Net++ TECHNOLOGY

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.

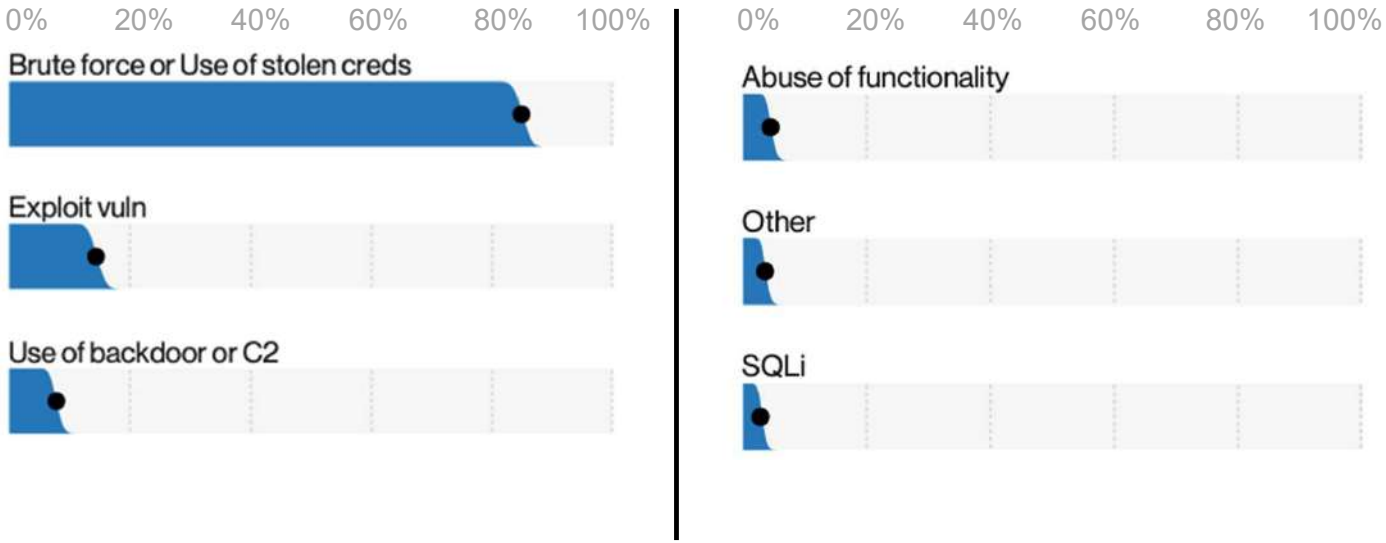


Figure20. Top Hacking varieties in breaches (n = 868)

Symantec by Broadcom

Compromised Devices

40% of breaches involved compromised web application servers.

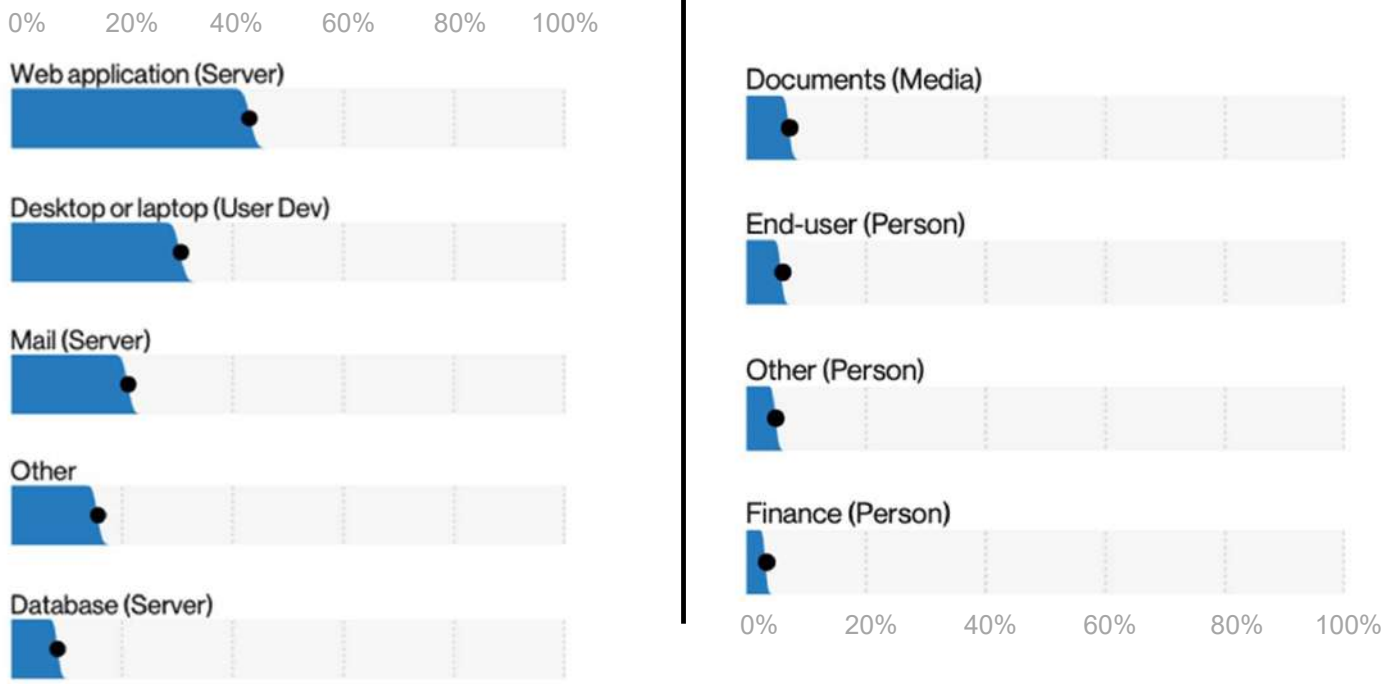


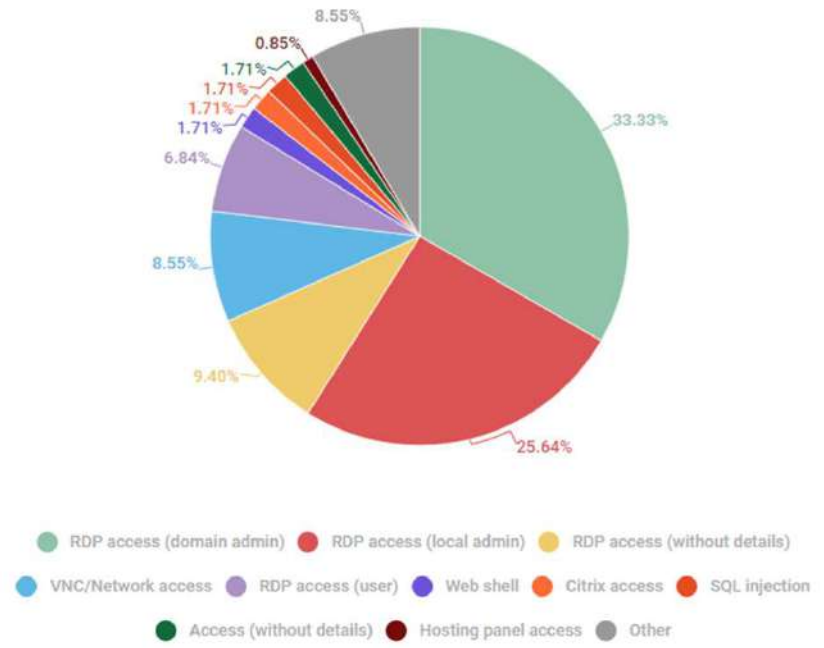
Figure 34. Top Asset varieties in breaches (n=2,667)

Symantec by Broadcom

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

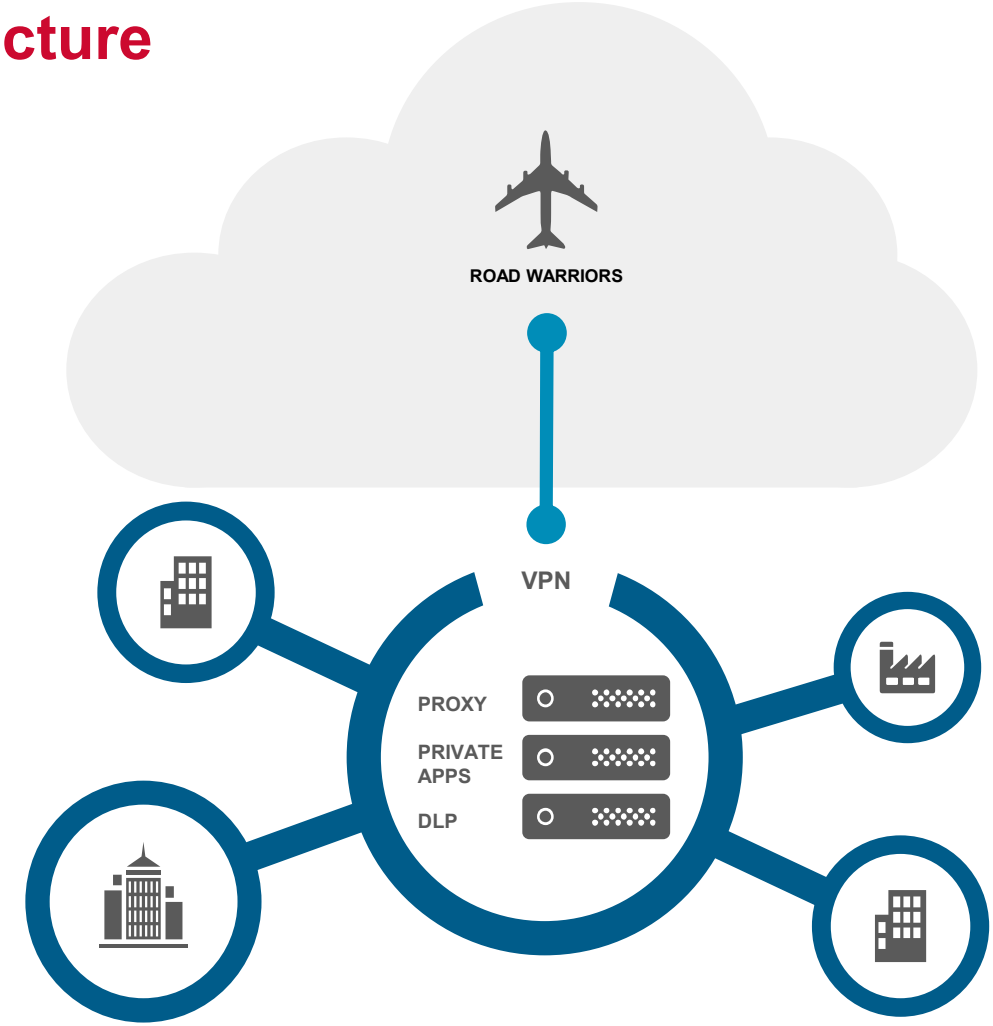
If analyzed in terms of access type, most posts offer RDP access or a VPN + RDP bundle (75.21% of lots). In the diagram below both of these options belong to the categories "RDP access (without details)", "RDP access (local admin)", "RDP access (domain admin)" and "RDP access (user)".



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

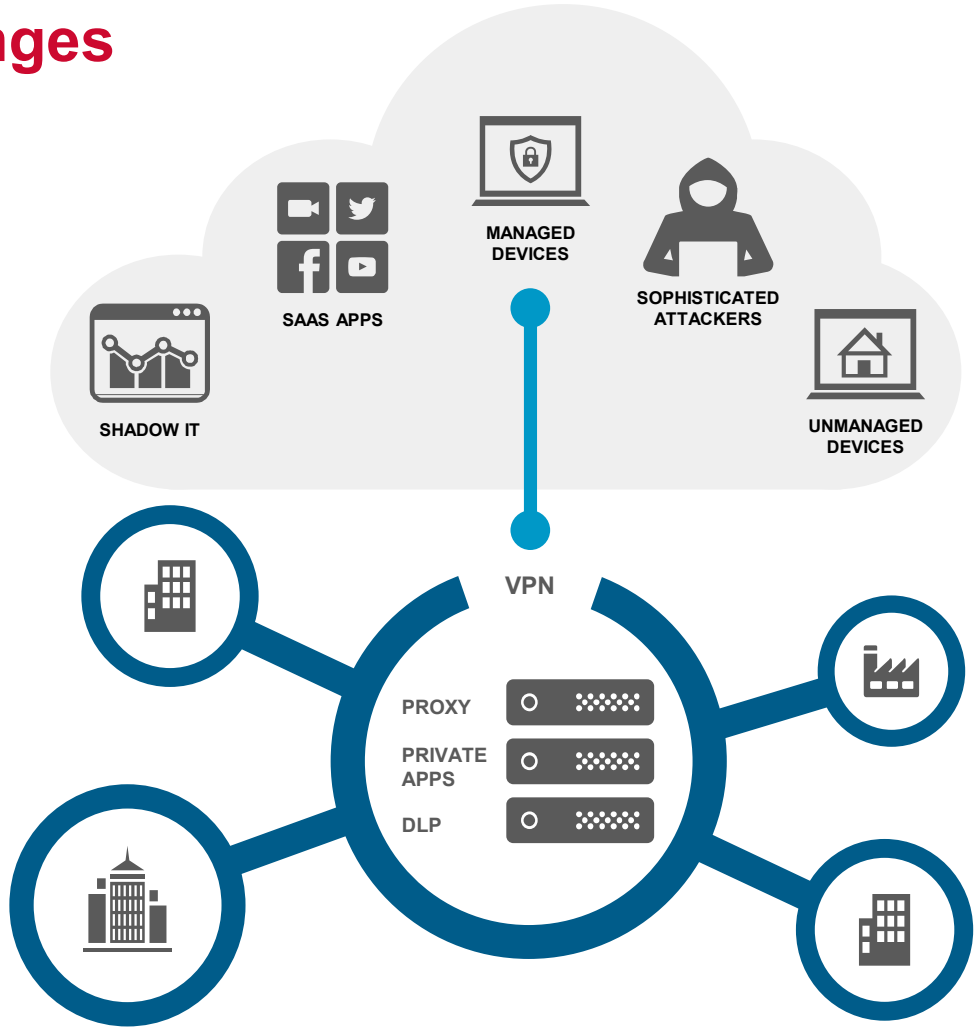
Symantec by Broadcom

Legacy Architecture



Symantec by Broadcom

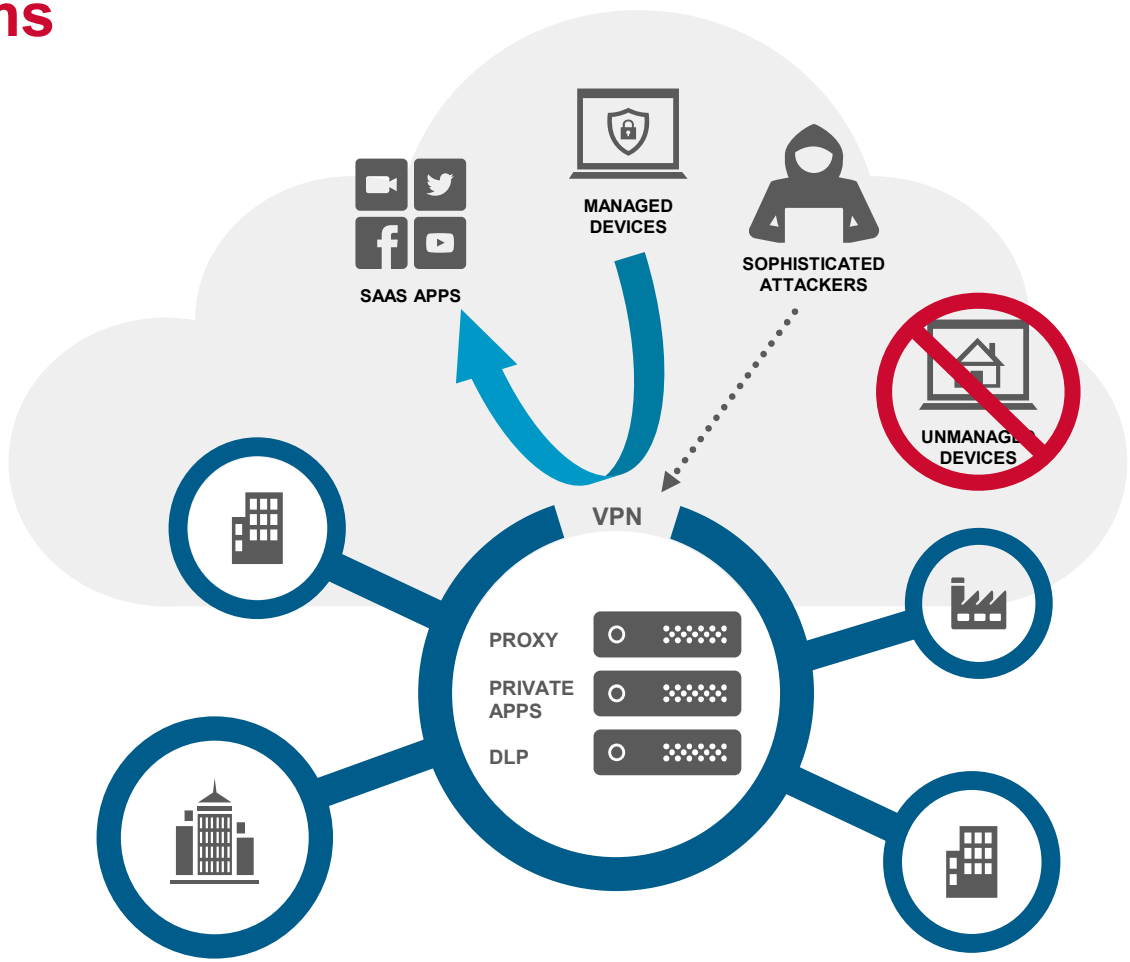
Modern Challenges



Symantec by Broadcom

Corporate VPN Problems

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

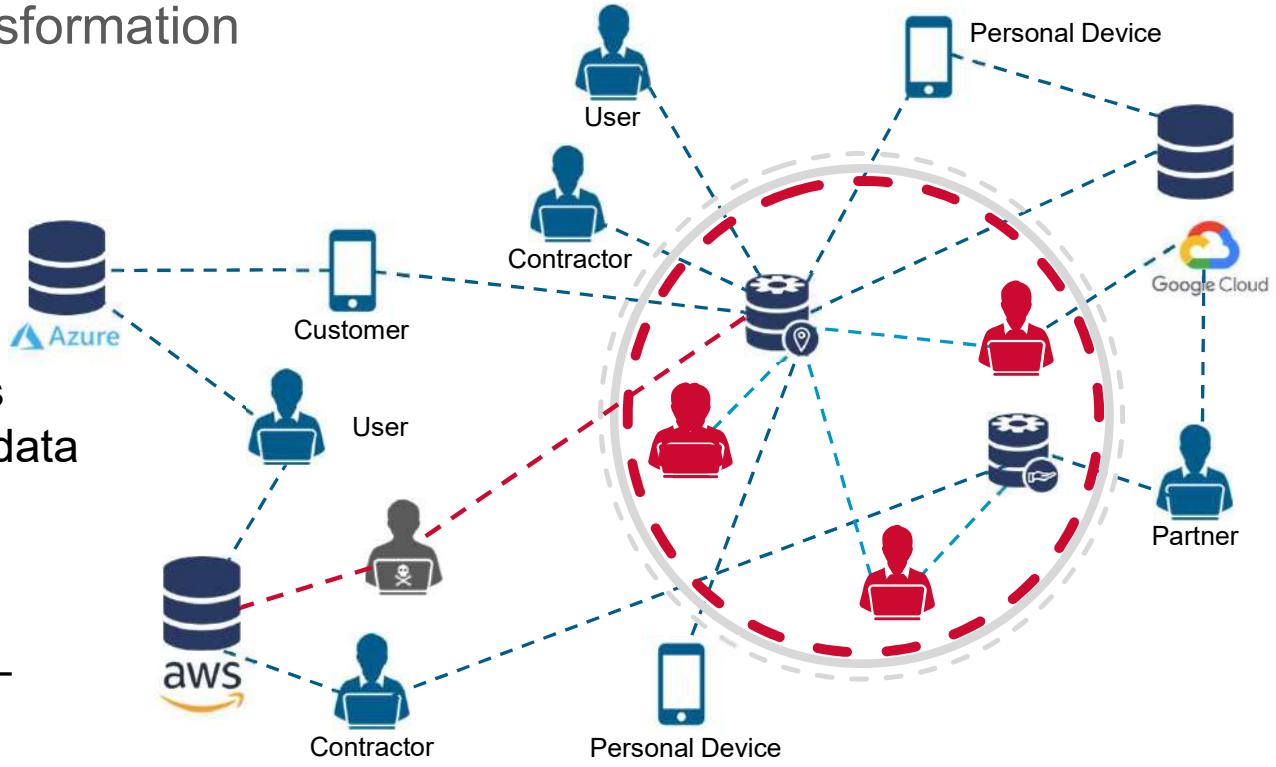


Symantec by Broadcom

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

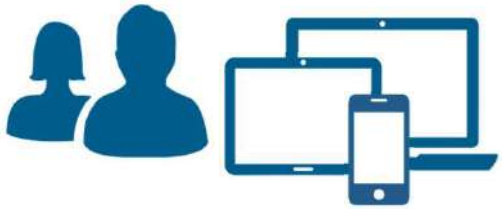


Applications left the walled garden….

Symantec by Broadcom

Zero Trust is a Fundamental Shift in Security Approach

Based on “Never Trust, Always Verify” Principle



Verify Every User / Device

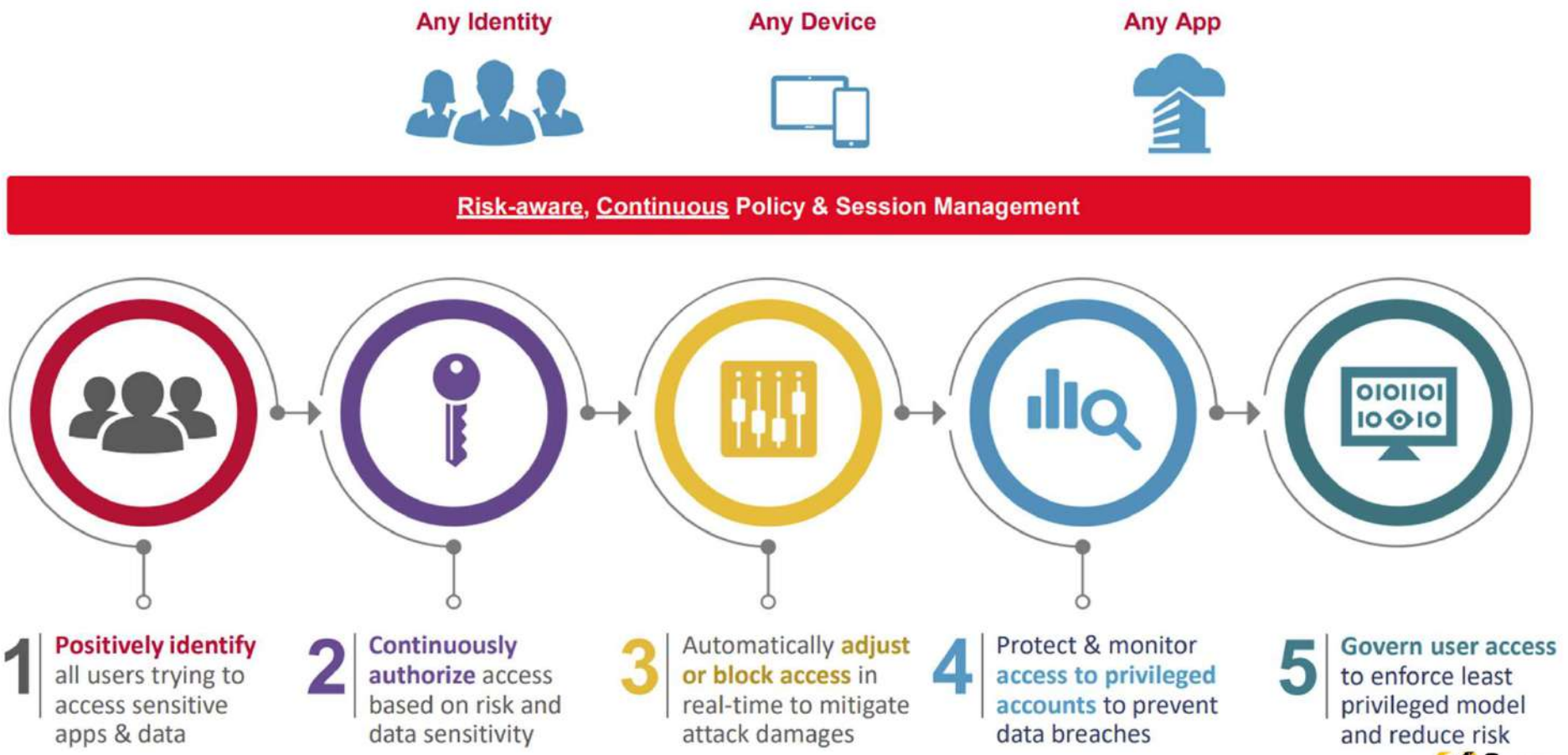
Enforce Least Privilege

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.

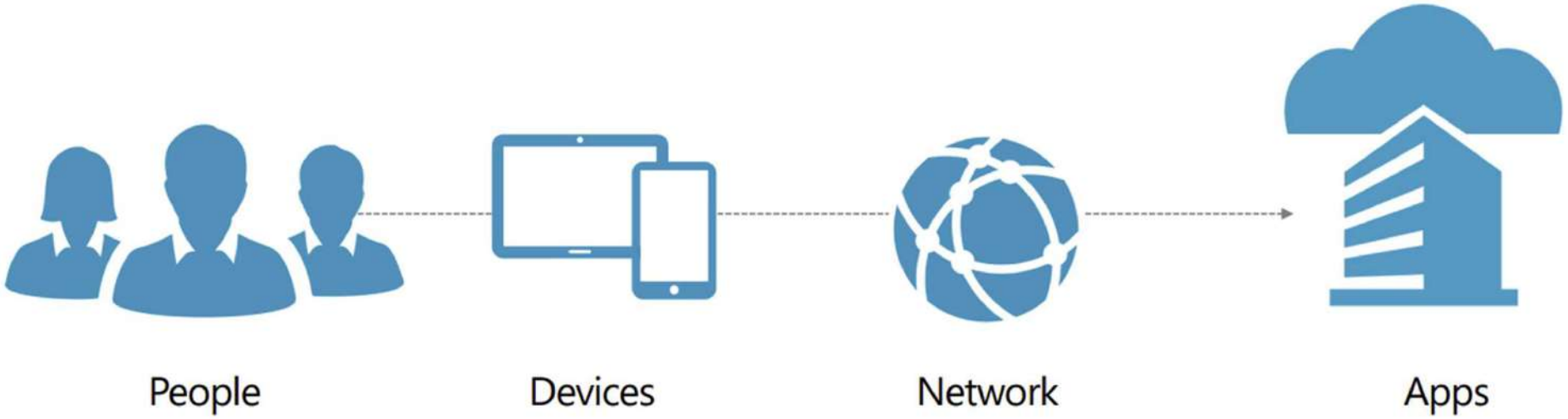
Symantec by Broadcom

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



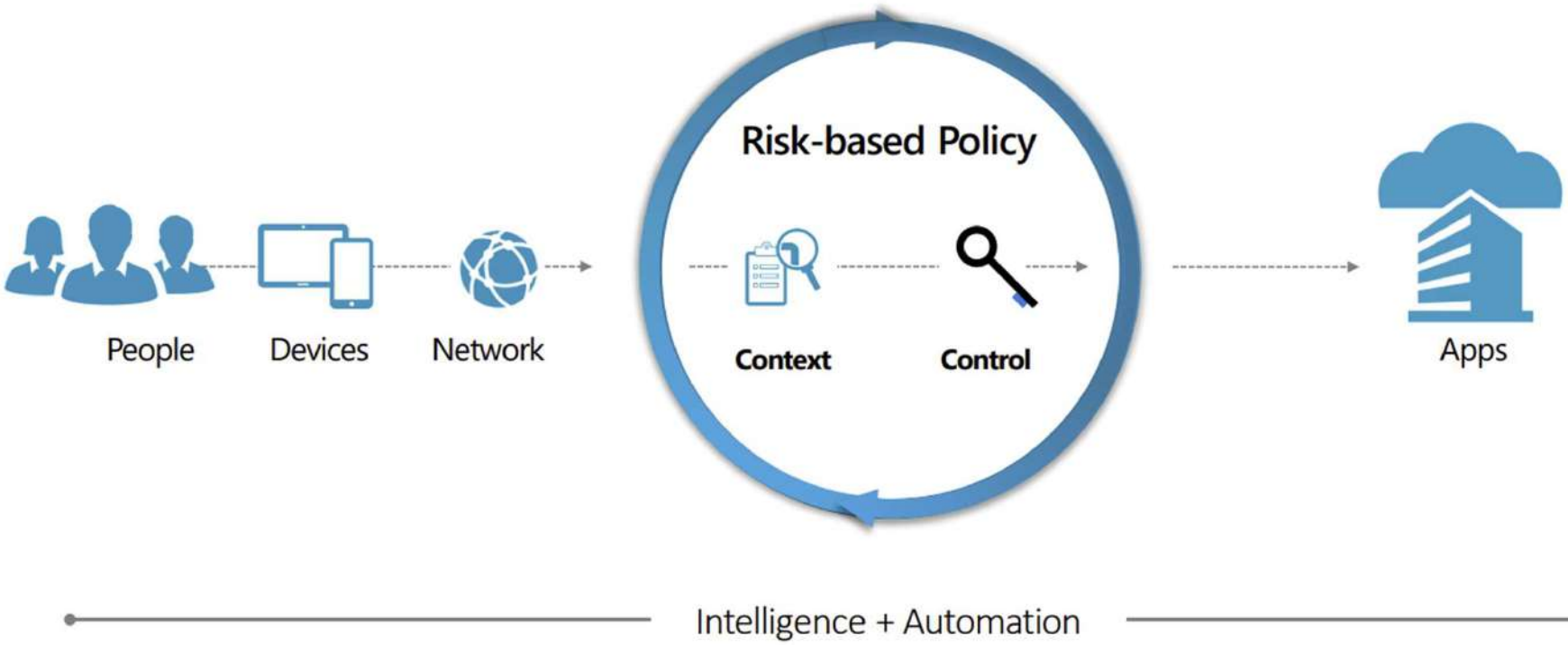
Symantec by Broadcom

Zero Trust



Symantec by Broadcom

Zero Trust

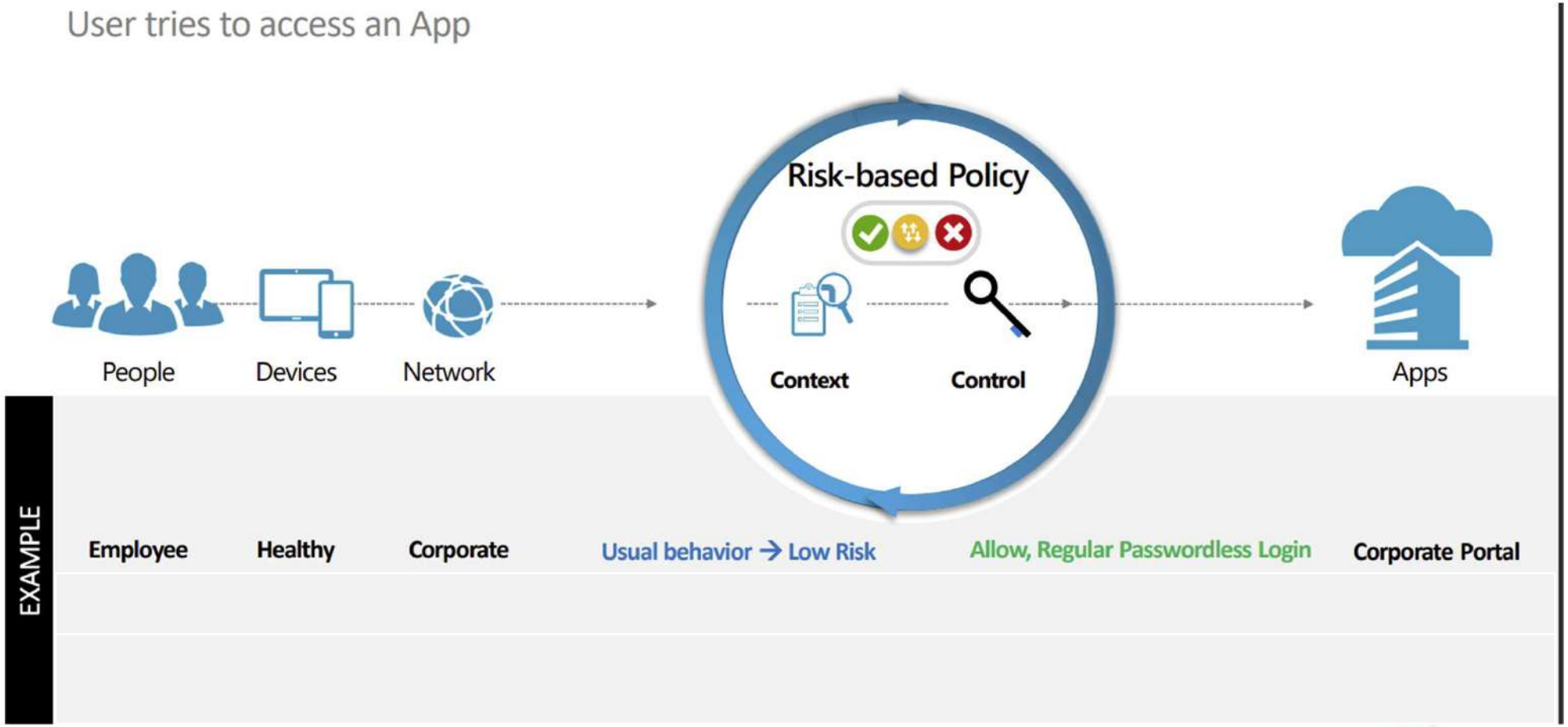


Symantec by Broadcom

Zero Trust

Symantec by Broadcom

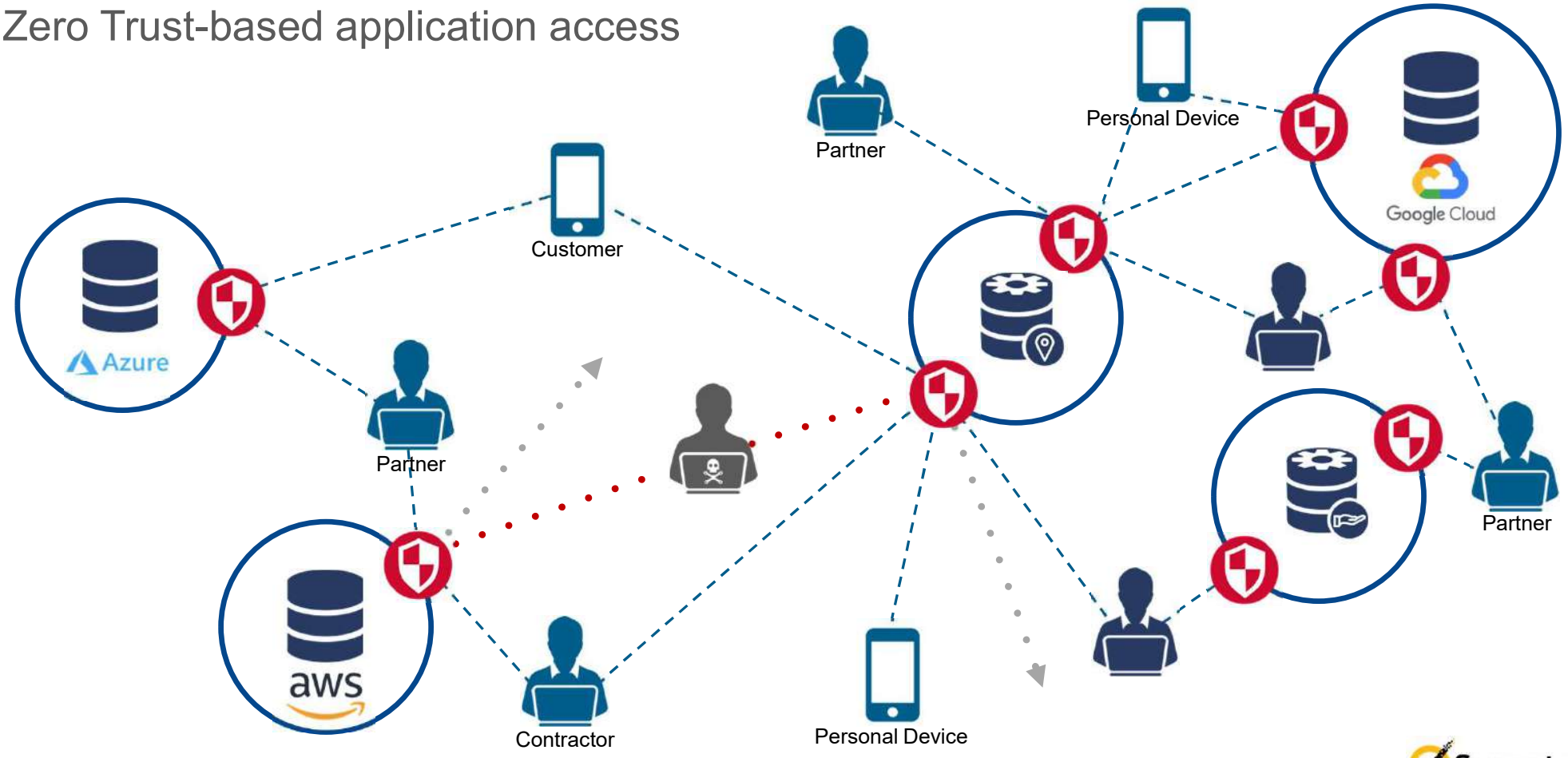
Zero Trust



Symantec by Broadcom

ZTNA Approach – Application-centric Security

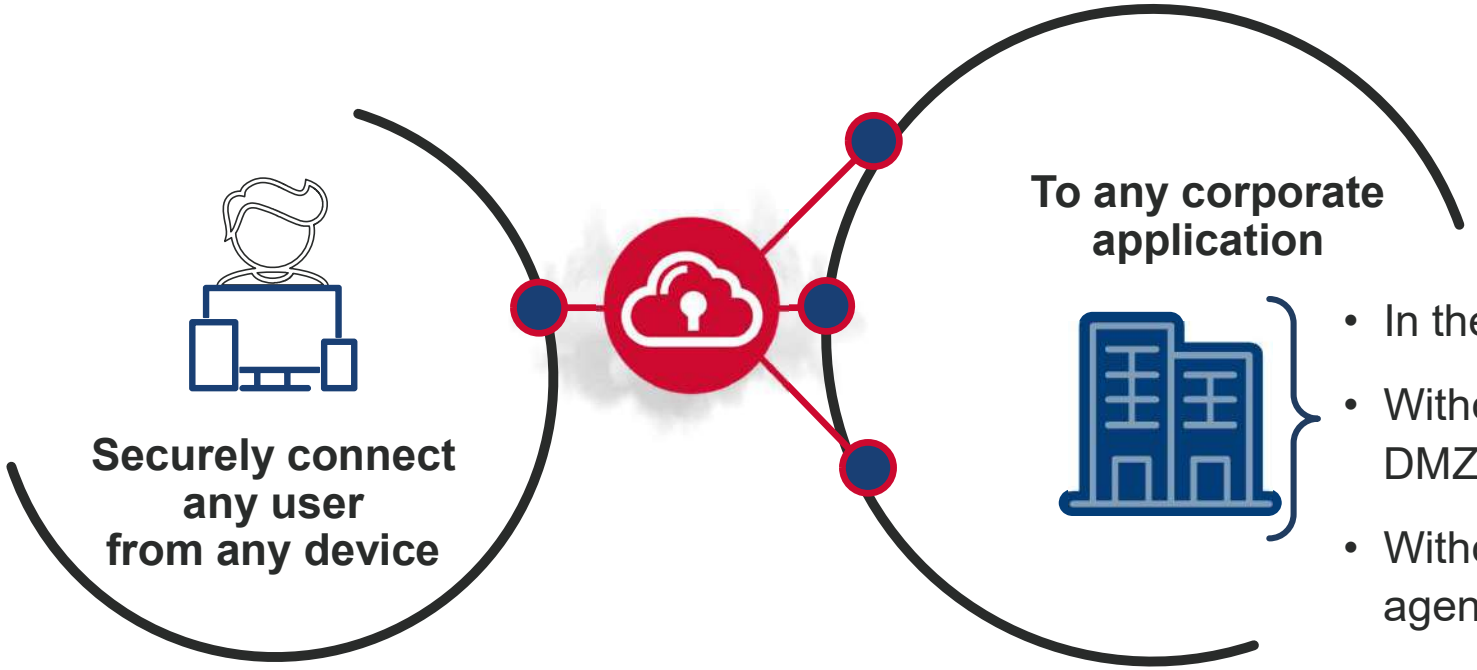
Zero Trust-based application access



Symantec by Broadcom

Zero Trust Network Access

Secure Access Cloud



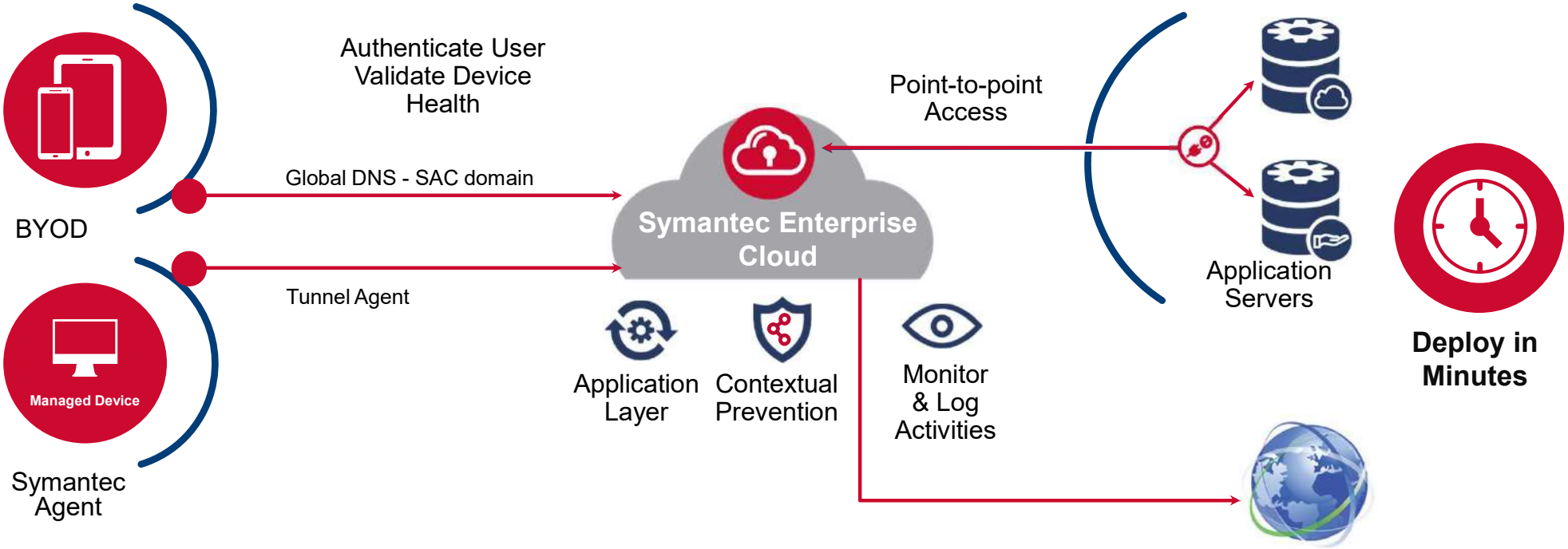
- In the cloud / on-premises
- Without provisioning VPN, DMZ
- Without managing endpoint agents

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

Symantec by Broadcom

How it works

Zero Trust-based application access

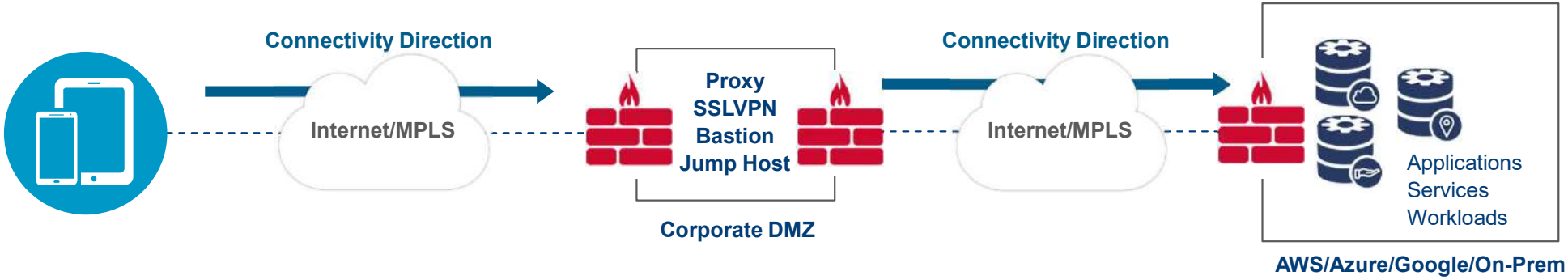


Anyone to anywhere – simple and secure app access

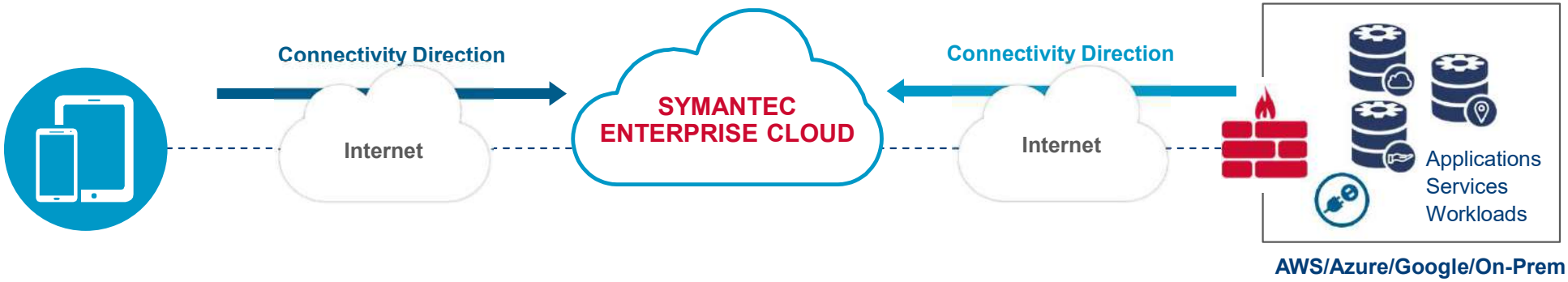
Symantec by Broadcom

Cloud Alternative to Traditional Access Methods

Traditional DMZ—Connected via the Network



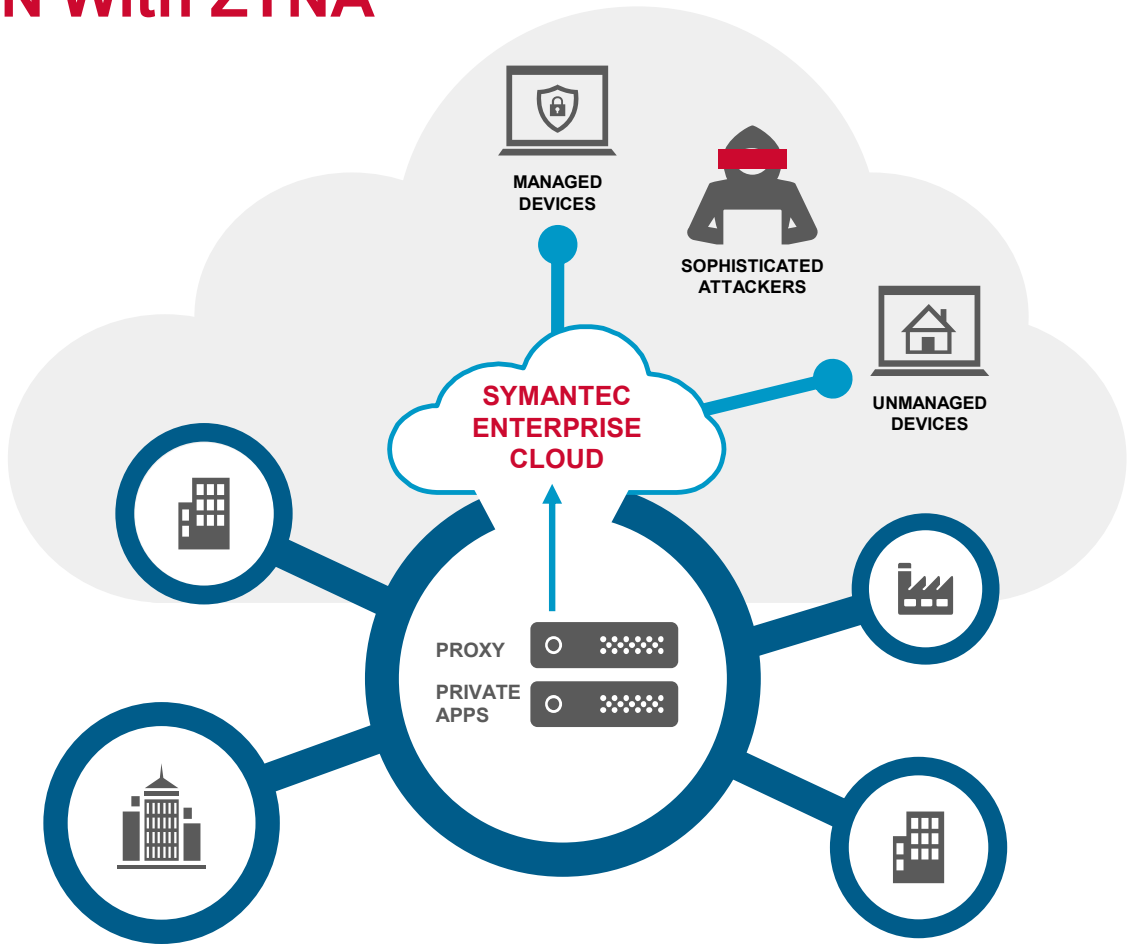
Symantec Secure Access Cloud—SDP-based Cloud Native Connectivity



Symantec by Broadcom

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



Symantec by Broadcom

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 CICD 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

Symantec by Broadcom

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

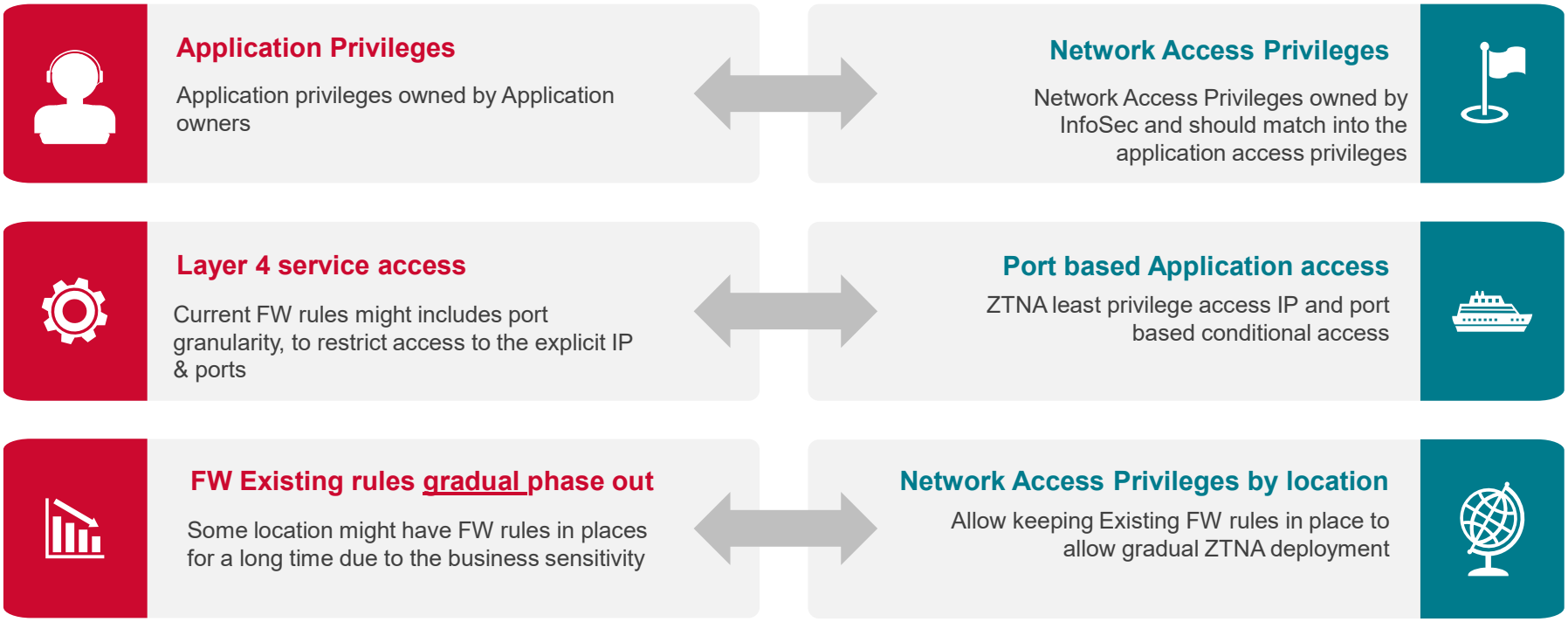
When it comes to the product maintenance, teams are struggling to handle a lot of daily operations related to the provisioning/deprovisioning for the resources or access privileges

4 Compatibility impact

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

Symantec by Broadcom

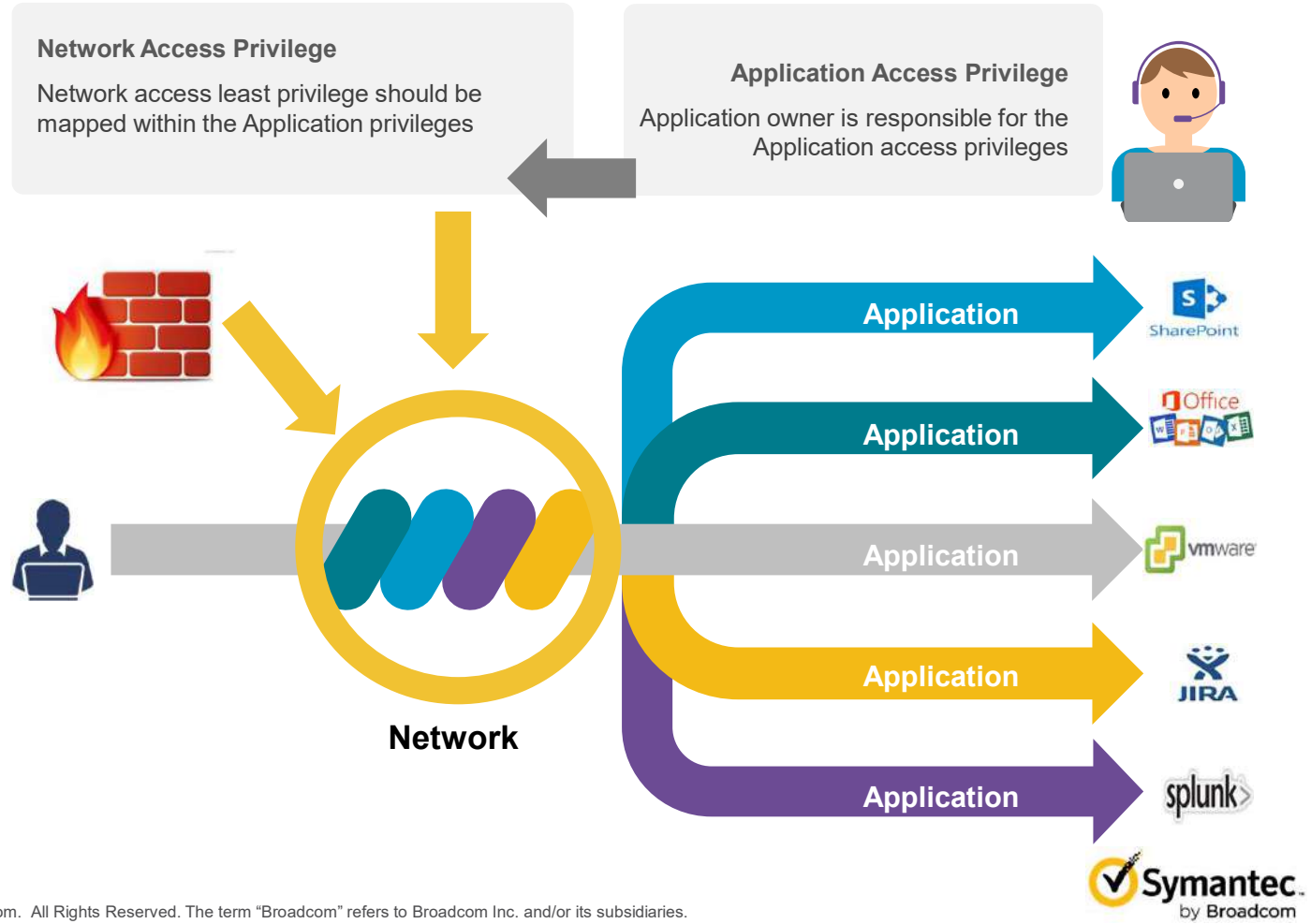
Network Onboarding challenges



Symantec by Broadcom

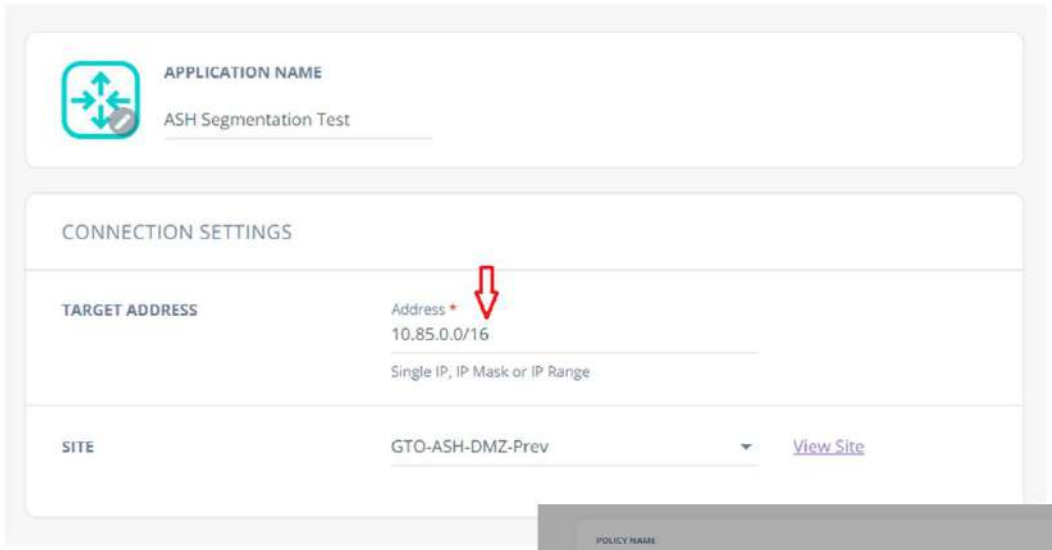
Heavy Lifting Onboarding (visualizing)

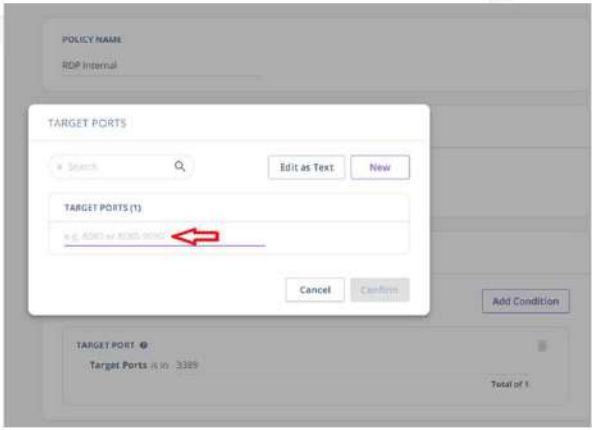
- Big effort
- Long project lead times
- High cost (pay twice)



How we solve it

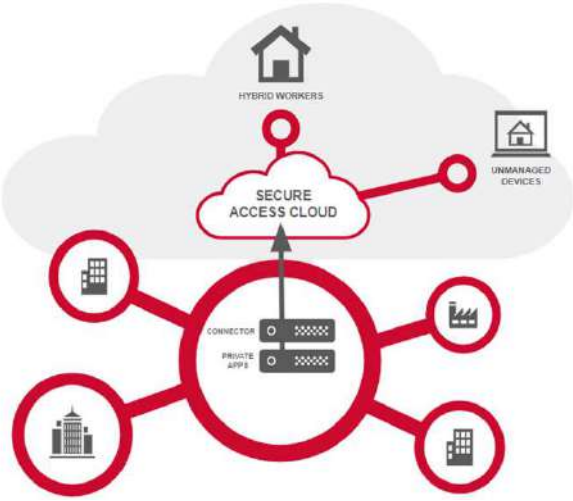
- We take it all ! - All network provisioned at once with few app and single policy
- Apply network policies gradually at any time without relying on the network team.
- No user impact
- Coexist with agentless access (due to the alternative data path)





Symantec by Broadcom

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**

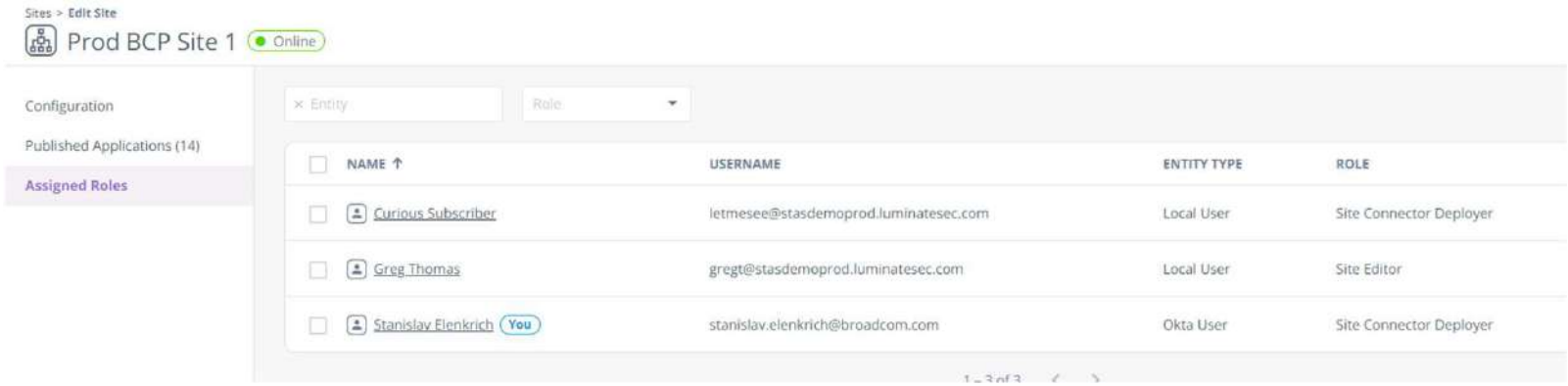
Conditional access for explicit applications has no business impact or application changes

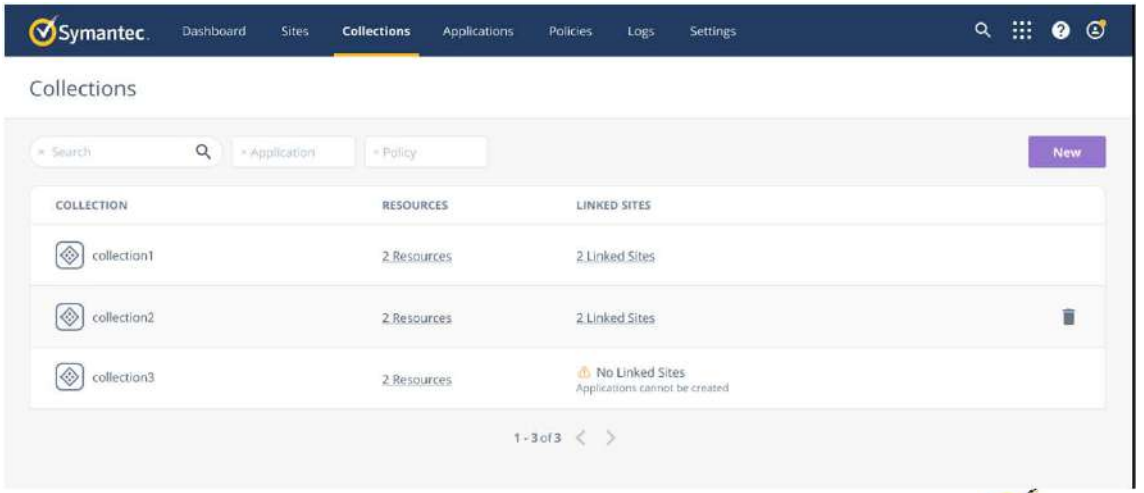
4 **Keep Your User Experience the Same**

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

Symantec by Broadcom

SecOps Impact - RBAC





Symantec by Broadcom

SecOps Challenges - Automation

Automate everything !

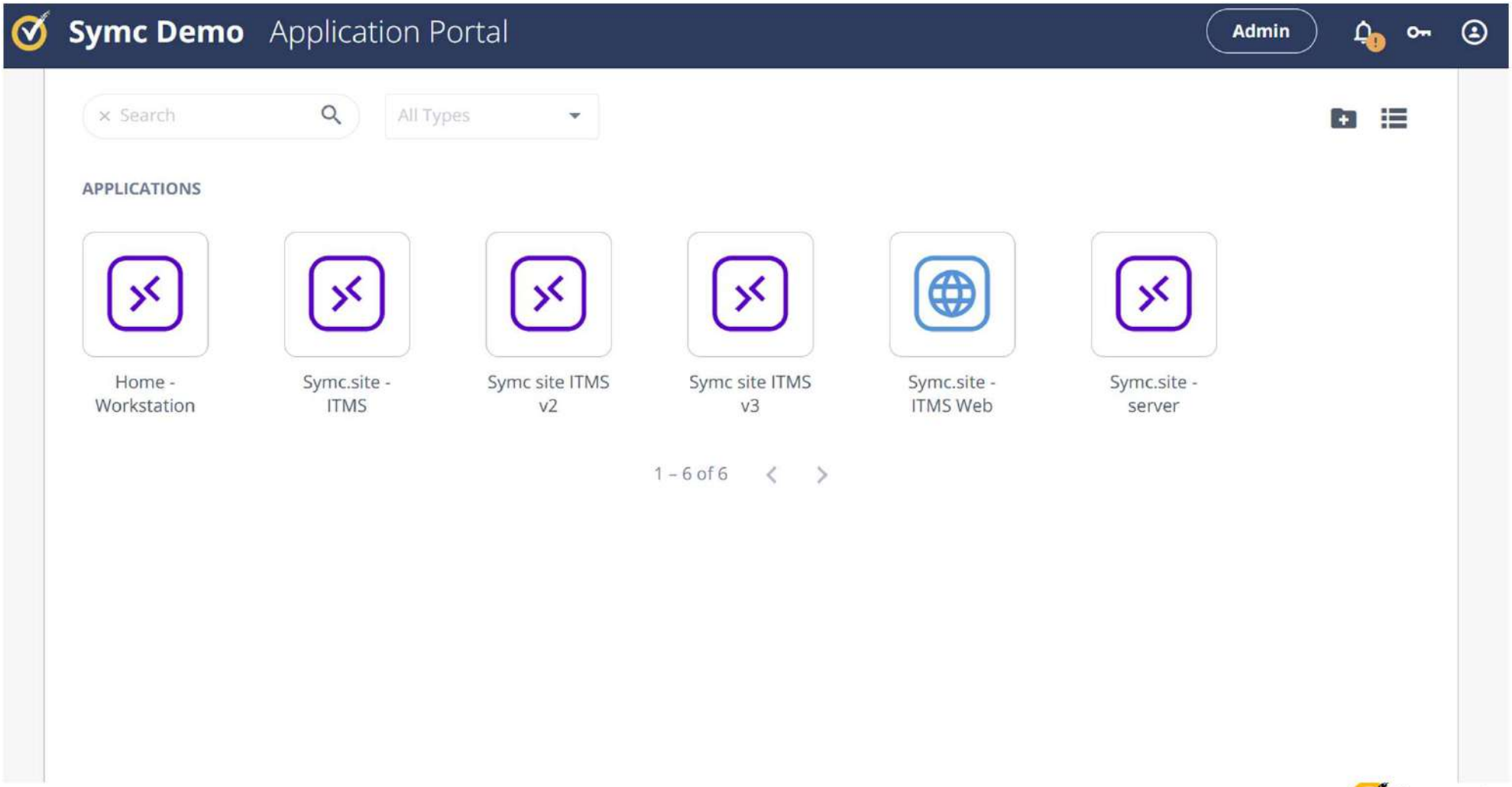
Full API control

Terraform Support

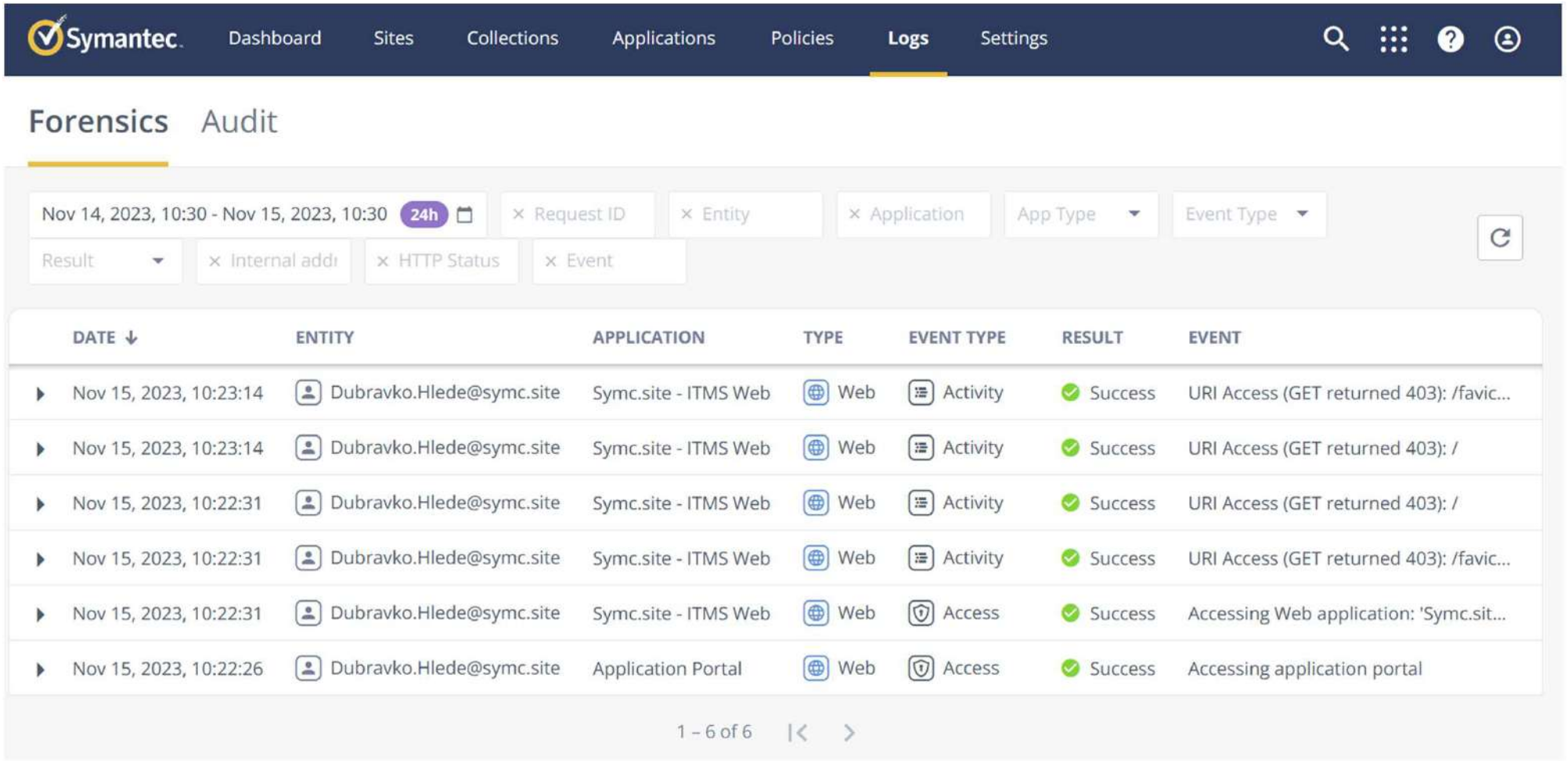
Slack Integration

RBAC

Symantec by Broadcom



Symantec by Broadcom



Symantec by Broadcom

NE VERUJ NIKOME 2023

HVALA NA PAŽNJI

Email: office@netpp.rs

Telefon: +381 11 3699 967