



# THYCOTIC

PRIVILEGED ACCESS MANAGEMENT

# More 5-star reviews than any other PAM vendor



**Agility & Security**



## Performance & Ease of Use

We are very pleased with **performance** and **ease of use**, especially compared to the product it will replace.

CISO, FINANCE INDUSTRY



## Requires Less, Covers More

Thycotic is 100% better than CyberArk at a fraction of the cost. And requires a **smaller footprint** and **covers more compliance requirements**.

IT SPECIALIST, SERVICE INDUSTRY



## Adoption Skyrockets

**Adoption** has been organic **without a need to strongly push** the tool. **It's intuitive**, requiring very little training to get our teams up and running.

INFOSEC MANAGER, SERVICE INDUSTRY

**Total Cost of Ownership**



# PRIVILEGED ACCOUNTS

## What is a privileged account?

- **Non or human accounts** used by IT staff which often have unfettered access to critical data and systems i.e. Domain Admin, root.
- **Exist everywhere** in nearly every connected device, server, hypervisor, OS, DB, or application: on-premises & cloud.
- Represent one of the **most vulnerable aspects** of an organization's IT infrastructure.

Secret Server

# Privileged Accounts



Domain Administrators  
Windows Local Administrators  
Domain Service Accounts



RedHat  
Debian  
Fedora



MSSQL  
Oracle  
MySQL



AS400 / OS390  
z/OS (RACF)  
SSH

thycotic



Secret Server



Privileged Accounts

Encrypted – AES256bit



Cisco / Juniper  
Checkpoint / Palo Alto  
Blue Coat / SonicWall



Google / Office365 / Salesforce  
SAP / Social Media  
AWS / Azure



VMware ESX/ESXi  
Dell DRAC / HP iLO  
SSH/Telnet Compatible



Config Files  
Scripts  
DevOps

# Accounts and Password's usage today..



- **Zsolt, 22 Years old, IT Administrator**  
responsible for 80 Servers and 260 Workstations
- Can't remember Passwords longer than 10 chars
- Is responsible for 500 Service Accounts within the organisation (Windows, Unix, IBM, Cloud)
- Uses usually same Passwords on all accounts he needs to manage
- Stores them in a secret location in a plain text document
- Changes usually every 2 Years Companies

**Zsolt also manages this cloud services and required Admin accounts:**

Google

Office365

Evernote

Azure

Egnyte

Salesforce

Adobe

Dropbox

Amazon AWS

PhoenixNAP

# ROI and Time Saving

Zsolt's company implemented Thycotic PAM and now he can



Manage all **privileged accounts** in one interface

Discover all **unknown privileged accounts**

Setup **secure encrypted vault**, permissions, users and structure

Store and **Rotate sensitive accounts** within **Secret Server**

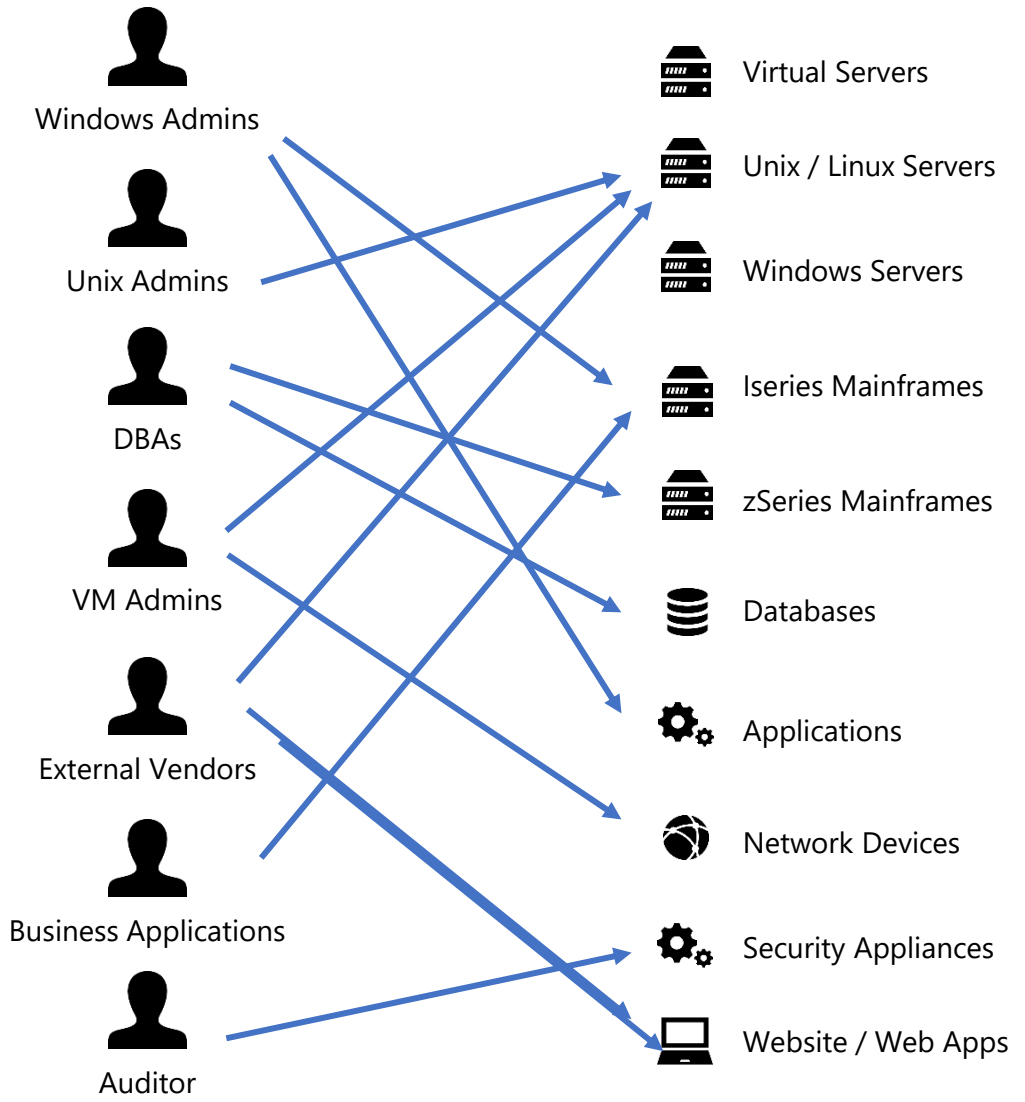
Implement **RBAC, Access Requests**, and other controls

He can now work with:

- **Session launching**
- **Session proxying**
- **Session monitoring**
- **Session recording**

Implement **least Privilege Access** accross his organisation without spending much time on administrative tasks

# PAM: Without Thycotic



## Why PAM Security is Difficult

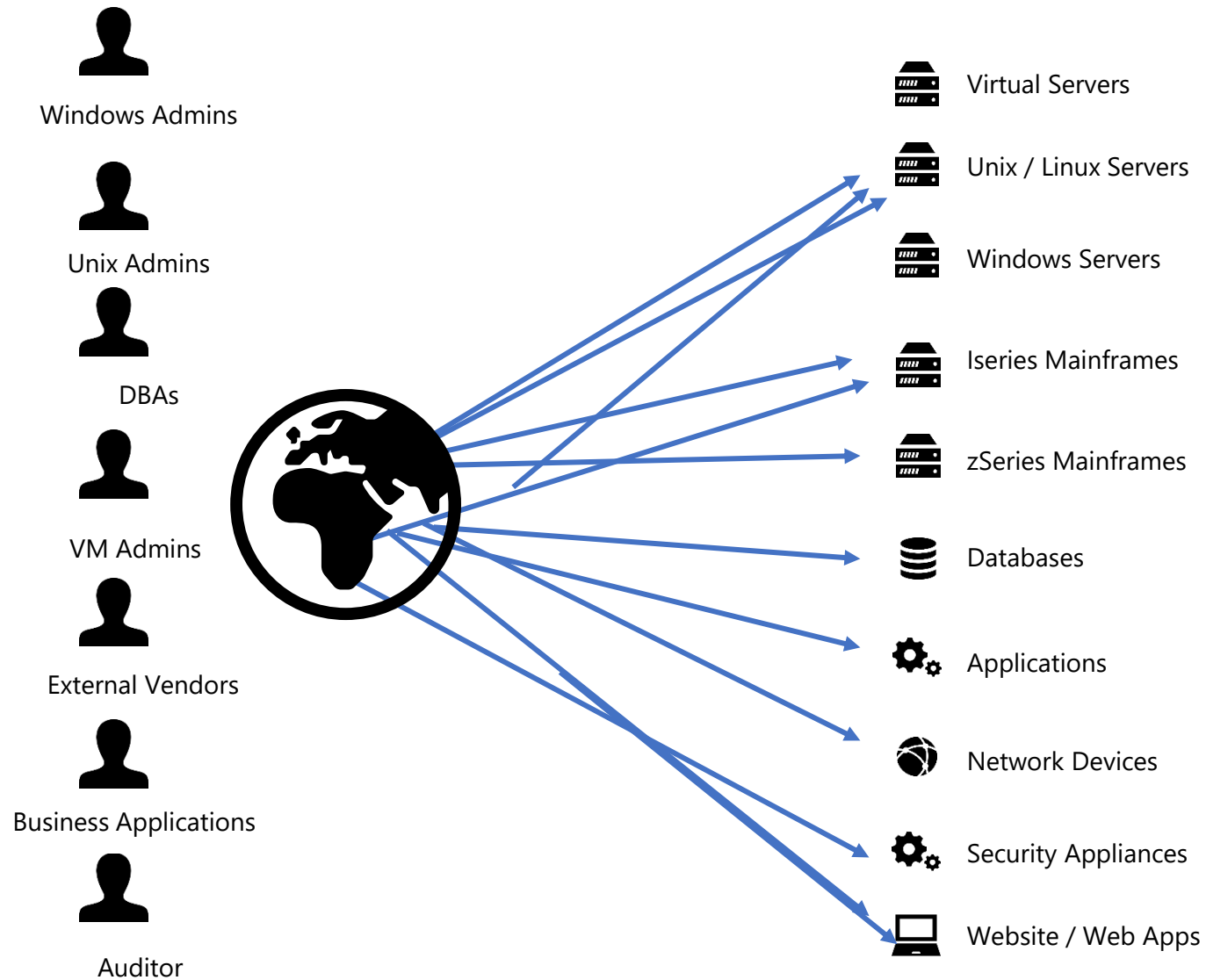
- Different-Systems,
- Environments,
- Applications
- Roles
- Databases
- Roles
- Devices

Different Roles need different access  
Employees need different access to different data

Cloud or on premise



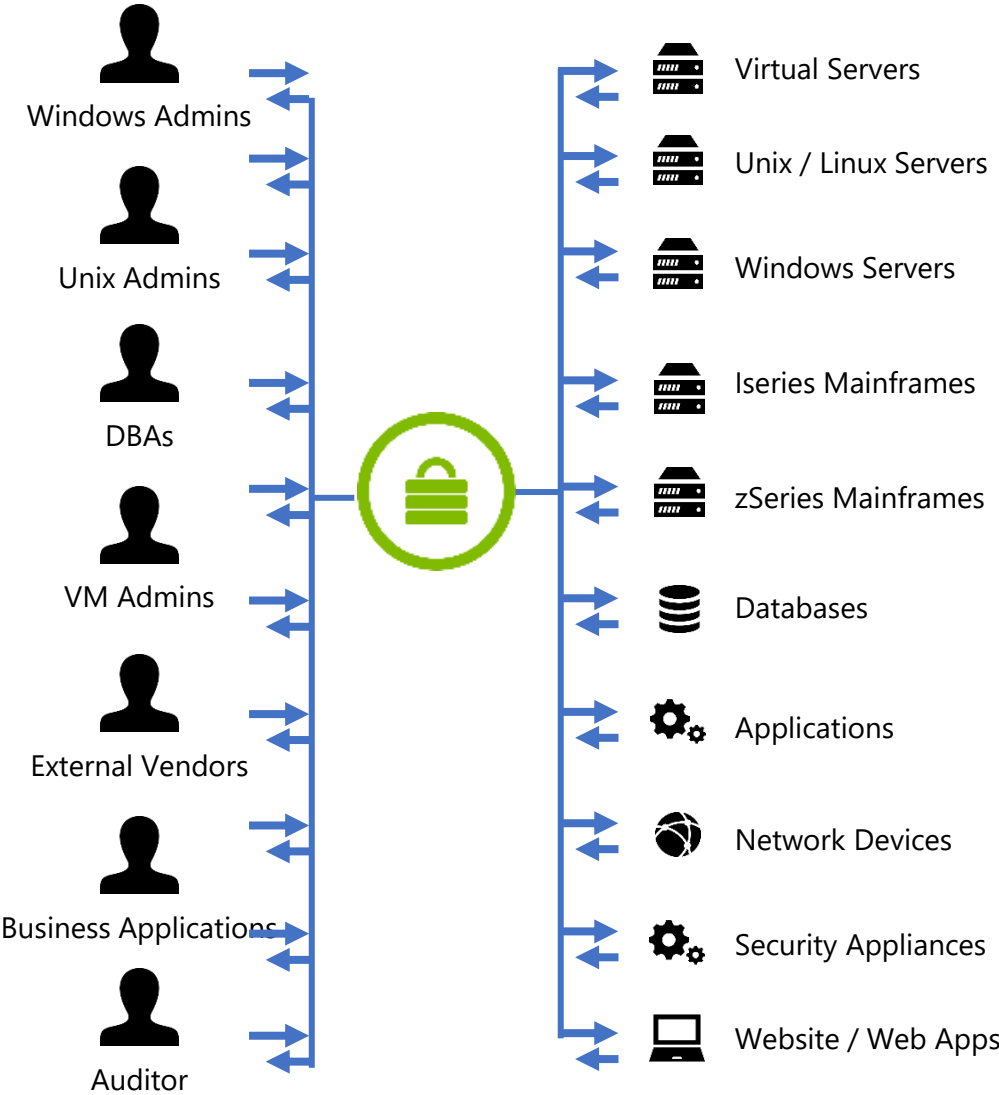
# PAM: Without Thycotic now





# PAM: With Thycotic

- **Automatic identification** of privileged account risk
- **Continuous monitoring** of suspicious behavior and secure storage of privileged accounts
- **Real-time detection**, alerting and response to malicious privileged account activity
- **Enforcement of least privilege** through application control



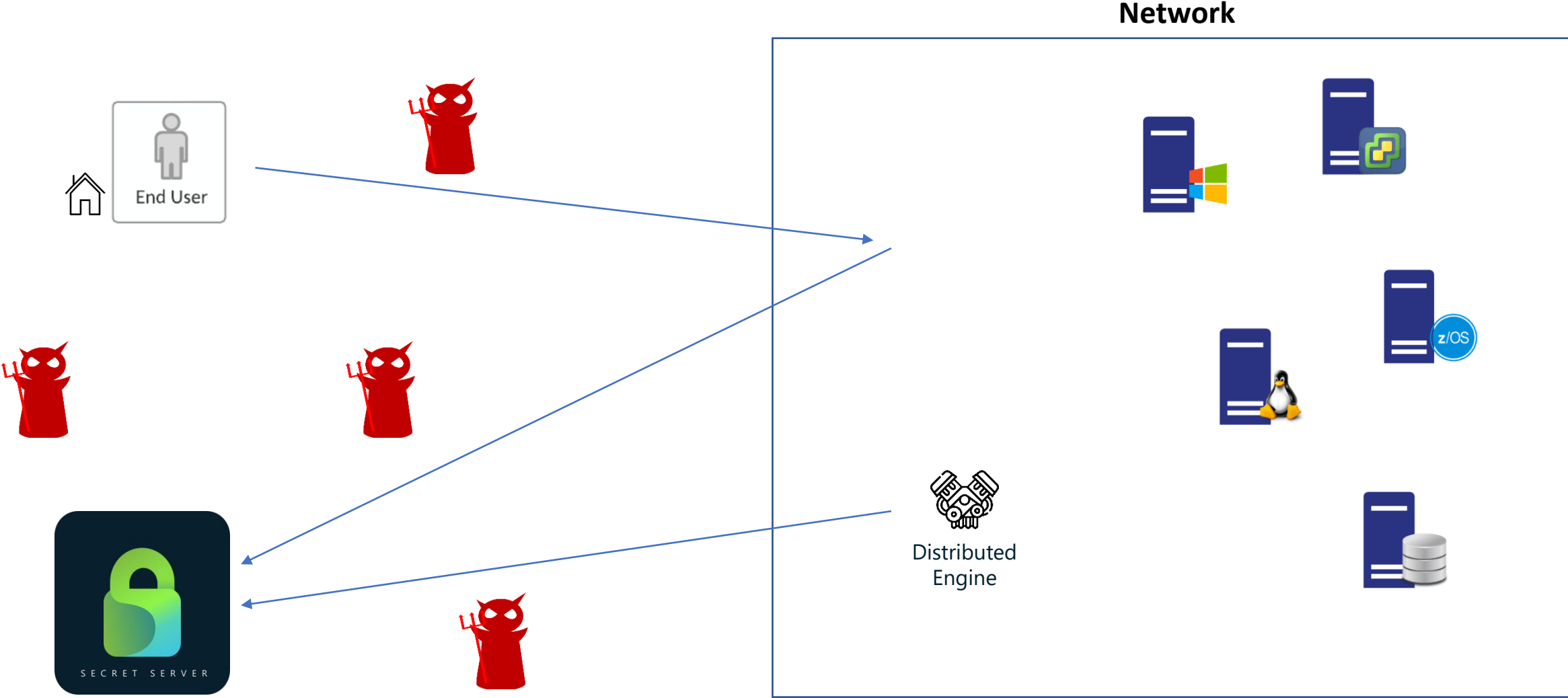
# Current remote working is not like “Homeoffice” was before

- **People now work Remote which never worked from home**
  - Distraction at home much higher than usually (Children etc.)
  - People not trained and aware about issues at home
- **Setup of Remote workers was done quick and in hurry**
  - People and Equipment went out of the Perimeter without long security planning
  - Private Home Internet Connection mainly used
  - Given access rights for Remote workers often too high





# To do something without proper planning is always a security risk

- **Forgotten Details?**
  - Configuration changes in AD
  - Configurations on Firewalls
  - Forgotten Webfiltering (usually internal proxy)
  - Missing Remote Management and Support solution?
  - No Endpoint Security or DLP solution?
  - Windows Firewall configuration?
  - Backup concept?

# VPN – Virtual Private Network



# The Challenge: Traditional PAM can miss Privileged Accounts

ACCOUNT TYPE	Business Users		✓		✓	
	External Vendors	✓	✓	✓	✓	✓
	Windows Admins	✓	✓	✓	✓	✓
	Unix Admins	✓	✓	✓	✓	✓
	Applications	✓	✓	✓	✓	✓
	Services	✓	✓	✓	✓	✓
						
	Data Center	Network Devices	Cloud	DevOps	Endpoints	Op Tech
	IT			OT		

## Under-the-radar service accounts

"These privileged credentials are usually not inventoried, changed, or controlled, meaning that hackers can use them to gain easy access to business-critical applications." – Forrester

## Cloud infrastructure

"The explosion of cloud services has driven proliferation of privileged accounts and credentials to a state that, for most organizations, is unmanageable without processes and tools" – Gartner

## DevOps CI/CD pipelines

"Instances of hard-coded credentials, credentials appearing in source code repositories, no credential rotation or highly fragmented approaches to credential vaulting... these challenges represent risk" – Gartner

“

Usability is so central to building security that works in the real world - not just on paper - that no savvy organisation can afford to ignore it. The only good security is usable security.



National Cyber  
Security Centre

Security and Usability: You CAN Have It All!



# 35 Industry Awards in 2019

