CyberArk – Dalla gestione degli utenti privilegiati alla protezione degli Endpoint

Marco Di Martino

Director of Presales and Professional Services - SEMEA
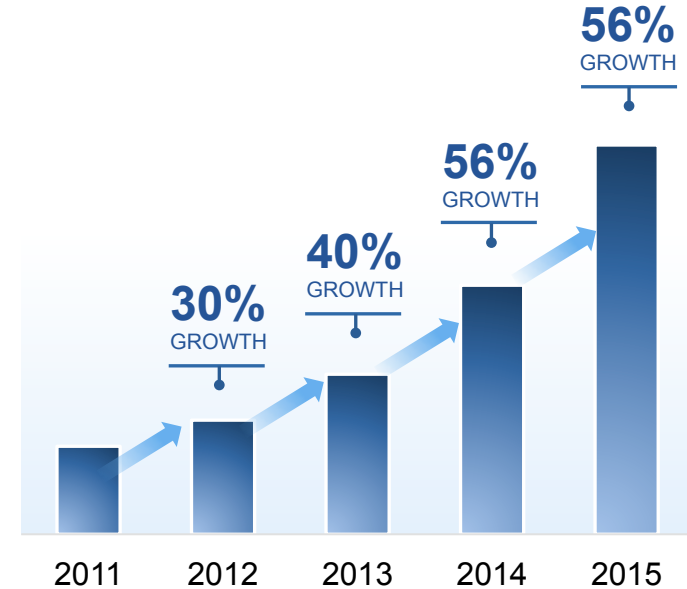
Marco.DiMartino@CyberArk.com

Trusted by Customers worldwide

Approach privileged accounts as a security challenge

- Designed and built from the ground up for security

2,500+ Global Customers

More than 40% of Fortune 100

More than 20% of Global 2000
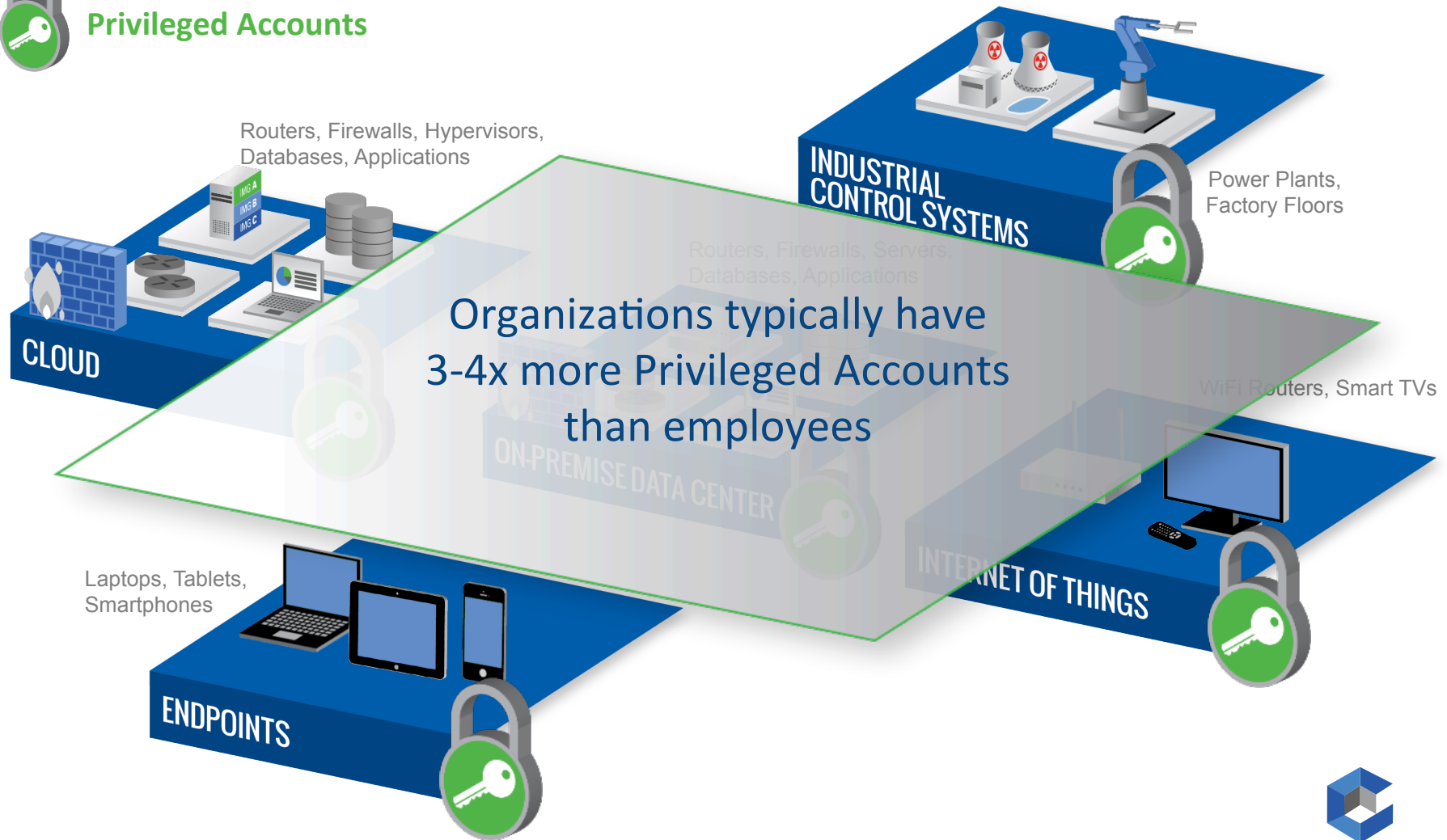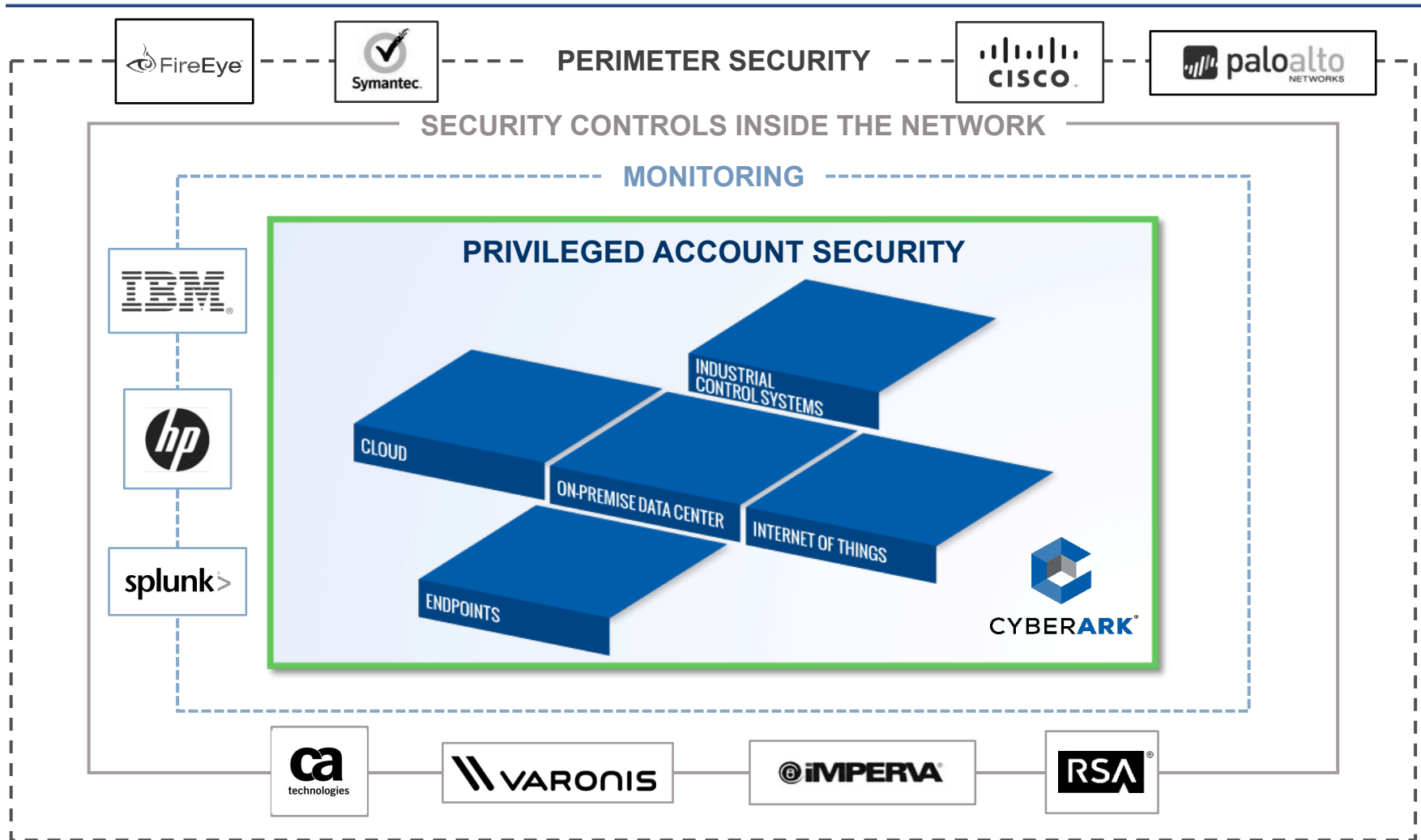
CyberArk Italy 13 employees

More than 80 customers

2011   2012   2013   2014   2015

30% GROWTH

40% GROWTH

56% GROWTH

56% GROWTH

Privileged Credentials are Everywhere

Privileged Accounts

Routers, Firewalls, Hypervisors, Databases, Applications

INDUSTRIAL CONTROL SYSTEMS

Power Plants, Factory Floors

Routers, Firewalls, Servers, Databases, Applications

CLOUD

Organizations typically have 3-4x more Privileged Accounts than employees

ON-PREMISE DATA CENTER

WiFi Routers, Smart TVs

Laptops, Tablets, Smartphones

INTERNET OF THINGS

ENDPOINTS

CYBERARK®

CyberArk Delivers a New Critical Security Layer

CyberArk's Privileged Account Security Solution

REAL-TIME THREAT DETECTION

Privileged Threat Analytics

PROACTIVE CONTROLS

Enterprise Password Vault®

SSH Key Manager

Privileged Session Manager®

Application Identity Manager™

Viewfinity

On-Demand Privileges Manager™

SHARED TECHNOLOGY PLATFORM

Web Management Interface

Master Policy

Discovery Engine

Secure Digital Vault™

PROTECT

DETECT

RESPOND

CYBERARK®

Creating a New, "Must Have" Security Layer

CORPORATE ENDPOINT

Privileged Account Security

THREAT ANALYSIS & PROTECTION

Protecting privileged accounts and detecting privilege threats

CYBERARK®

Comprehensive Controls on Privileged Activity

Lock Down Credentials

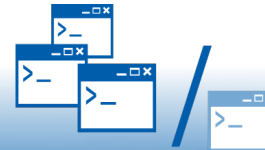Protect privileged passwords and SSH keys

Enterprise Password Vault
SSH Key Manager
Application Identity Manager

Enforce Least Privilege

Remove admin rights. Escalate privilege on demand

On-Demand Privileges Unix.
Windows
ViewFinity

Isolate & Control Sessions

Prevent malware attacks and control privileged access
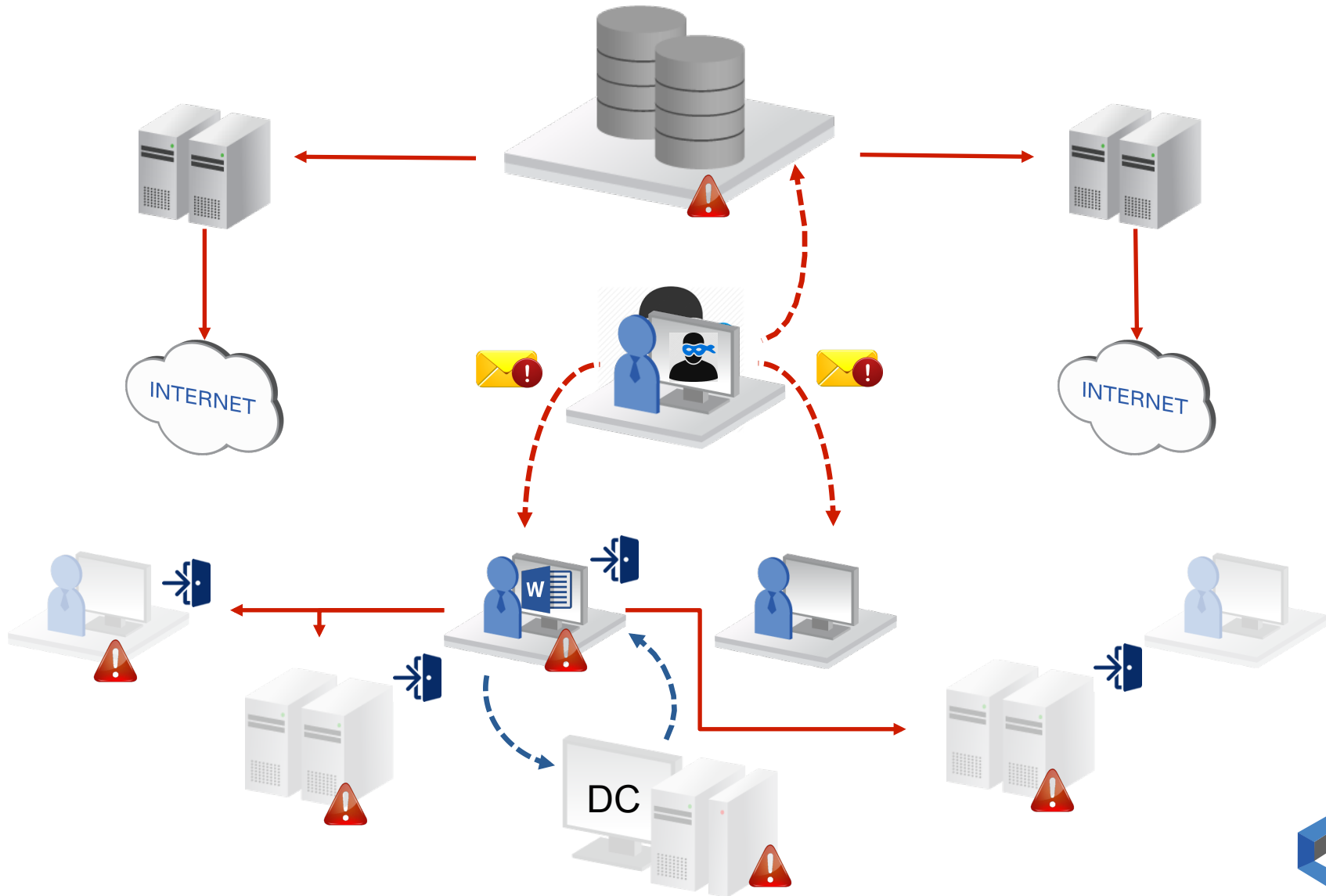
Privileged Session Manager

Continuously Monitor

Implement continuous monitoring across all privileged accounts

Privileged Threat Analytics

CYBERARK®

Real Cyber Attack Case Study: Attacker conducts lateral movement, privilege escalation, executes a Golden Ticket attack, and successfully exfiltrates sensitive data

INTERNET

INTERNET

DC

CYBER**ARK**

Least Privilege + App Control = Least Risk

Least Privilege	Application Control
Remove and manage privileges for business and administrative users	Only allow whitelisted, trusted applications
Gap: Malicious applications that don't need privileges can still get in	**Gap:** Applications that require privileges requires providing admin privileges to users

PRIVILEGES

APPLICATIONS

Combined, least privilege and application control enable organizations to **reduce the attack surface** and **block the progression of malware-based attacks**

CYBERARK®

Prevent CryptoLocker with CyberArk Viewfinity

CryptoLocker

- Ransomware trojan that enters the environment via infected email attachments

- Admin rights are NOT required
  - The malware encrypts data using standard user rights

- Causes immediate business impact
  - The malware encrypts and renders all files in the corporate environment unreadable

CyberArk Viewfinity can help prevent CryptoLocker from entering an organization

Least Privilege	Application Control
- Remove local admin privileges to block CryptoLocker from deleting the shadow copy command - Enable security team to restore encrypted files using shadow copy	- Block untrusted applications - Restrict or deny access for unknown applications (such as CryptoLocker) - Continuously monitor applications entering the environment

CYBERARK®

Thank You