



N E V E R U J N I K O M E 2 0 2 3

Zero Trust Network Access

Zero Trust is a Fundamental Shift in Security Approach
Never Trust, Always Verify

Dubravko Hlede





Compromised Credentials

Over **80%** of breaches within hacking involve brute force or the use of lost or stolen credentials.

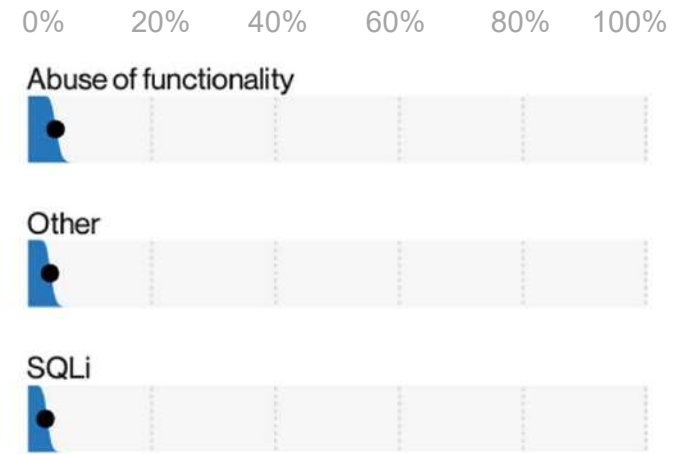
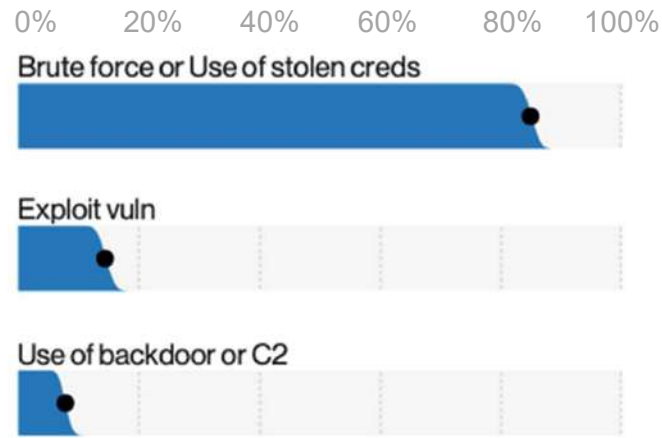


Figure20. Top Hacking varieties in breaches (n = 868)



Compromised Devices

40% of breaches involved compromised web application servers.

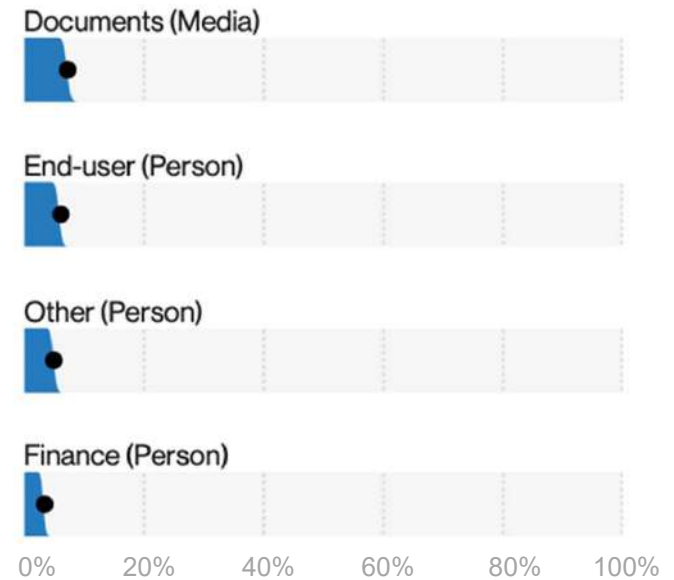
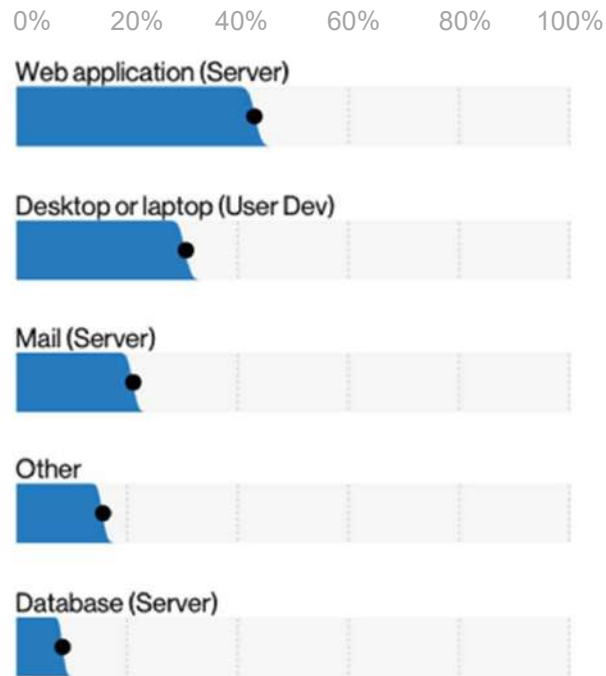
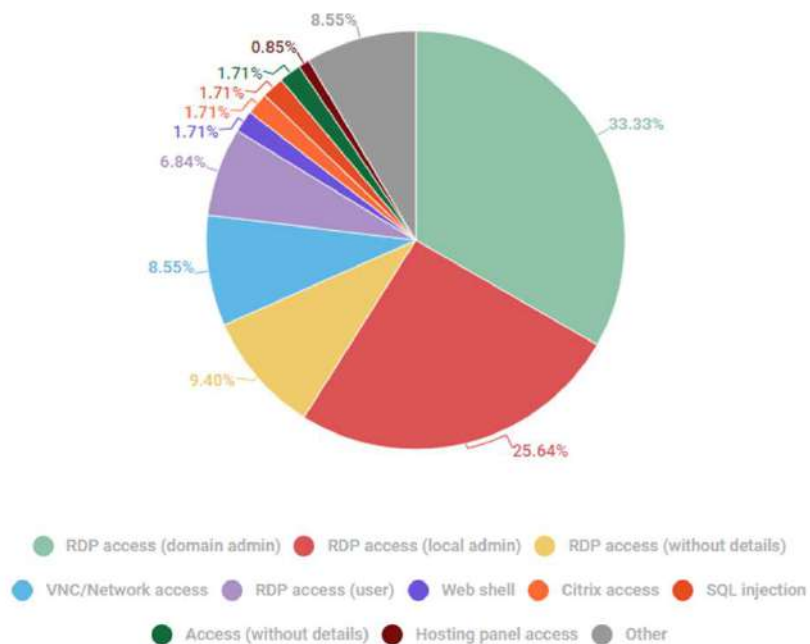


Figure 34. Top Asset varieties in breaches (n=2,667)

RDP Access compromises are hitting new heights

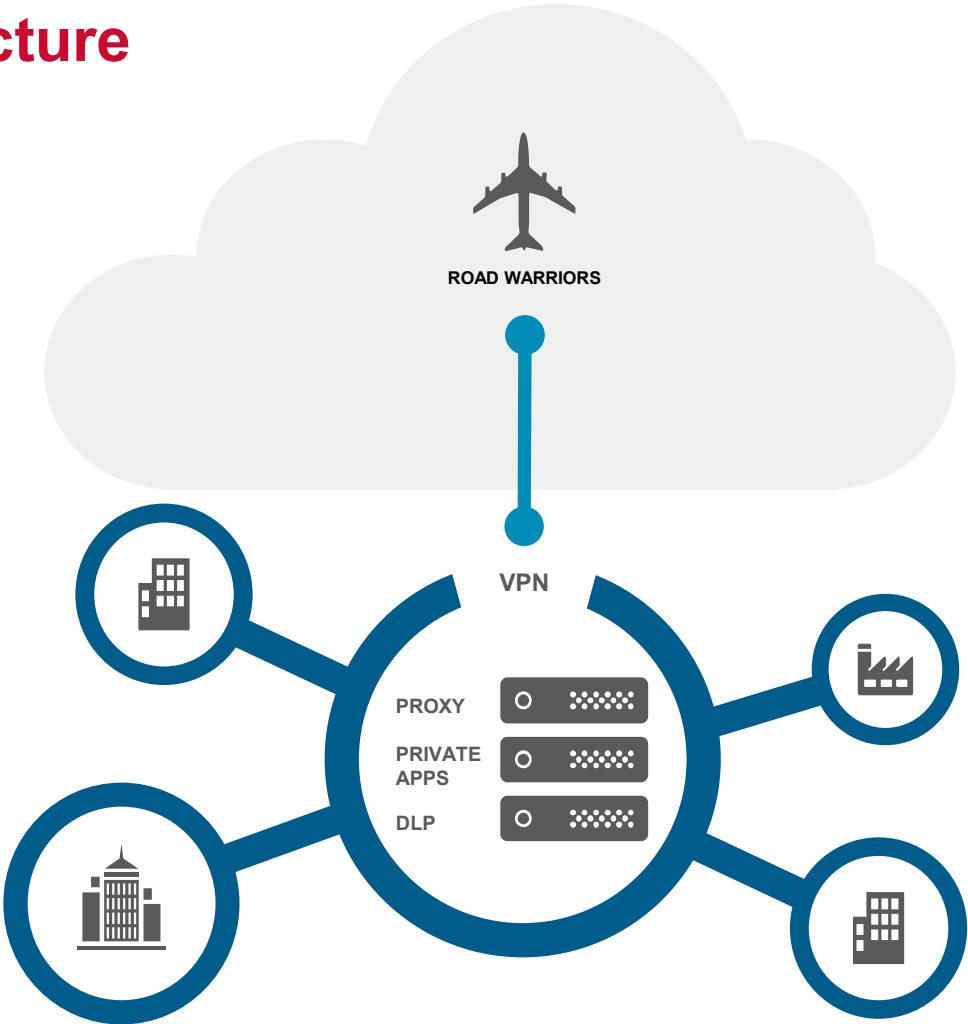
- Environments in the public cloud are mostly accessed directly through the internet
- 4,901,966 RDP servers publicly accessible (by Shodan.io)
- 23,158,423 SSH servers publicly accessible (by Shodan.io)
- Attackers get brute force access to those servers and sell the credentials to cyber criminals

If analyzed in terms of access type, most posts offer RDP access or a VPN + RDP bundle (75.21% of lots). In the diagram below both of these options belong to the categories "RDP access (without details)", "RDP access (local admin)", "RDP access (domain admin)" and "RDP access (user)".

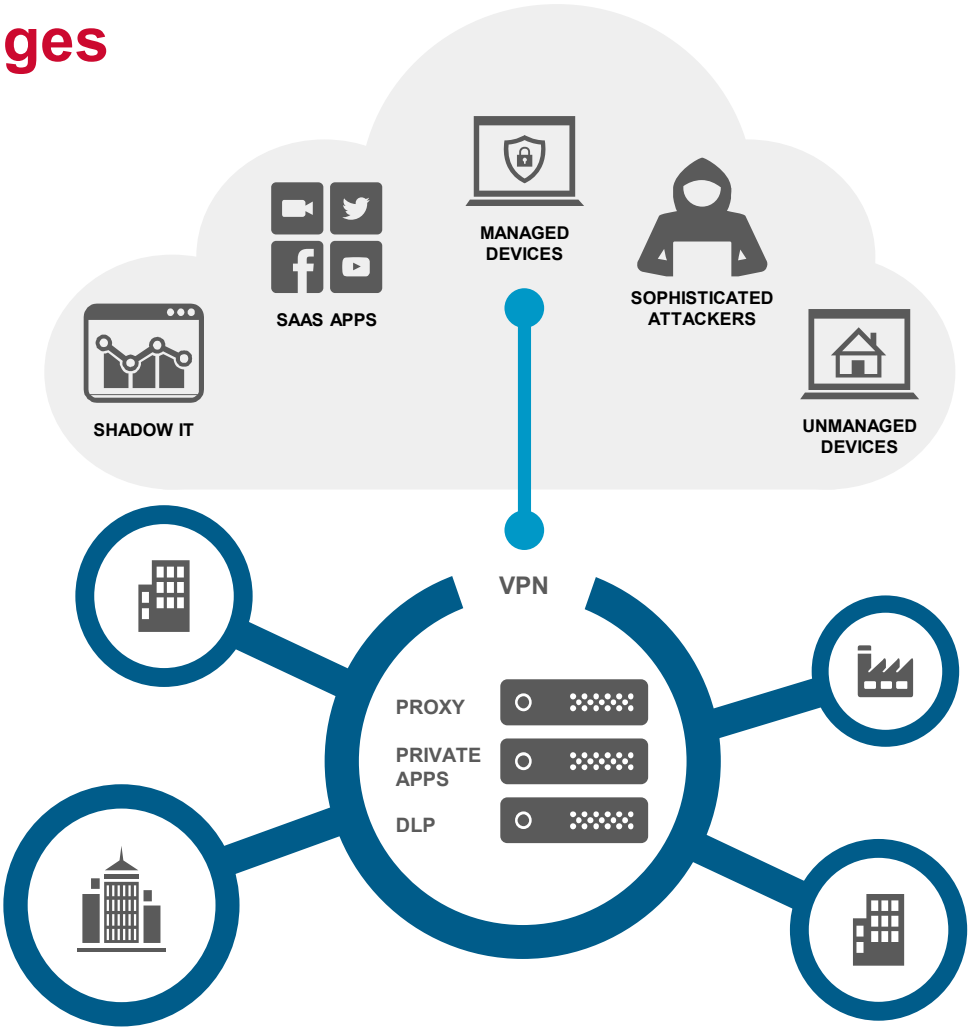


<https://securelist.com/initial-access-data-price-on-the-dark-web/106740/>

Legacy Architecture

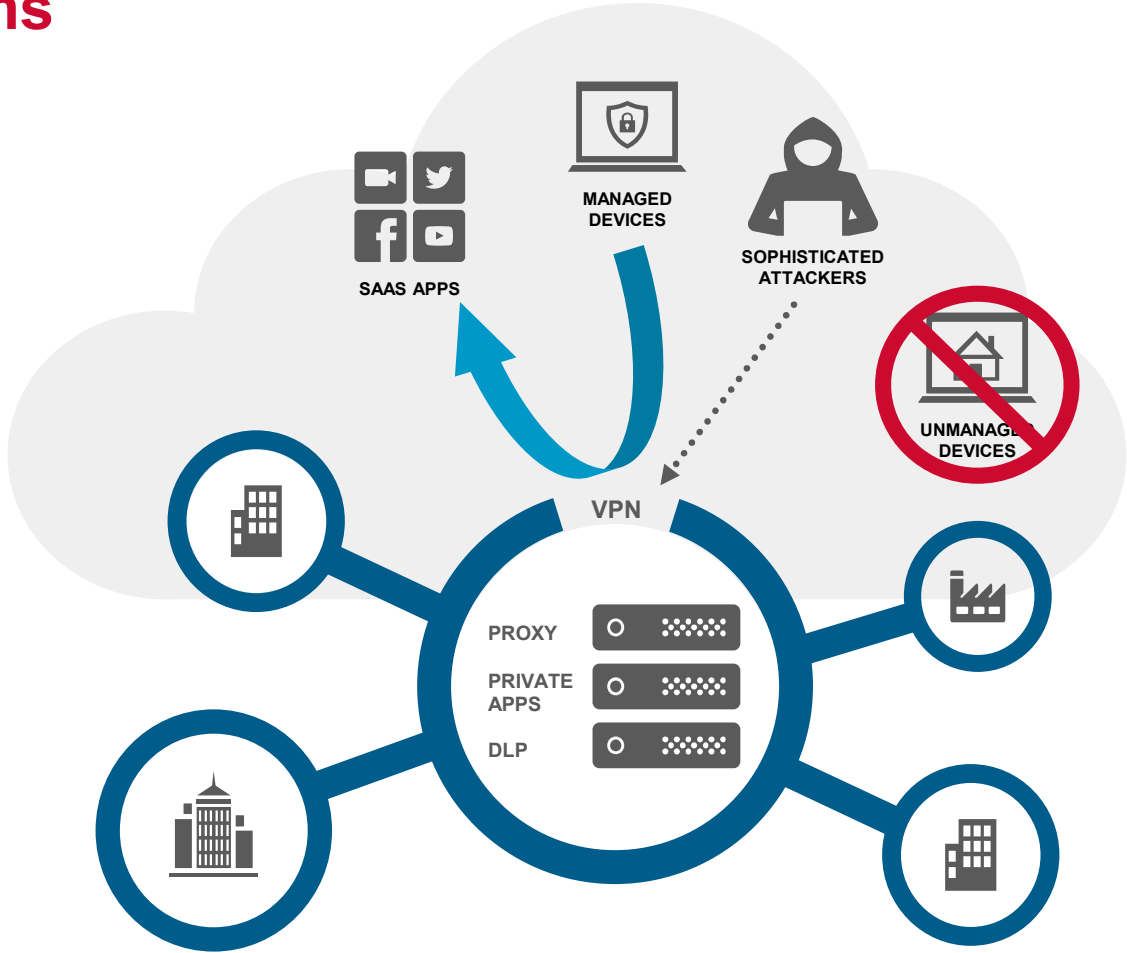


Modern Challenges



Corporate VPN Problems

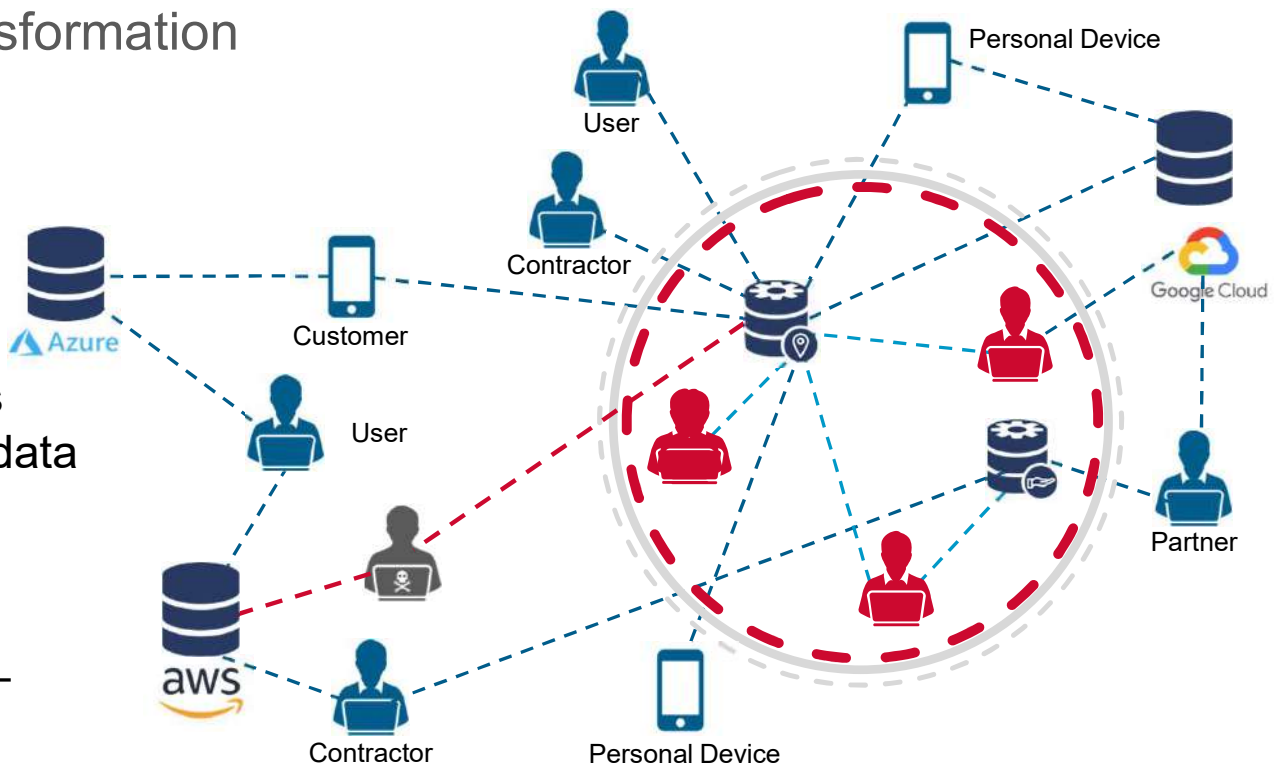
- Inefficient Traffic “Hairpin”
- Full Network Access
- Scalability
- Managed Devices Only
- Operational Cost



Modern IT Network—Application Centric

The Challenges of Digital Transformation

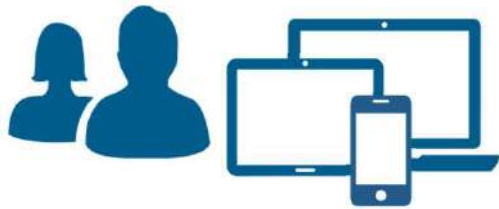
- Apps, data and employees have moved outside of the traditional network—there is no perimeter to defend
- Partners, contractors and others need access to corp. Apps and data
- Access needs to be limited/restricted
- Device types have proliferated—including BYOD



Applications left the walled garden....

Zero Trust is a Fundamental Shift in Security Approach

Based on “Never Trust, Always Verify” Principle



Verify Every User / Device



Enforce Least Privilege



Assume Breach

Zero Trust is a data-centric security model centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and must assume they will be breached. Organization must verify and validate every user, app, and device before granting access and enforce least privileged access to minimize exposure.

The role of Security in ZT - Fundamental Shift in Identity Security Approach

Any Identity



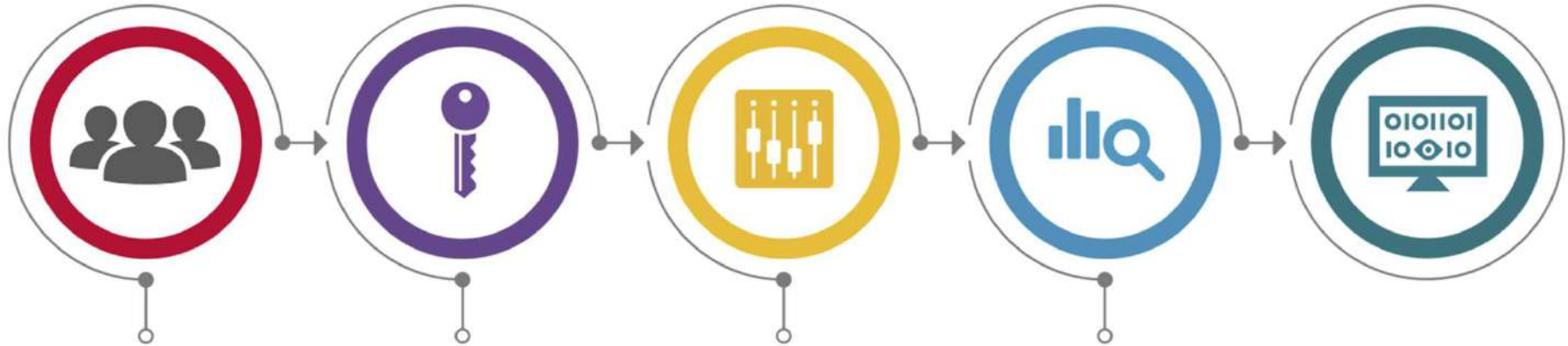
Any Device



Any App



Risk-aware, Continuous Policy & Session Management



1 **Positively identify** all users trying to access sensitive apps & data

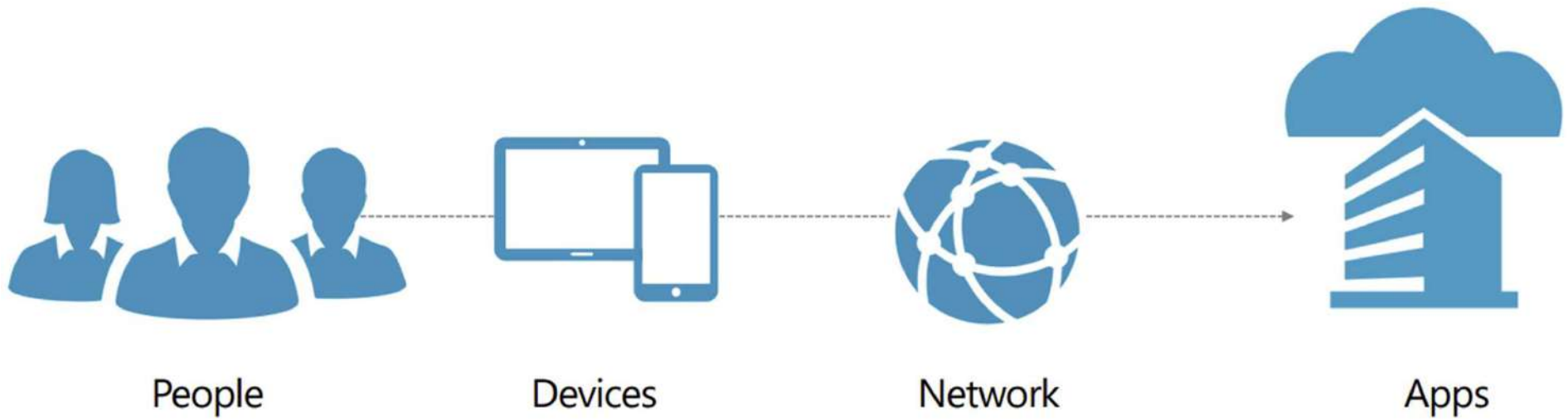
2 **Continuously authorize** access based on risk and data sensitivity

3 Automatically **adjust or block access** in real-time to mitigate attack damages

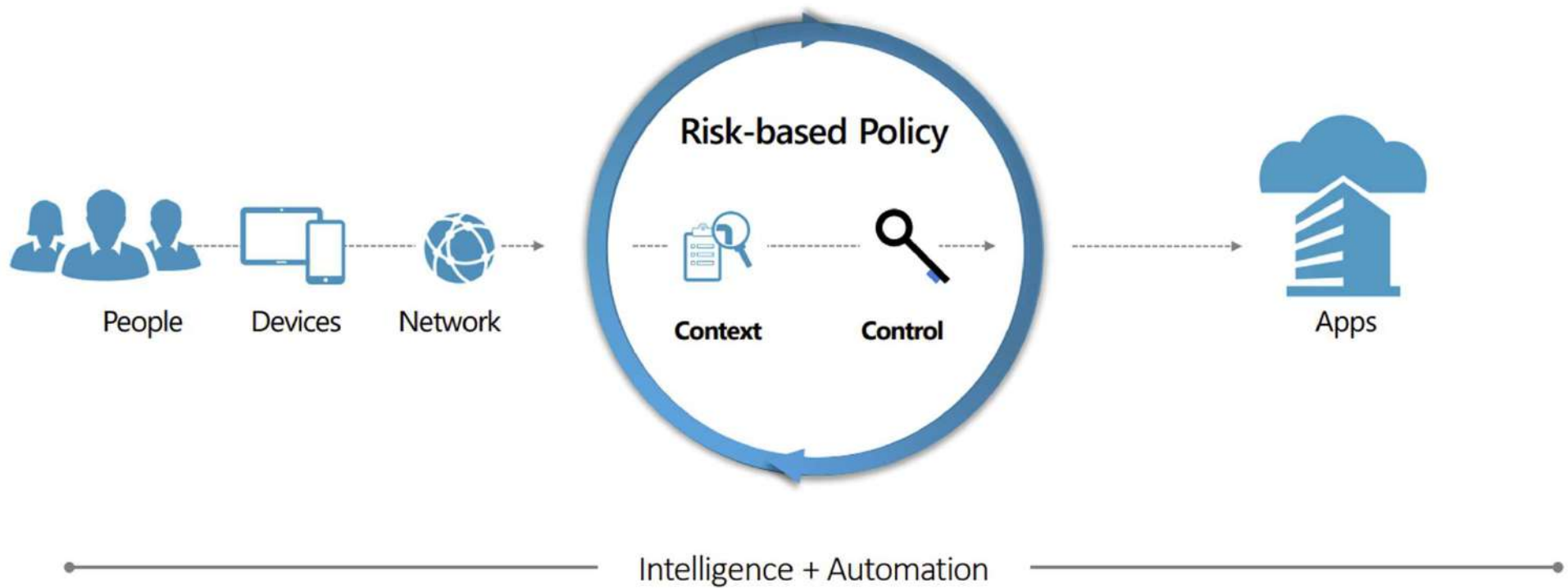
4 Protect & monitor **access to privileged accounts** to prevent data breaches

5 **Govern user access** to enforce least privileged model and reduce risk

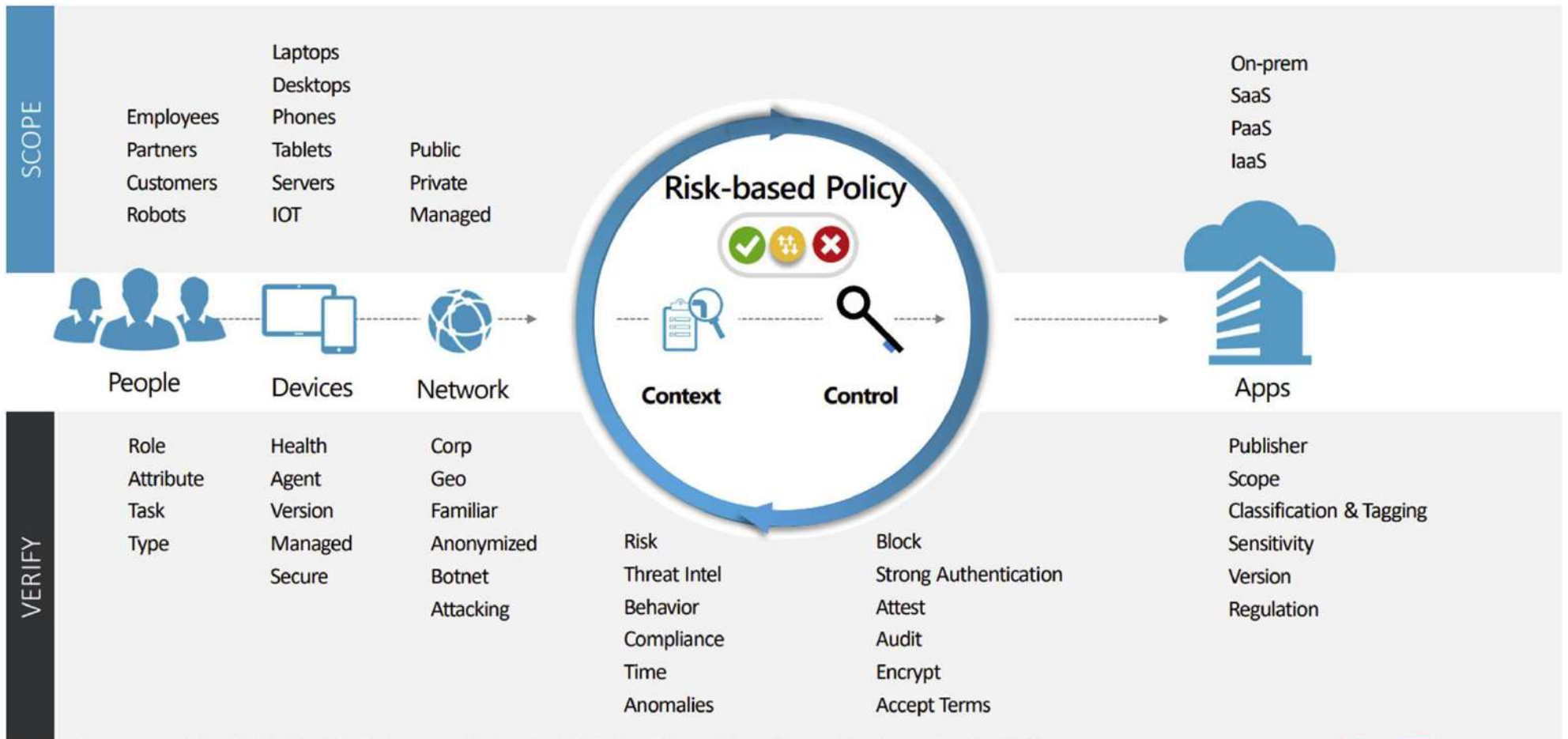
Zero Trust



Zero Trust



Zero Trust



Zero Trust

User tries to access an App

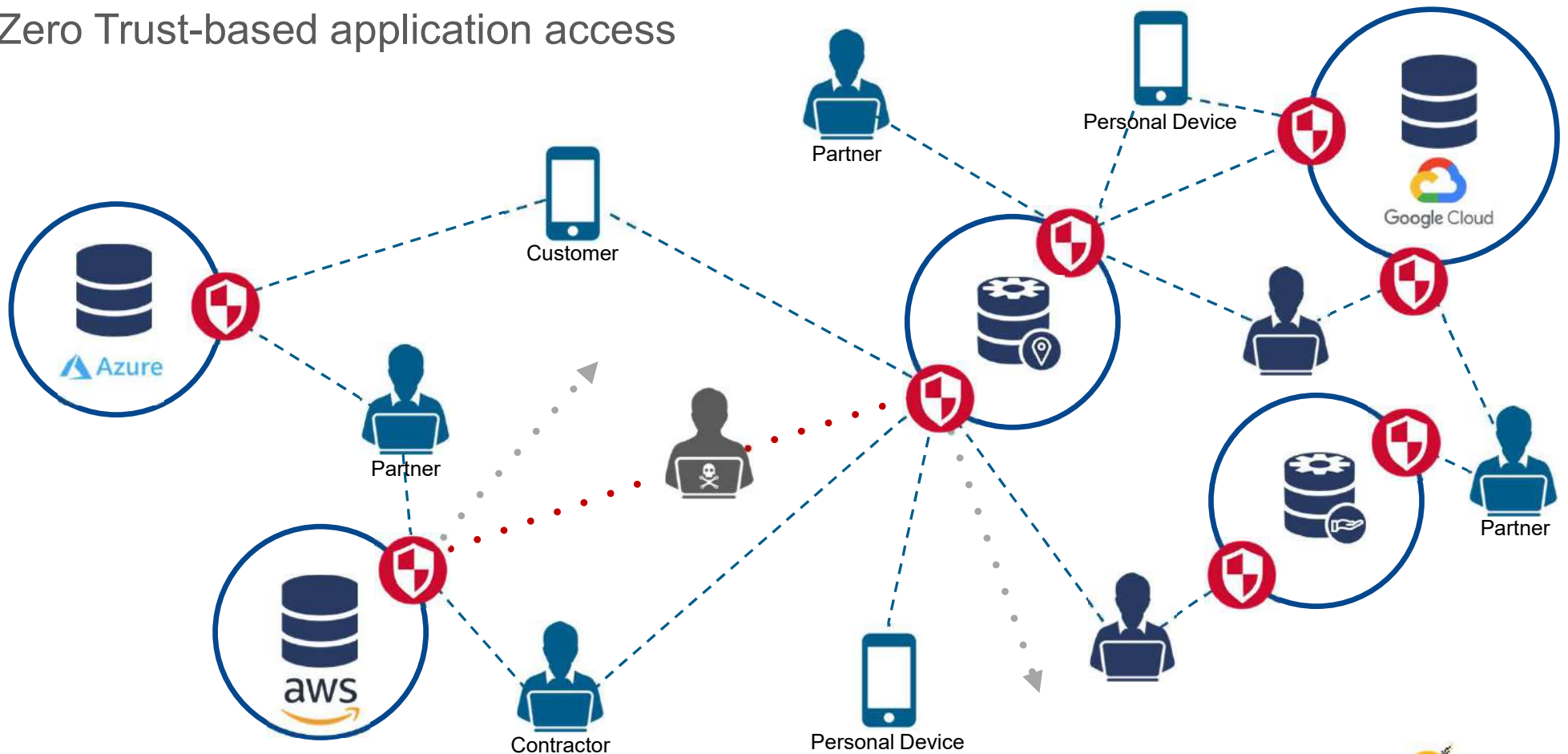


EXAMPLE

Employee	Healthy	Corporate	Usual behavior → Low Risk	Allow, Regular Passwordless Login	Corporate Portal
----------	---------	-----------	---------------------------	-----------------------------------	------------------

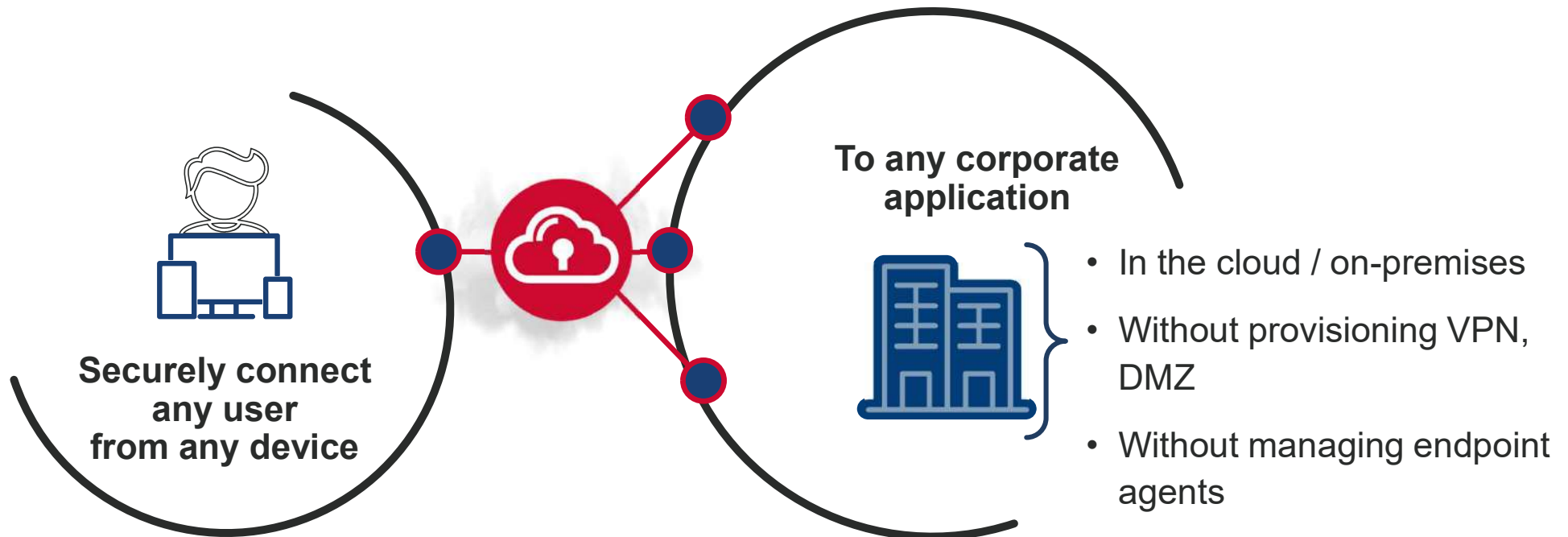
ZTNA Approach – Application-centric Security

Zero Trust-based application access



Zero Trust Network Access

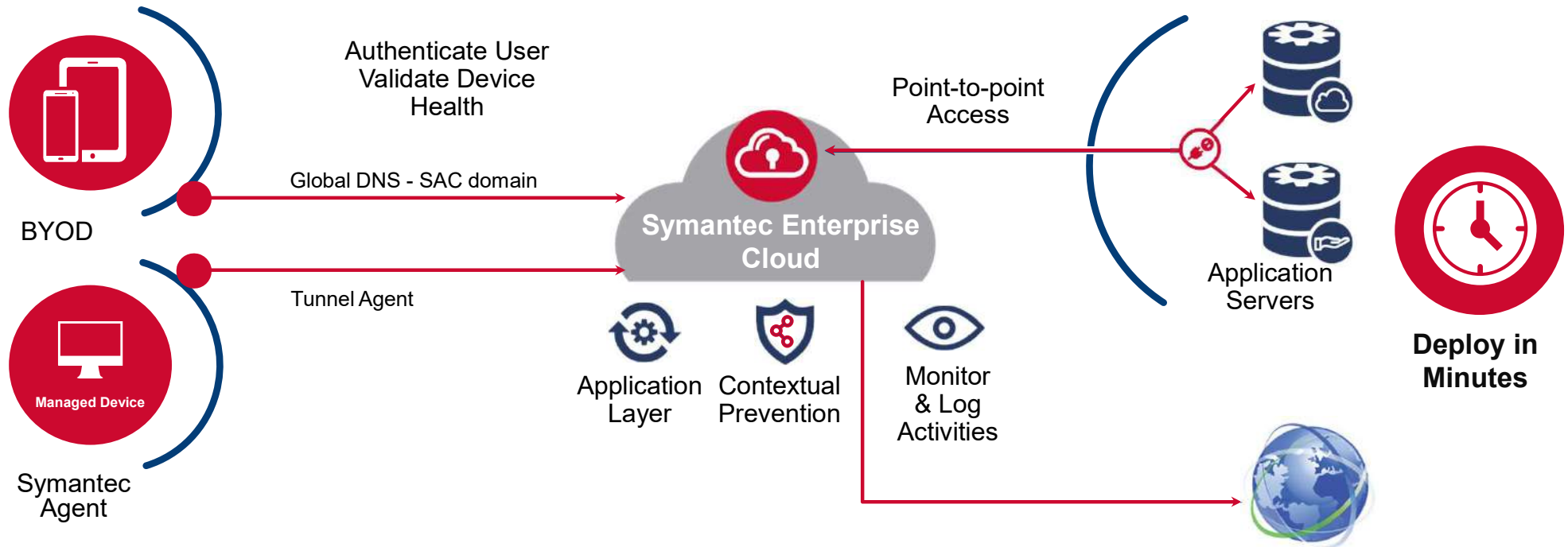
Secure Access Cloud



Zero Trust access: Trust is continuously verified, access is limited
Security category – Software Defined Perimeter (SDP)

How it works

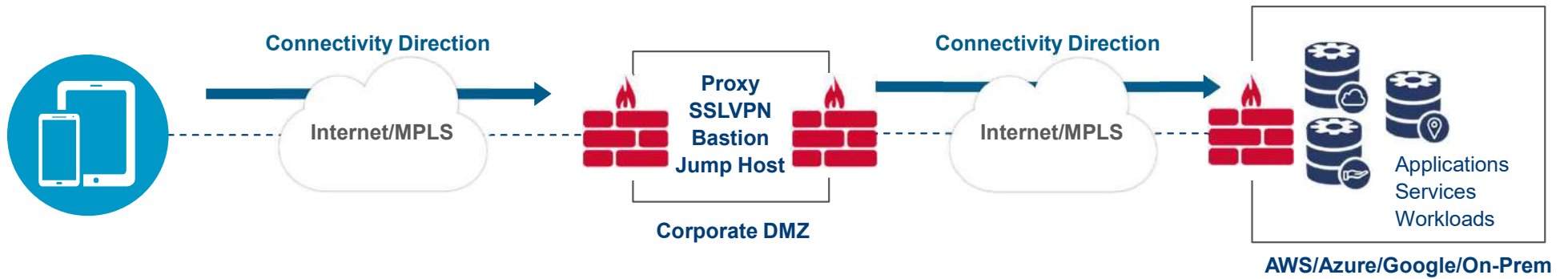
Zero Trust-based application access



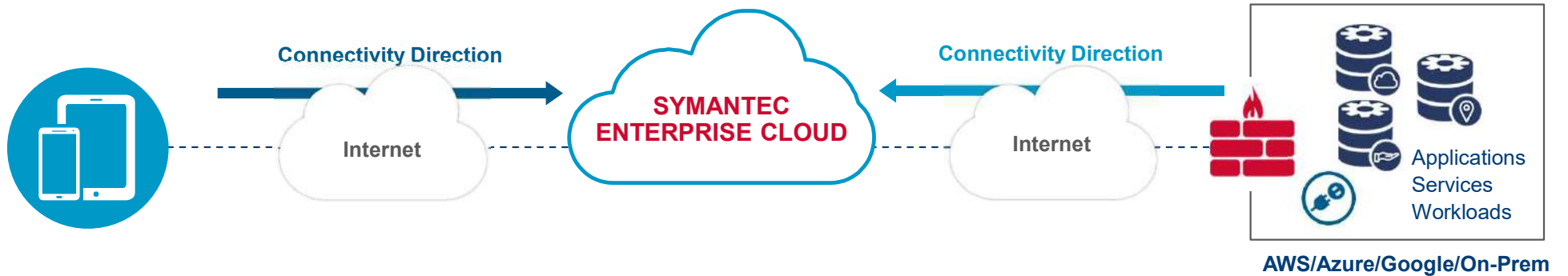
Anyone to anywhere – simple and secure app access

Cloud Alternative to Traditional Access Methods

Traditional DMZ—Connected via the Network

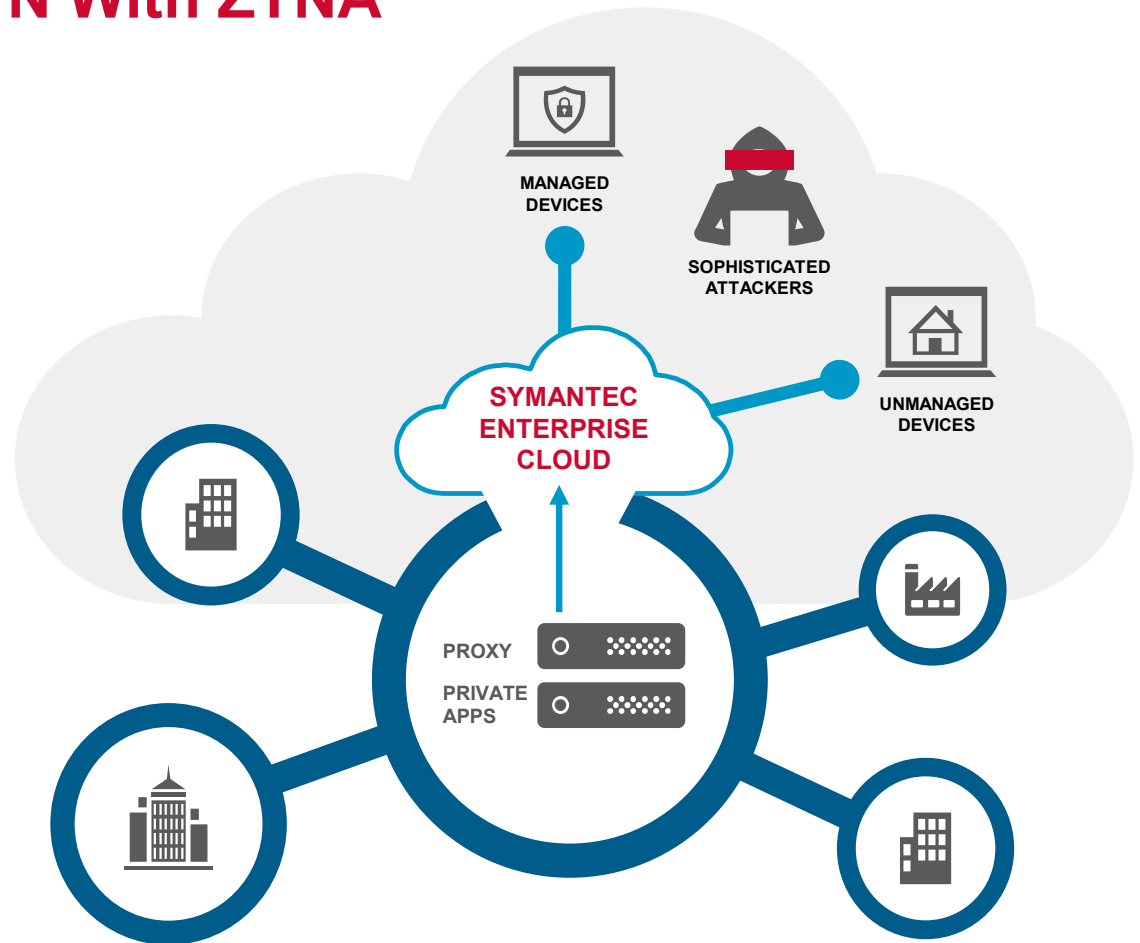


Symantec Secure Access Cloud—SDP-based Cloud Native Connectivity



Start Phasing Out Your VPN With ZTNA

- Agentless Access for Unmanaged Devices
- No Lateral Movement
- Full Audit
- Native DevOps access (SSH, RDP, TCP)
- Multi-cloud Capable



Why do companies adopt Zero Trust Network Access?

- Replace unsecure VPN network access with application-based access with conditional user and device validation and continuous monitoring.
 - Improves security, reducing risk
 - Lowers cost and complexity
- Secure access to public and private cloud environments, including automation where ZTNA access is part of the CI/CD pipeline.
 - Less time to provision (cloud) environments
- Enable users to use their private devices (BYOD) to securely access corporate applications.
 - Lowers cost
 - Faster onboarding for users



ZTNA Onboarding Challenges



Business impact



1 Cross-teams Heavy Lifting

Consolidating the network policies which has been by managed on application side by application owners takes effort and time - users are used to having access to all applications on the network and application owners deciding who is provisioned - ZTNA changes this paradigm

2 User's impact

Users love to have the best experience as possible: lowest latency regardless of the user location, minimal number of client tools, keep the domain space consistent

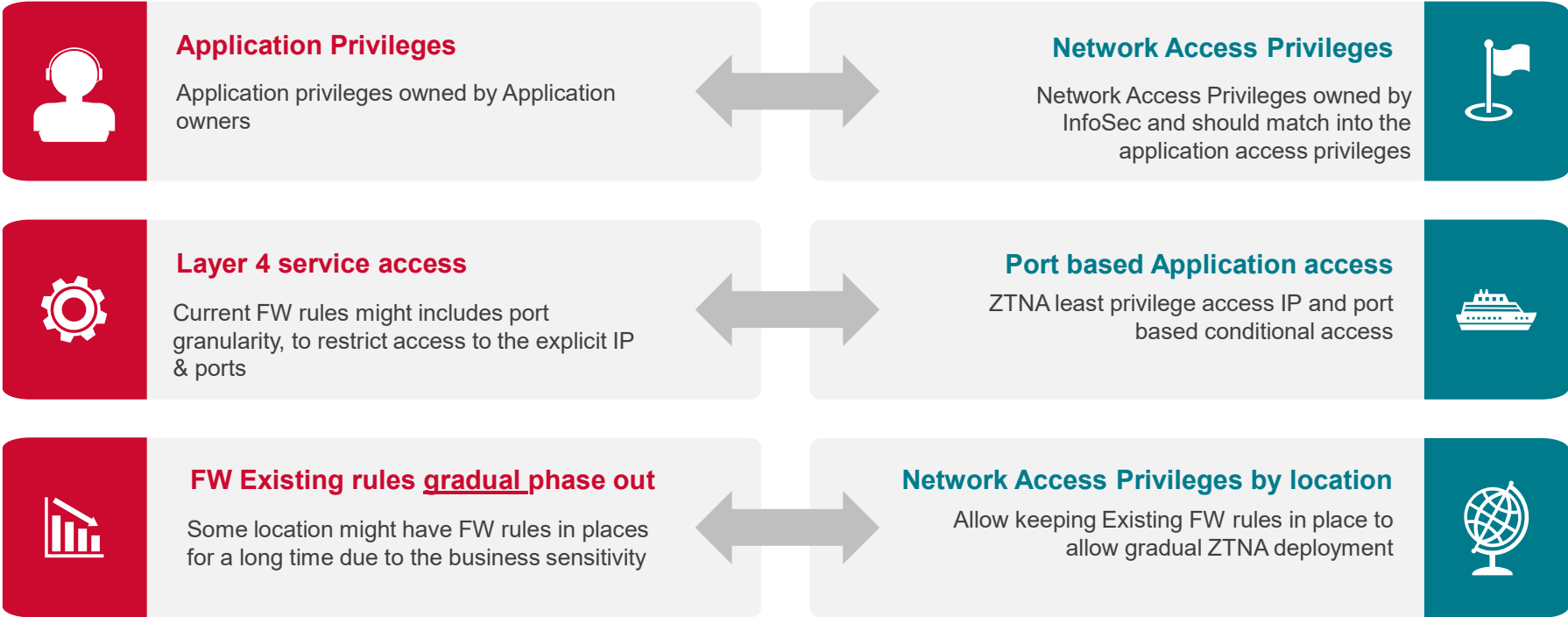
3 SecOps impact

When it comes to the product maintenance, teams are struggling to handle a lot of daily operations related to the provisioning/deprovisioning for the resources or access privileges

4 Compatibility impact

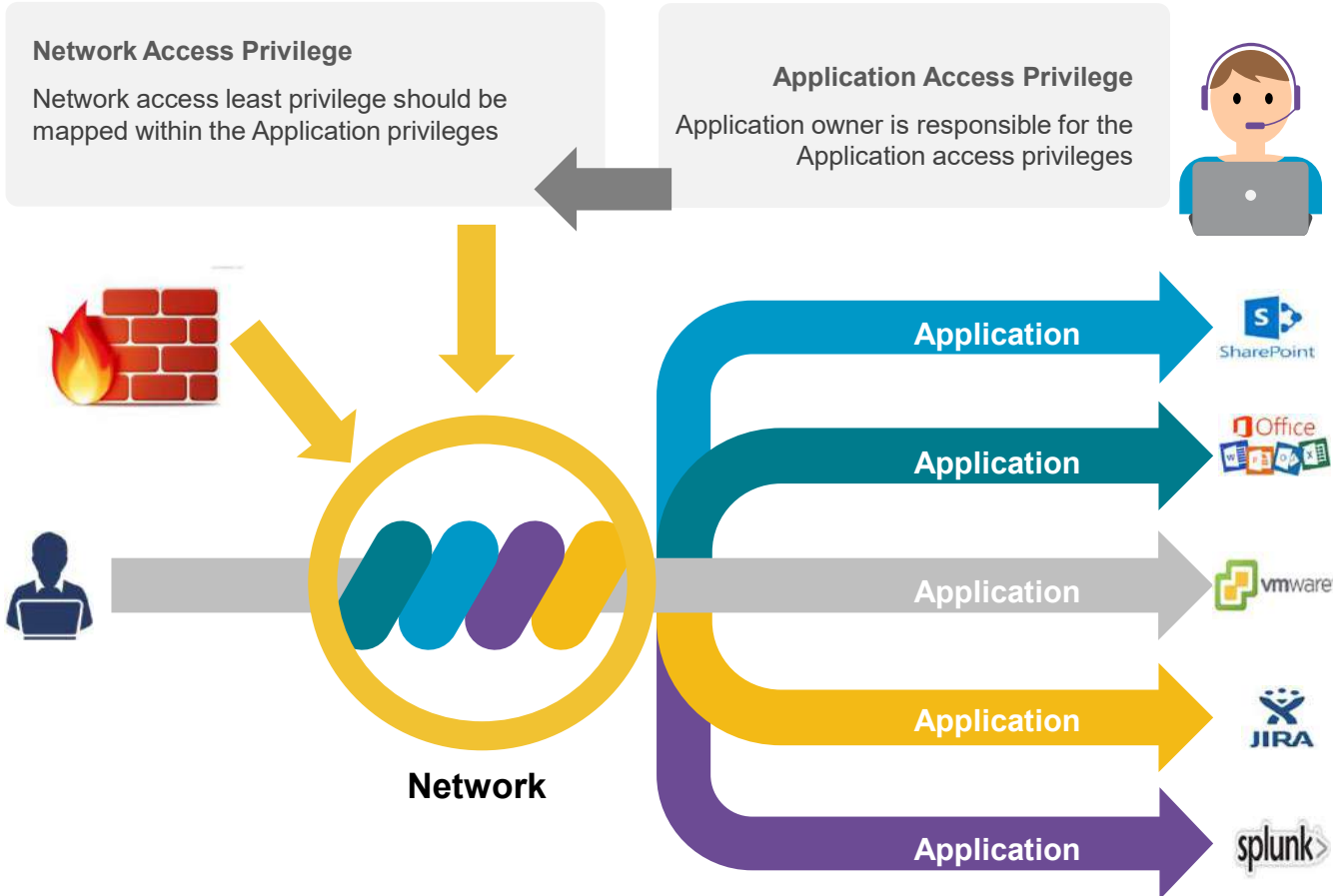
Replacing VPN with ZTNA solution might introduce the compatibility challenge, conflicting with different agents for traffic steering and device compliance solutions

Network Onboarding challenges



Heavy Lifting Onboarding (visualizing)

- Big effort
- Long project lead times
- High cost (pay twice)



How we solve it

- We take it all ! - All network provisioned at once with few app and single policy
- Apply network policies gradually at any time without relying on the network team.
- No user impact
- Coexist with agentless access (due to the alternative data path)



The screenshot shows a configuration page for an application named "ASH Segmentation Test". The "APPLICATION NAME" field is at the top. Below it, the "CONNECTION SETTINGS" section includes a "TARGET ADDRESS" field with the value "10.85.0.0/16" and a red arrow pointing to it. The "SITE" dropdown is set to "GTO-ASH-DMZ-Prev" with a "View Site" link.

The screenshot shows a "TARGET PORTS" configuration dialog. It has a search bar and "Edit as Text" and "New" buttons. The "TARGET PORTS (1)" field contains "e.g. 8080 or 3389-3390" with a red arrow pointing to it. Below the dialog, a list shows "TARGET PORT" with "Target Ports (1) 3389".

Have Symantec Agent? You're done!



1 Zero Touch Provisioning (ZTP)

Migration process from the legacy solution to SAC requires **no** IP or domain name changes and can be accomplished in a hours

2 Side by Side Coexistence

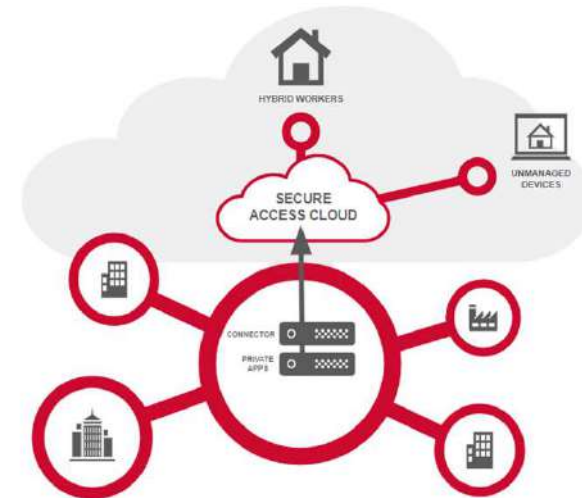
Symantec solution live side by side with the VPN, to avoid business impact through the migration process

3 Network Policy Construction with no Business Impact

Conditional access for explicit applications has no business impact or application changes

4 Keep Your User Experience the Same

Following Symantec agent deployment on user's machine, user keep his UX with no changes



SecOps Impact - RBAC

Sites > Edit Site
 Prod BCP Site 1 ● Online

Configuration

Published Applications (14)

Assigned Roles

<input type="checkbox"/>	NAME ↑	USERNAME	ENTITY TYPE	ROLE
<input type="checkbox"/>	Curious Subscriber	letmesee@stasdemoprod.luminatesec.com	Local User	Site Connector Deployer
<input type="checkbox"/>	Greg Thomas	gregt@stasdemoprod.luminatesec.com	Local User	Site Editor
<input type="checkbox"/>	Stanislav Elenkrich You	stanislav.elenkrich@broadcom.com	Okta User	Site Connector Deployer

1 - 3 of 3

Symantec Dashboard Sites **Collections** Applications Policies Logs Settings

Collections

Search Application Policy New

COLLECTION	RESOURCES	LINKED SITES
collection1	2 Resources	2 Linked Sites
collection2	2 Resources	2 Linked Sites 🗑️
collection3	2 Resources	No Linked Sites Applications cannot be created

1 - 3 of 3



SecOps Challenges - Automation

Automate everything !



Full API control



Terraform Support



Slack Integration



RBAC



APPLICATIONS

- 
Home - Workstation
- 
Symc.site - ITMS
- 
Symc site ITMS v2
- 
Symc site ITMS v3
- 
Symc.site - ITMS Web
- 
Symc.site - server

1 - 6 of 6  

Forensics Audit

Nov 14, 2023, 10:30 - Nov 15, 2023, 10:30

24h

× Request ID

× Entity

× Application

App Type ▾

Event Type ▾

Result ▾

× Internal addi

× HTTP Status

× Event



DATE ↓	ENTITY	APPLICATION	TYPE	EVENT TYPE	RESULT	EVENT
▶ Nov 15, 2023, 10:23:14	Dubravko.Hlede@symc.site	Symc.site - ITMS Web	Web	Activity	Success	URI Access (GET returned 403): /favic...
▶ Nov 15, 2023, 10:23:14	Dubravko.Hlede@symc.site	Symc.site - ITMS Web	Web	Activity	Success	URI Access (GET returned 403): /
▶ Nov 15, 2023, 10:22:31	Dubravko.Hlede@symc.site	Symc.site - ITMS Web	Web	Activity	Success	URI Access (GET returned 403): /
▶ Nov 15, 2023, 10:22:31	Dubravko.Hlede@symc.site	Symc.site - ITMS Web	Web	Activity	Success	URI Access (GET returned 403): /favic...
▶ Nov 15, 2023, 10:22:31	Dubravko.Hlede@symc.site	Symc.site - ITMS Web	Web	Access	Success	Accessing Web application: 'Symc.sit...
▶ Nov 15, 2023, 10:22:26	Dubravko.Hlede@symc.site	Application Portal	Web	Access	Success	Accessing application portal

1 - 6 of 6 |< >



Net++
TECHNOLOGY

NE VERUJ NIKOME 2023

HVALA NA PAŽNJI

Email: office@netpp.rs

Telefon: +381 11 3699 967

