PRIVILEGED ACCOUNTS UNDERESTIMATED SECURITY RISK

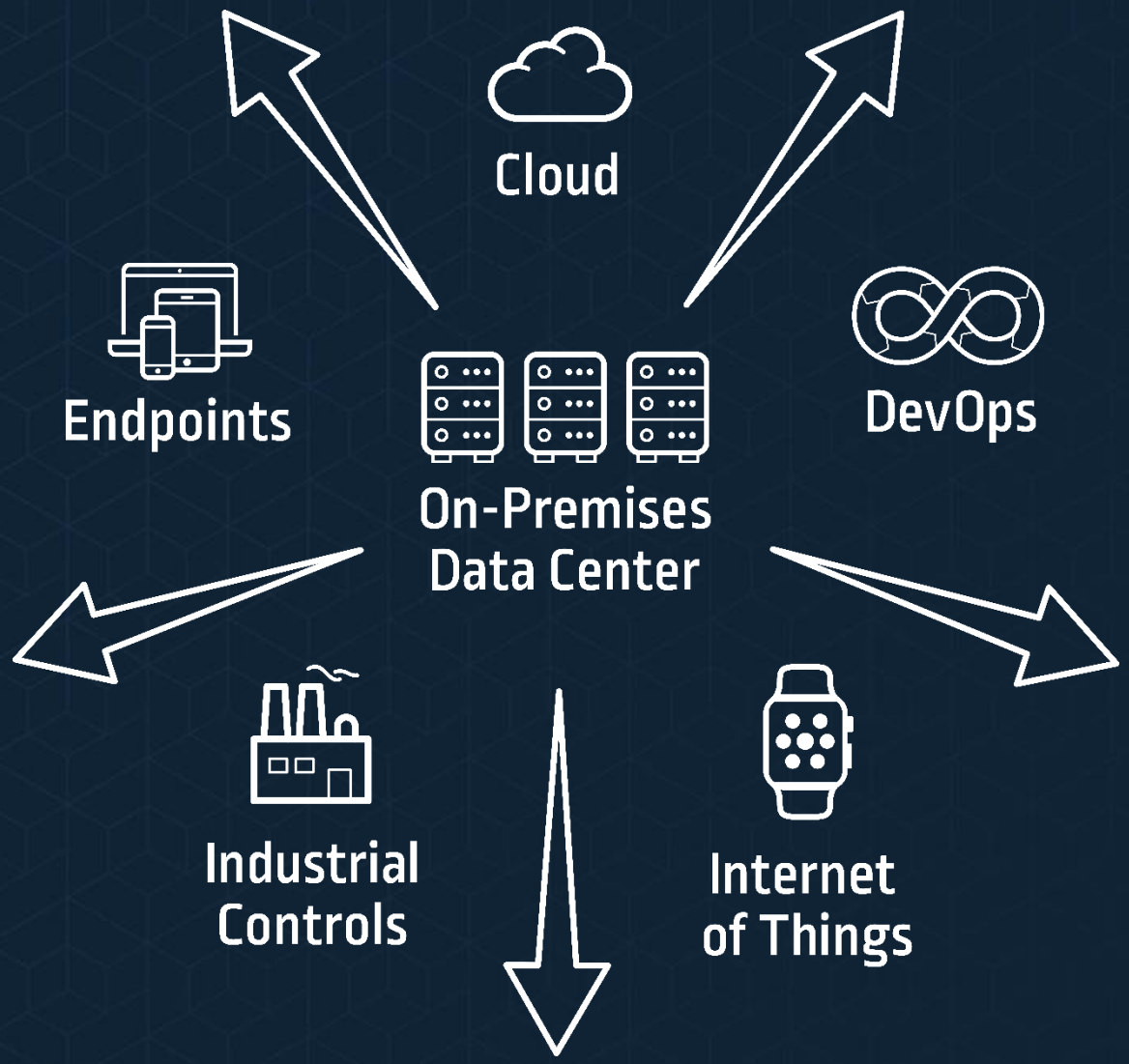
Marcin Paciorkowski

Regional Sales Engineer, CISSP

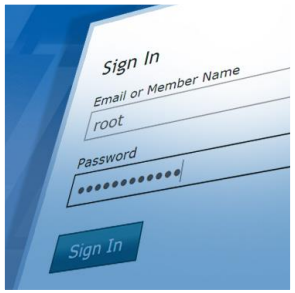
marcin.paciorkowski@cyberark.com

CYBERARK

THE ATTACK SURFACE CONTINUES TO GROW



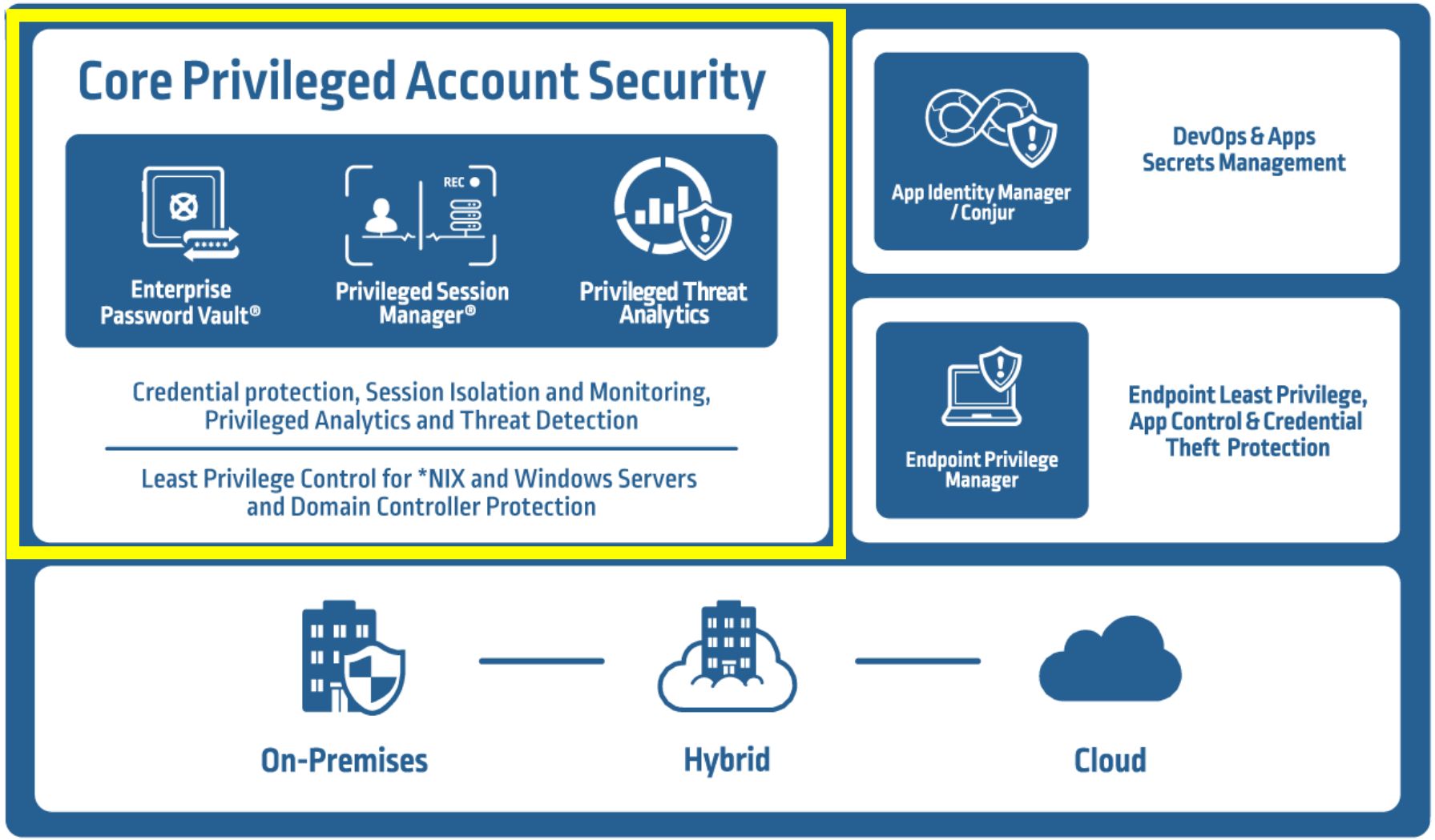
ATTACK VECTORS (SIMPLIFIED)

PtH – Pass-the-Hash	• The password hash of an account is used instead of an password to log on to different machines as long they have the same account with the password(-hash) • Can be used with local or domain accounts • PtH is often done before an successful Golden Ticket attack	
Golden Ticket	• Attack against the KRBTGT account residing on the DC • KRBTGT is the account which is used by DCs to generate Kerberos tickets • Means the attacker can impersonate to everyone • ”Easy to fix“ but it may break a lot of stuff, without proper preparation	
SSH Keys	• Orphaned and forgotten SSH Keys may enable access to unexpected systems • Nearly impossible to control how they are distributed and copied	
Credential Theft	• Windows Computers are vulnerable to credential theft from memory, SAM, config files, browsers or processes like LSASS	

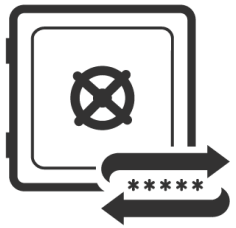
CYBERARK

PRIVILEGED ACCOUNT SECURITY SOLUTION

CYBERARK PRIVILEGED ACCOUNT SECURITY SOLUTION



FOUNDATIONAL PRIVILEGED SECURITY SOLUTIONS

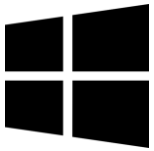


CREDENTIAL PROTECTION & MANAGEMENT

SESSION ISOLATION, MONITORING & RECORDING

THREAT DETECTION & ANALYTICS

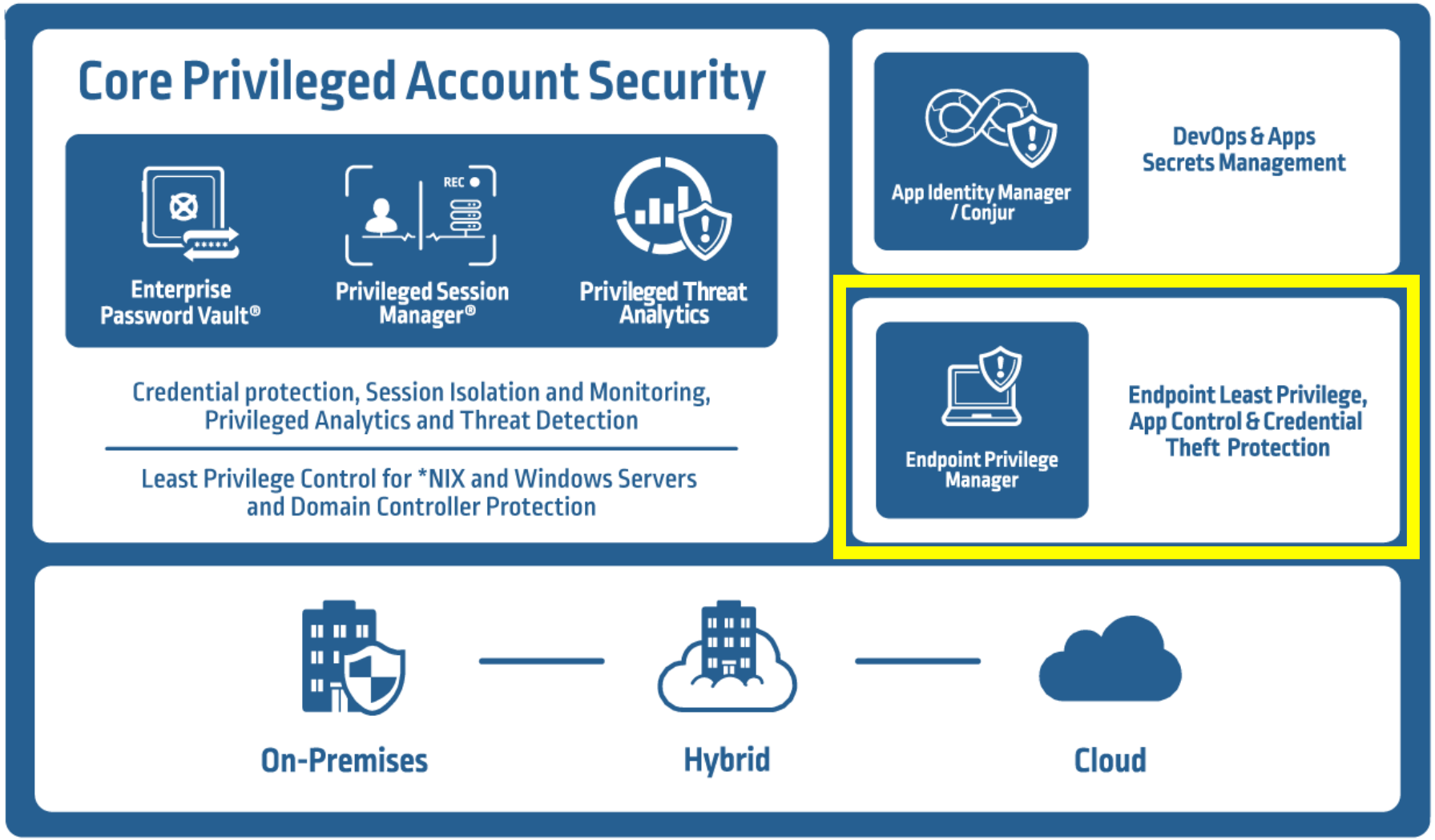
***NIX SERVER PROTECTION**



WINDOWS SERVER PROTECTION

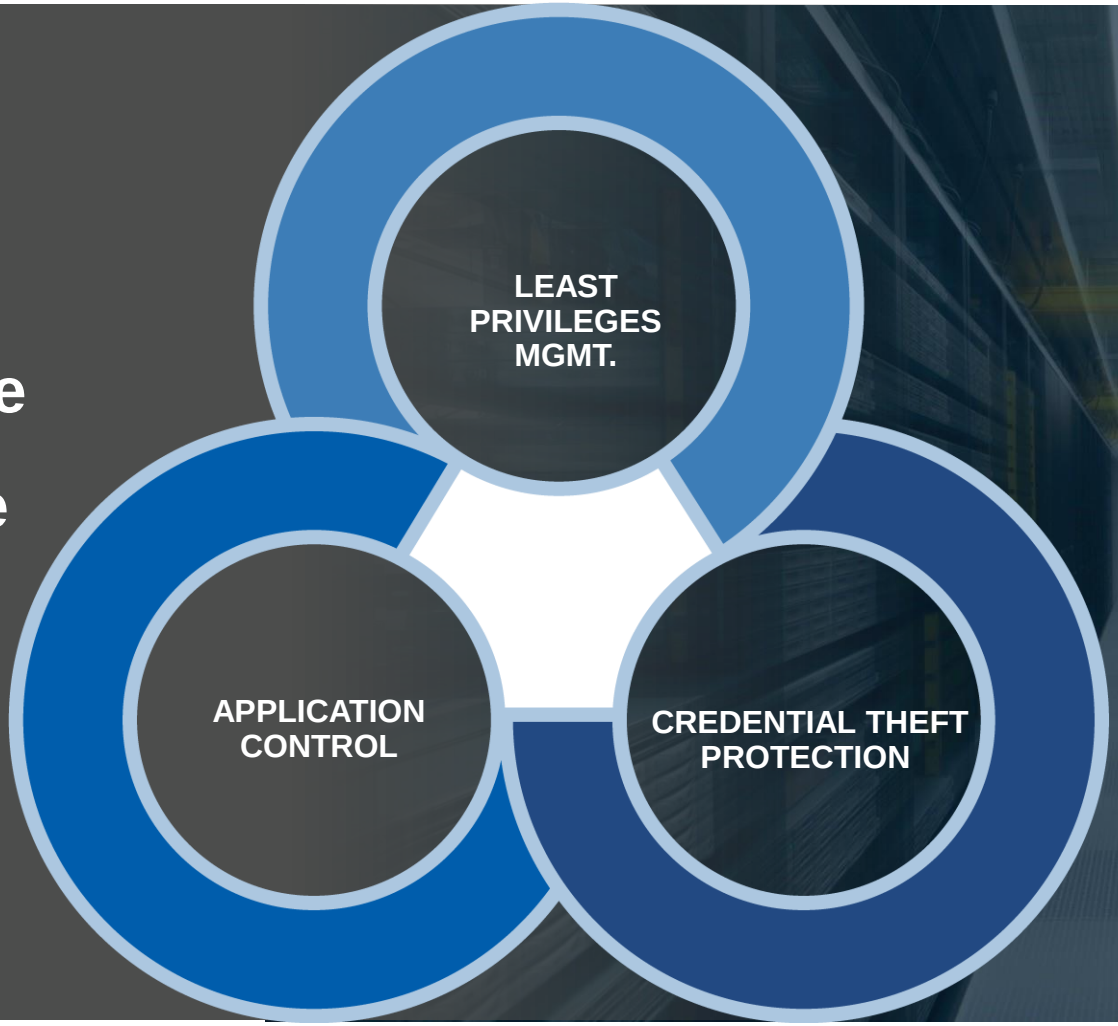
DOMAIN CONTROLLER PROTECTION

CYBERARK PRIVILEGED ACCOUNT SECURITY SOLUTION

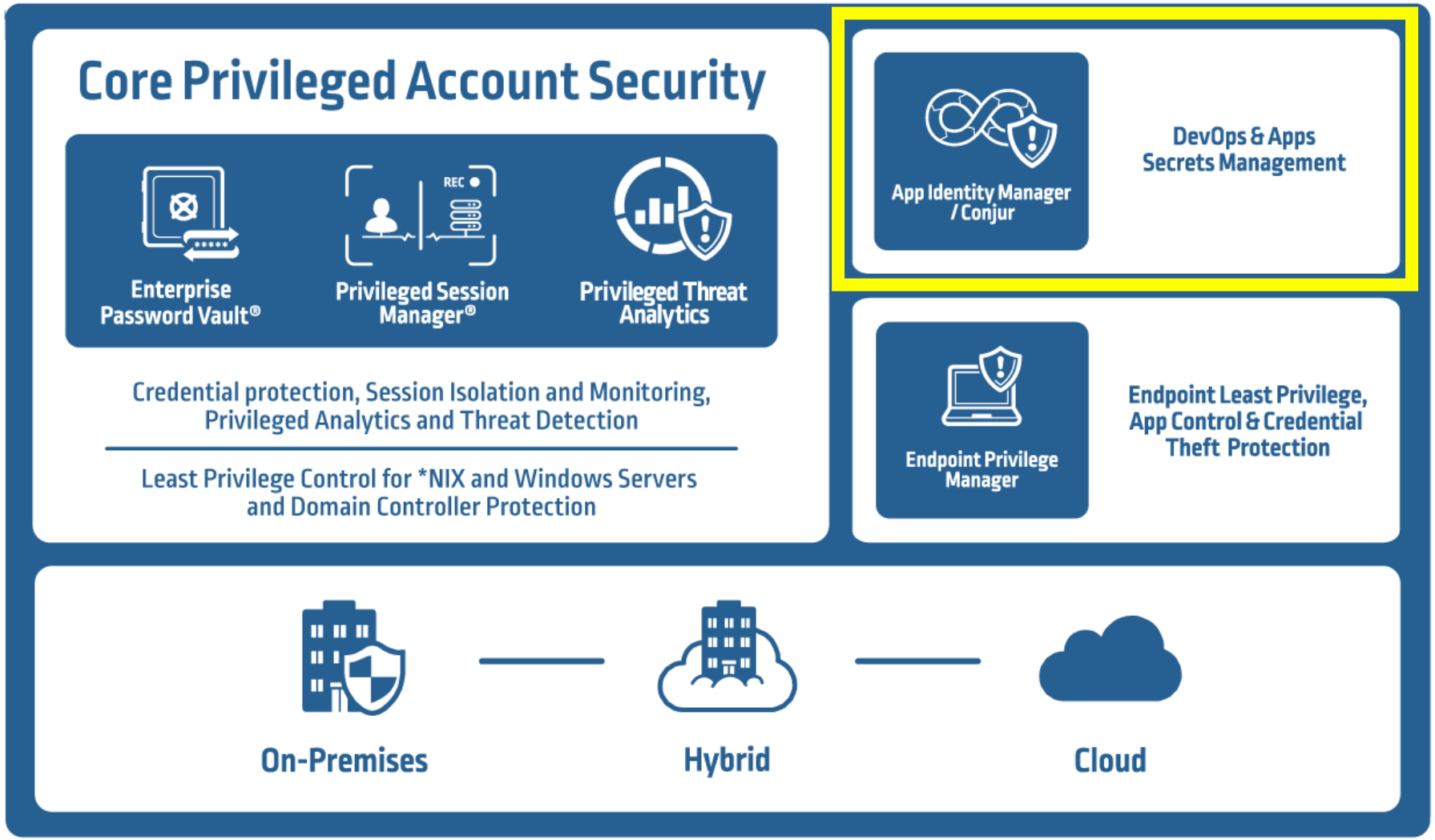


CYBERARK ENDPOINT PRIVILEGE MANAGER

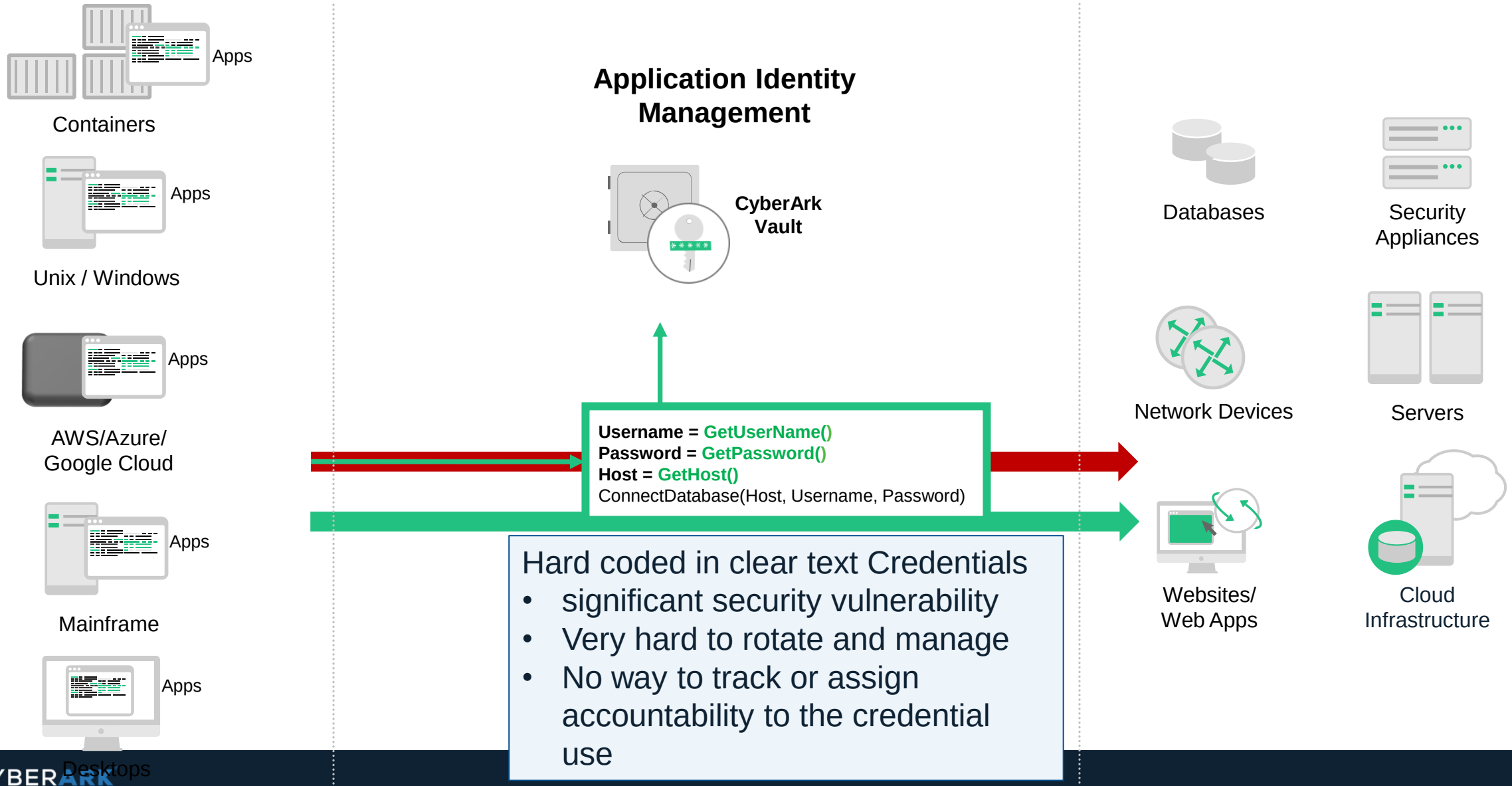
Enable privilege security on the endpoint



CYBERARK PRIVILEGED ACCOUNT SECURITY SOLUTION



ARCHITECTURE: HIGH-LEVEL TOPOLOGY



WHAT IS DNA?

- Gives you insight in your Privileged Account estate
- Gives insight in your Risks
- Helps to define the scope of your project

DISCOVERY AND AUDIT: WHAT DOES IT FIND?

- Windows accounts
- Unix accounts
- Mac OS accounts
- Accounts with access rights to desktops and servers (backdoors)
- Embedded Windows credentials in service accounts, Scheduled Tasks, IIS App Directories, and more.
- Hard-coded credentials in WebSphere, WebLogic and IIS Servers
- Hard-code credentials in Ansible Playbooks
- SSH Keys
- Cloud Assets: AWS IAM Users and Access Keys, EC2 Instances and their Key pairs
- Credential-harvesting detection
- Databases accounts

CYBERARK

THANK YOU

Marcin Paciorkowski
Regional Sales Engineer, CISSP
marcin.paciorkowski@cyberark.com