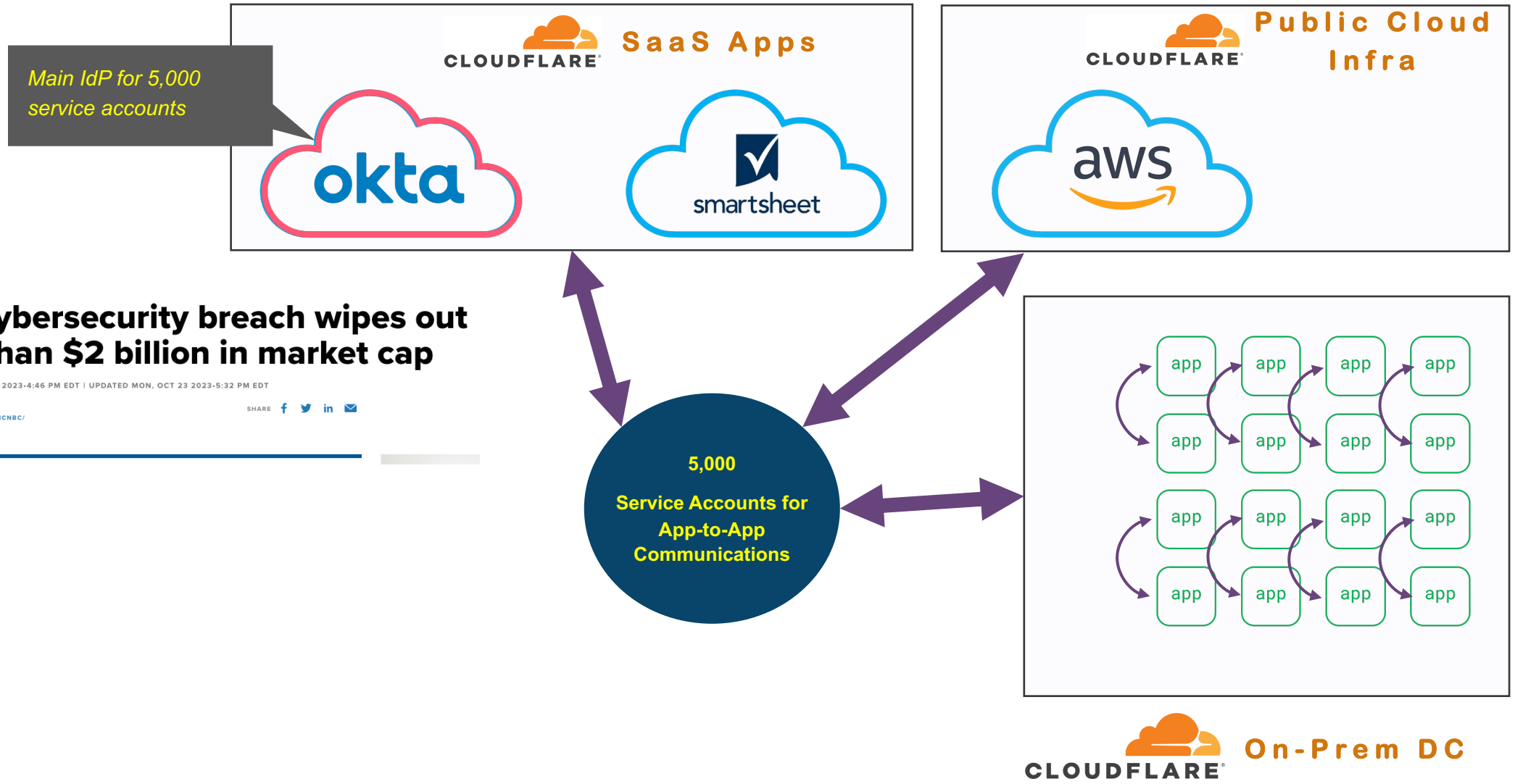
Product News | Speed & Reliability | Security | Serverless | Zero Trust | Developers | Deep Div

Thanksgiving 2023 security incident

02/02/2024

5,000 Service Accounts Used for Massive App-to-App Access

Everything was begun from the App-to-App Access



TECH

Okta cybersecurity breach wipes out more than $2 billion in market cap

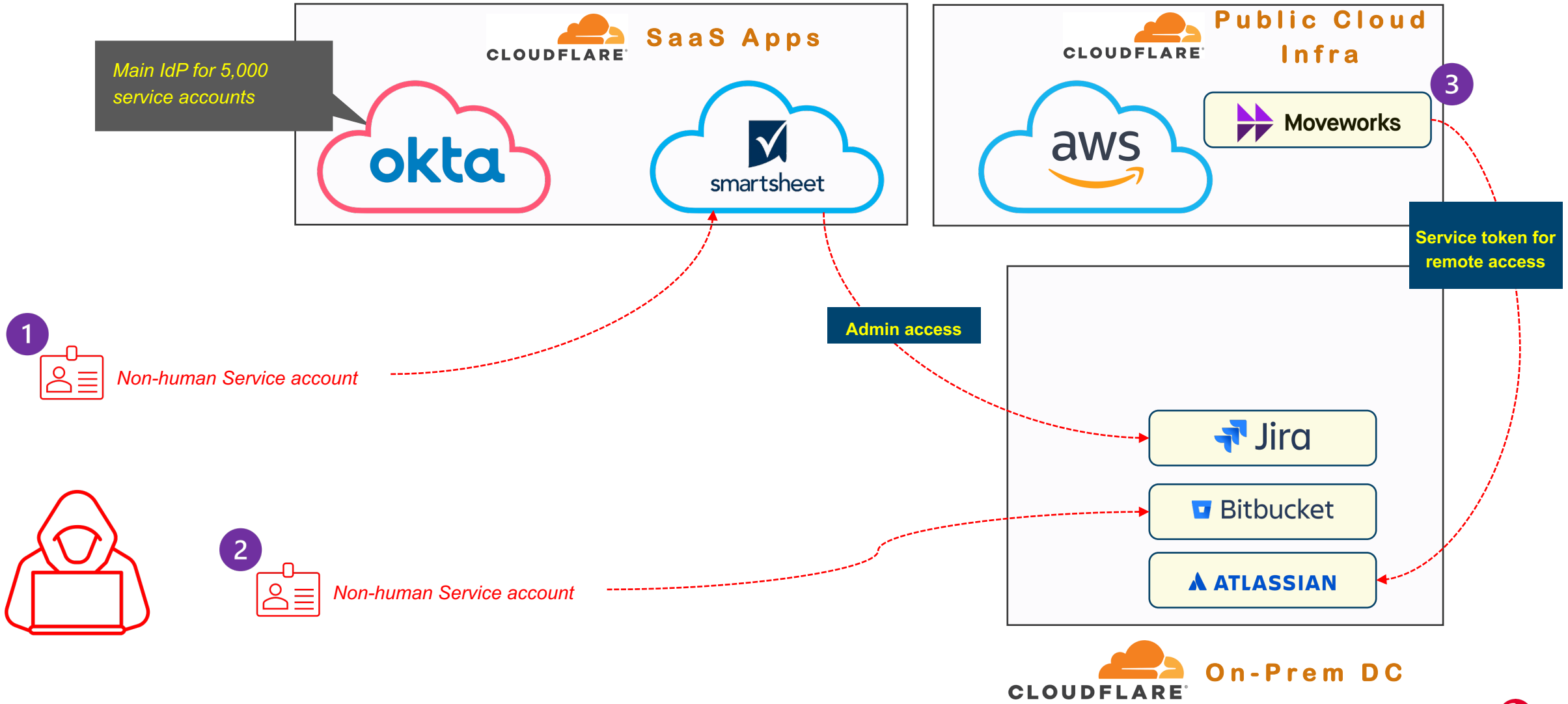
PUBLISHED MON, OCT 23 2023·4:46 PM EDT | UPDATED MON, OCT 23 2023·5:32 PM EDT

Rohan Goswami
@IN/ROHANGOSWAMICNBC/
@ROGOSWAMI

SHARE

5,000 Service Accounts Used for Massive App-to-App Access

Everything was begun from the App-to-App Access



Real World Breach Case by the ‘East-West App-to-App’ Access

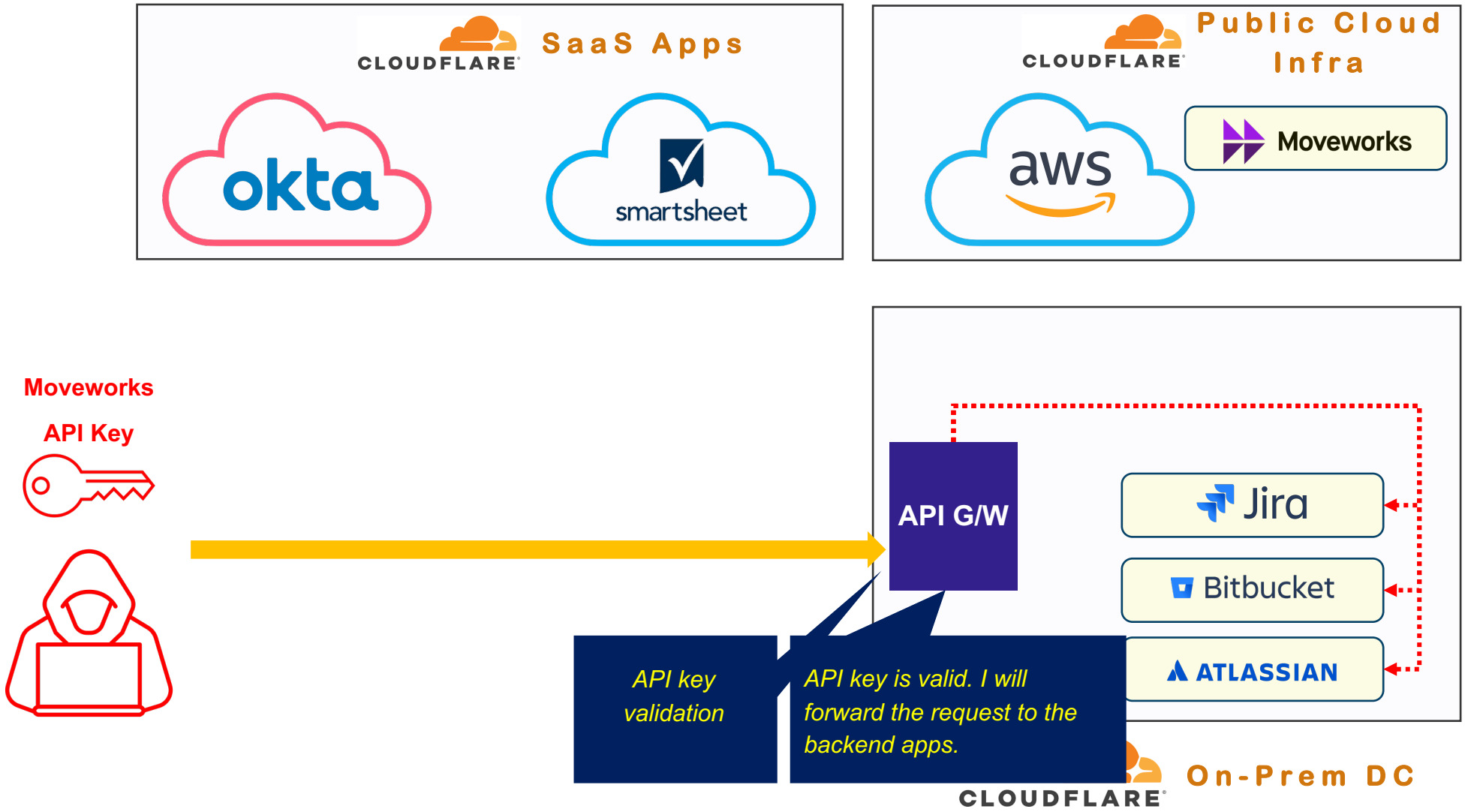
The Importance of the ‘East-West App-to-App’ Protection

November 15 16:28:38 - threat actor gains access to Atlassian services

The threat actor successfully accessed Atlassian Jira and Confluence on November 15 using the Moveworks service token to authenticate through our gateway, and then they used the Smartsheet service account to gain access to the Atlassian suite. The next day they began looking for information about the configuration and management of our global network, and accessed various Jira tickets.

Real World Breach Case by the ‘East-West App-to-App’ Access

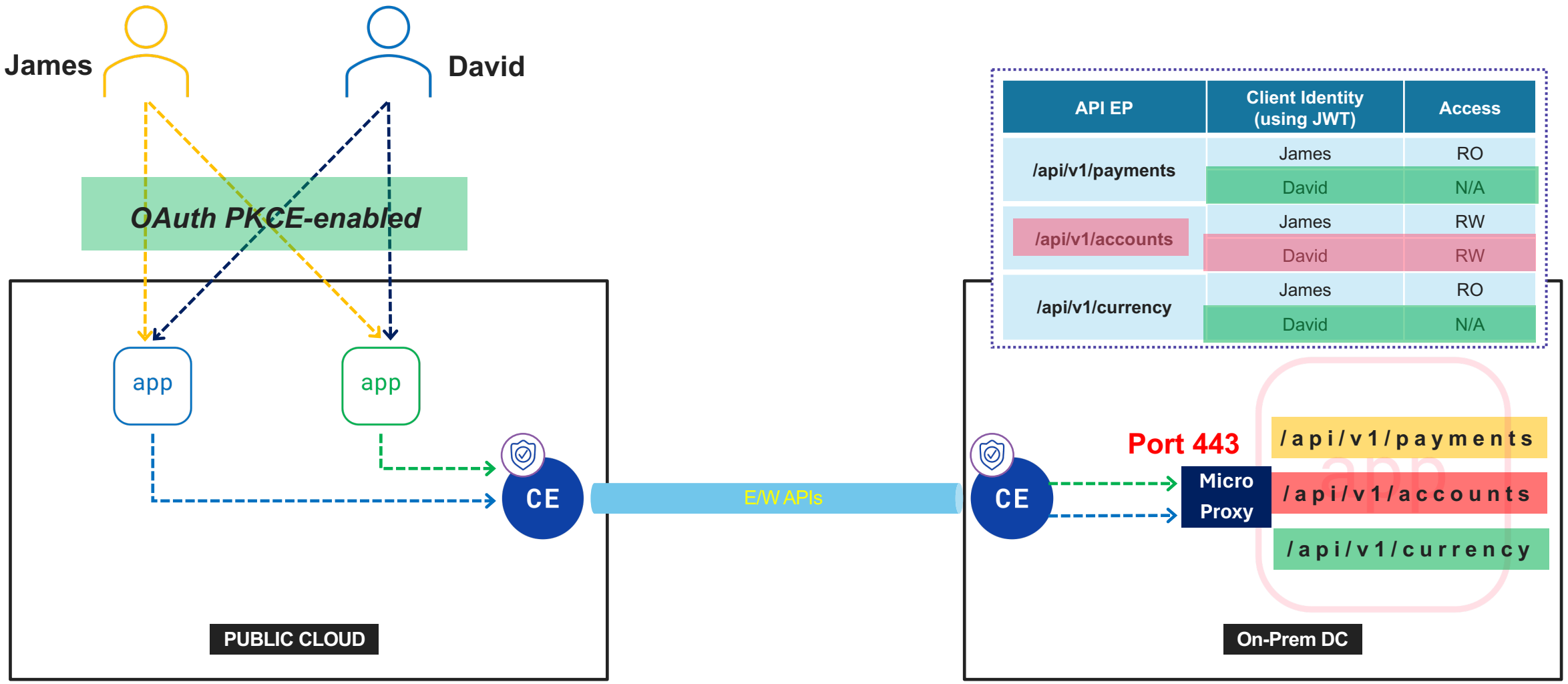
The Importance of the ‘East-West App-to-App’ Protection



Zero Trust API Access with API Micro-Segmentation

API Microsegmentation – Micro Proxy Control

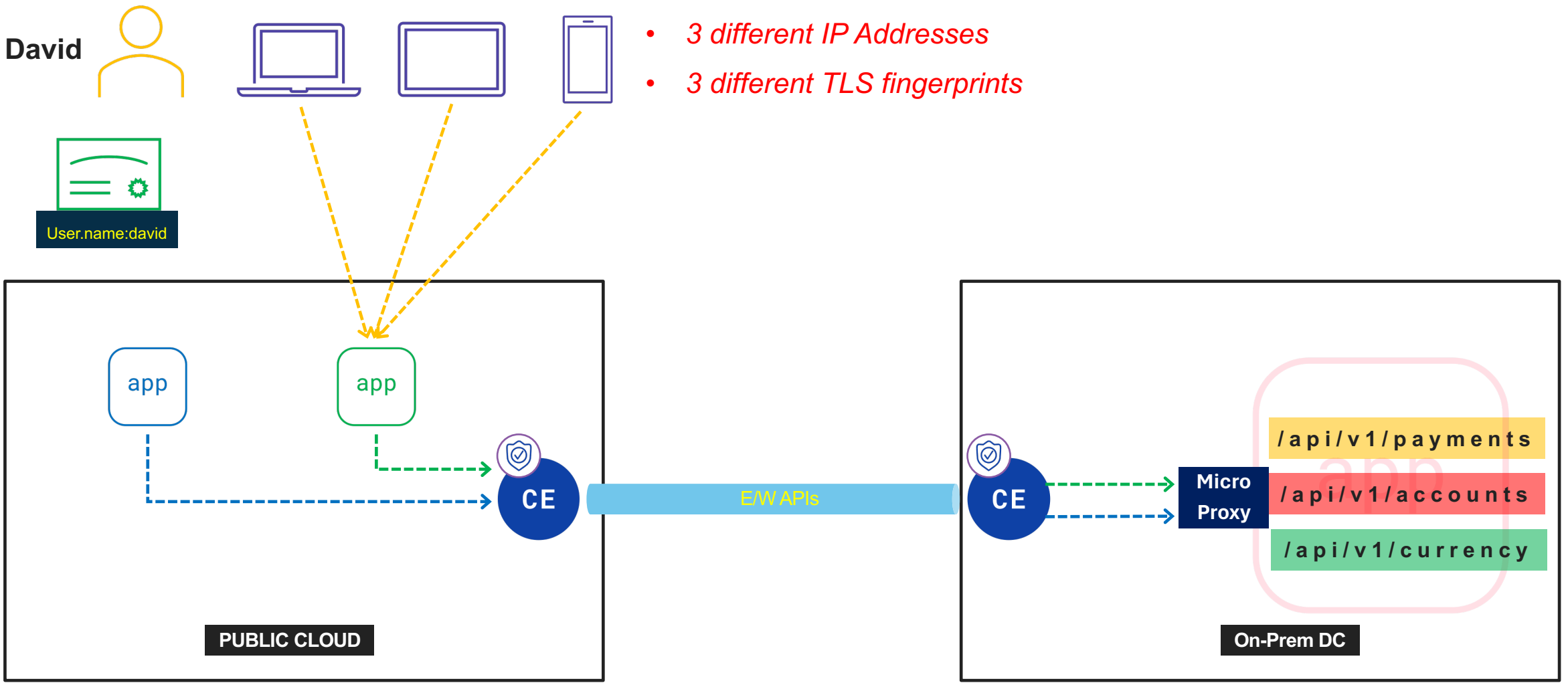
API Micro-Segmentation Flow Diagram



API EP	Client Identity (using JWT)	Access
/api/v1/payments	James	RO
	David	N/A
/api/v1/accounts	James	RW
	David	RW
/api/v1/currency	James	RO
	David	N/A

API Microsegmentation – Behavioral Detection

API Micro-Segmentation Flow Diagram

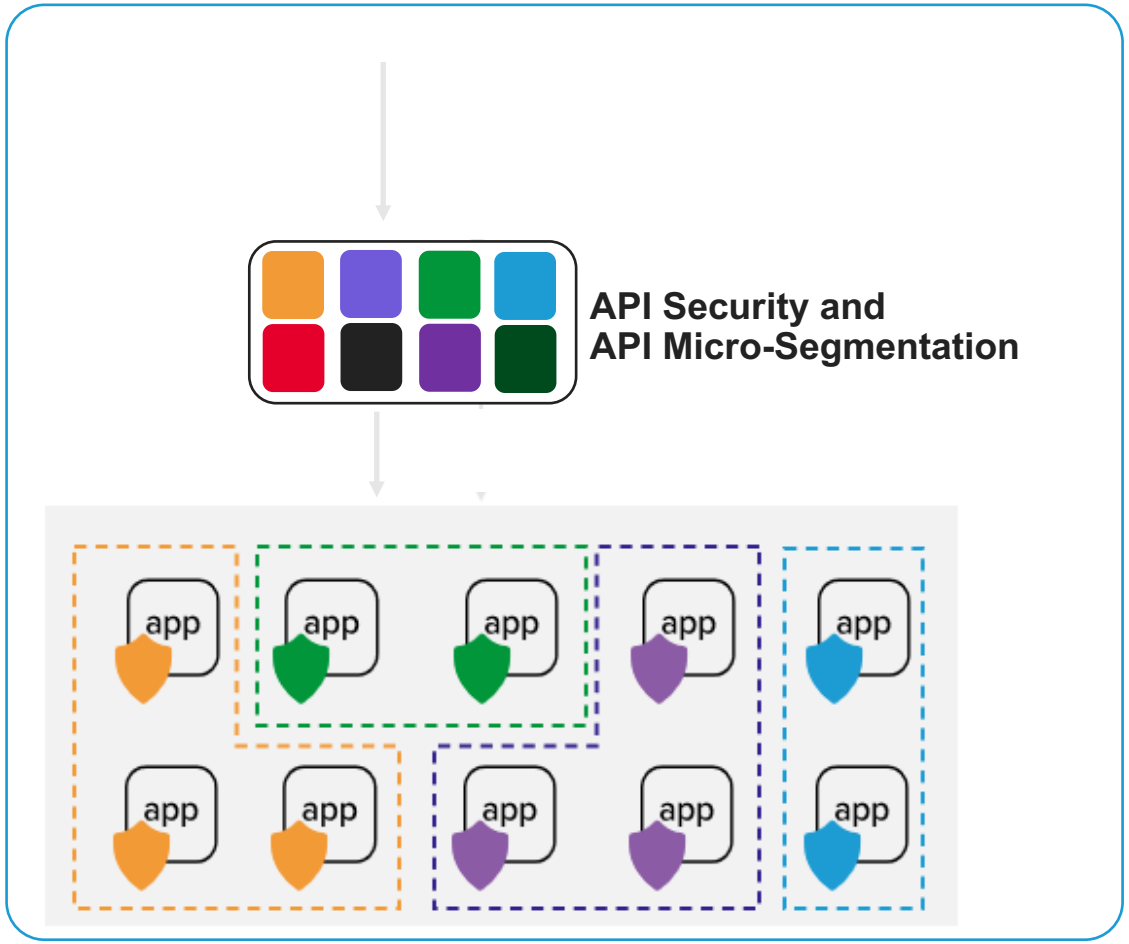


- *3 different IP Addresses*
- *3 different TLS fingerprints*

Zero Trust API Access with API Micro-Segmentation

Benefits of API Security + API Micro-segmentation

- **Enhanced defense**: The layered approach provides multiple layers of security, making it difficult for attackers to breach defenses.
- **Reduced attack surface**: By isolating APIs and controlling traffic flow, attackers have fewer opportunities to exploit vulnerabilities.
- **Improved data protection**: Sensitive data transmitted through APIs is protected by both API security controls and network segmentation.
- **Faster incident response**: Breaches can be contained within smaller segments, minimizing the impact and simplifying incident response.



MICROSEGMENTATION

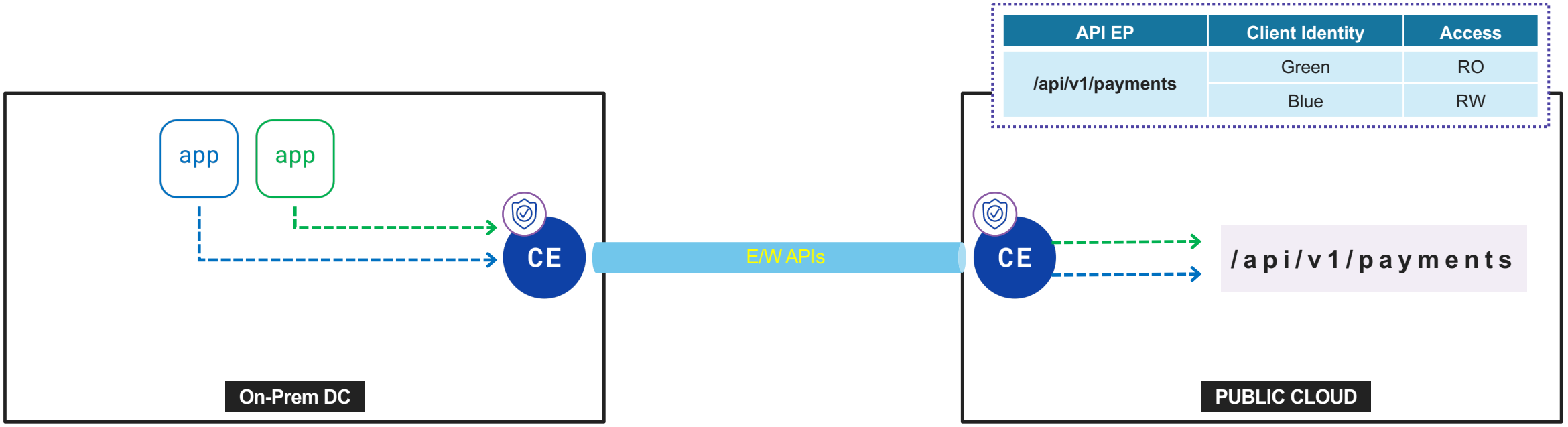
Each API endpoint is isolated into a network segment

Granular rules control east-west traffic between API segments and other internal services.

Each API server runs within its own secure segment, minimizing the attack surface.

East-West API Microsegmentation

API Micro-Segmentation Flow Diagram



- API calls in the East-West flow can be segmented with the relevant API-group basis.
- For example, the 'Green' app in the on-prem DC can access the 'Green API endpoint' in the public cloud with the 'Read privilege'. However, the 'Blue App' in the DC can access the same API endpoint, but can perform more actions.
- F5 XC CE can apply a different set of API security policies based on the app identity in this case.