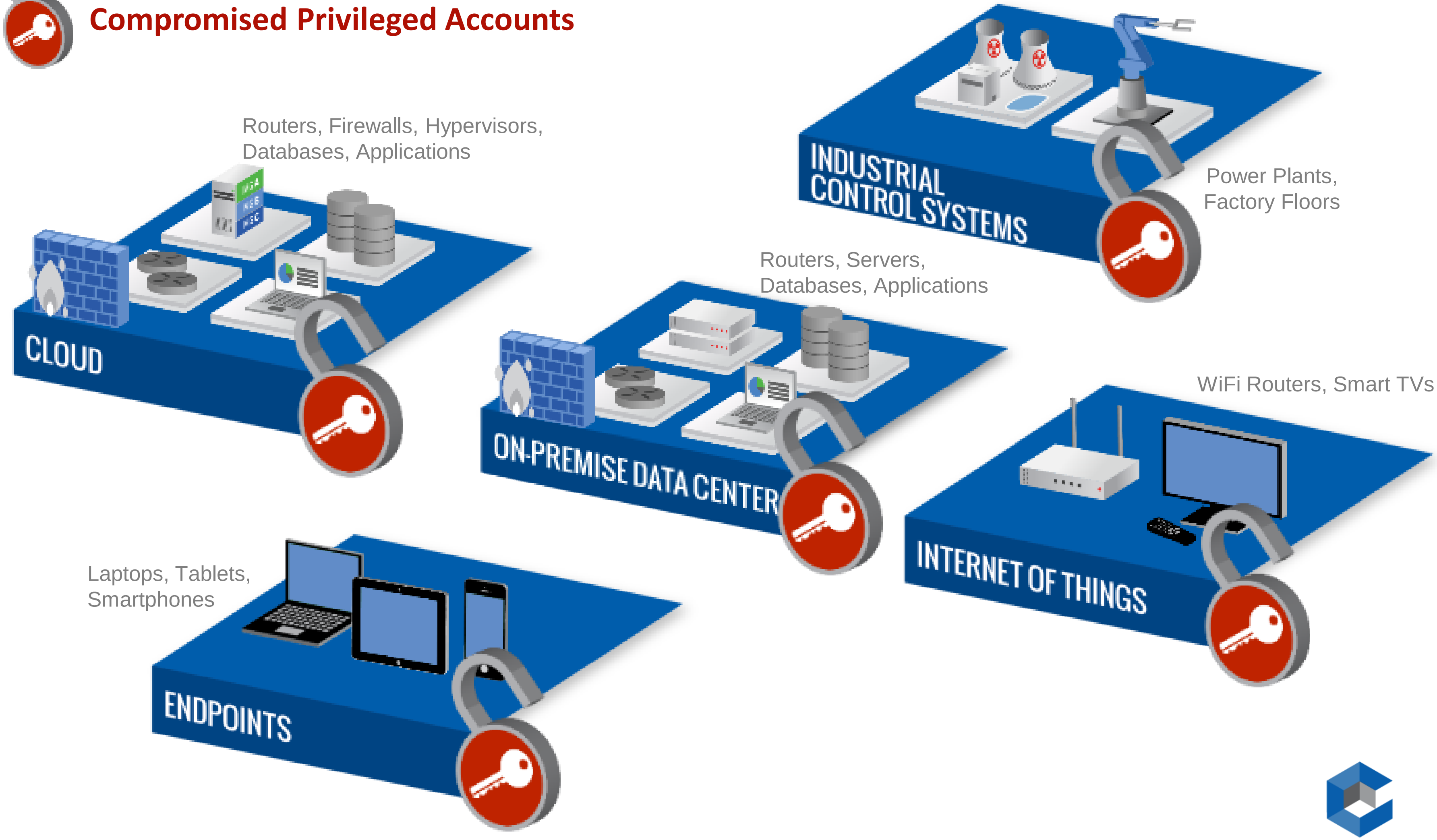
Don’t fight with consequences, Protect the cause!

Anton Fridrikh
anton.fridrikh@cyberark.com

April 16

Hijacked Credentials Put the Attacker in Control

Compromised Privileged Accounts



Routers, Firewalls, Hypervisors, Databases, Applications

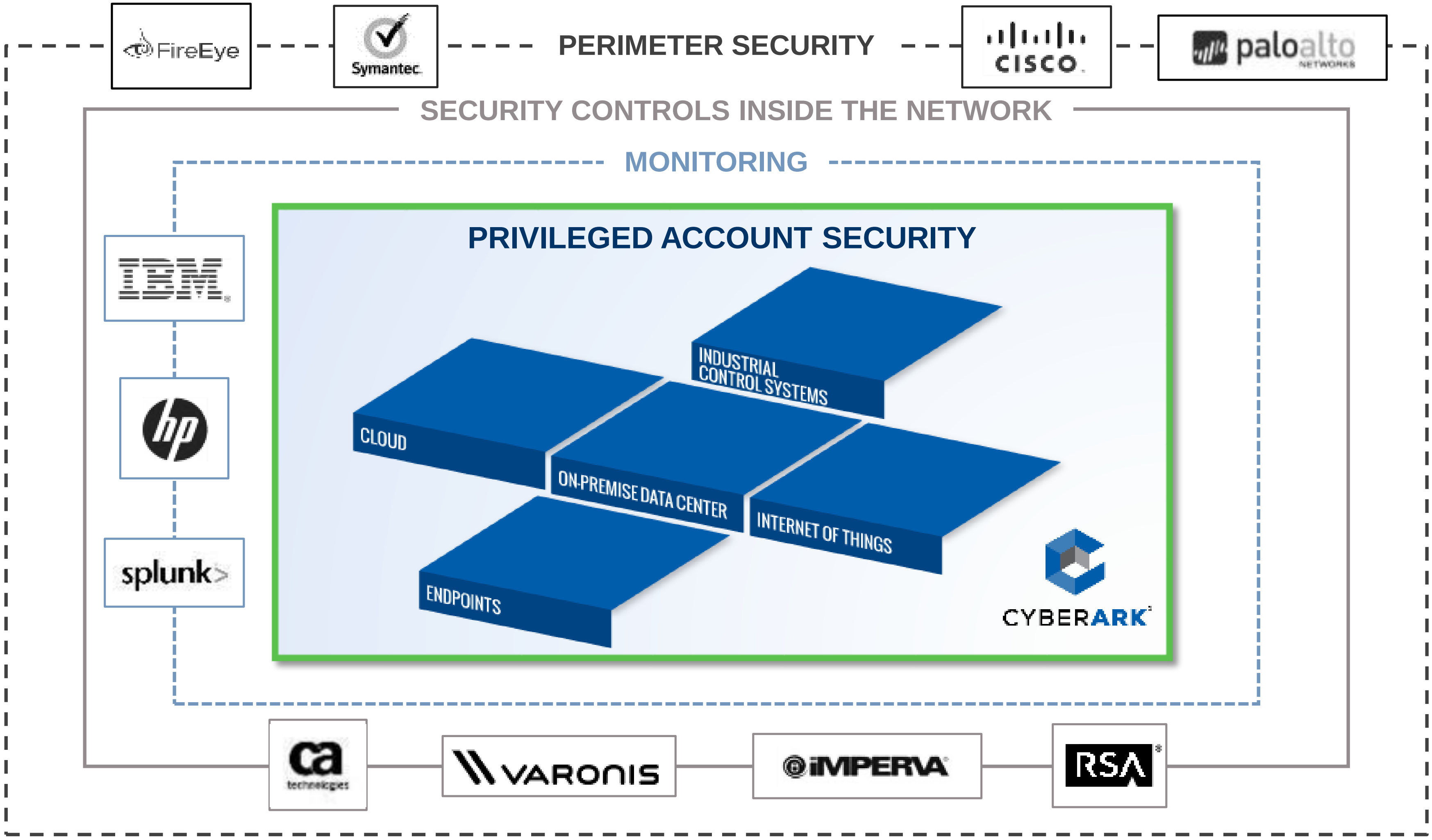
Power Plants, Factory Floors

Routers, Servers, Databases, Applications

WiFi Routers, Smart TVs

Laptops, Tablets, Smartphones

Heart of the enterprise



PERIMETER SECURITY

SECURITY CONTROLS INSIDE THE NETWORK

MONITORING

PRIVILEGED ACCOUNT SECURITY

Attack phases

As defenses evolve, attackers adapt and innovate. In 2014 we observed new and emerging techniques at each stage of the attack lifecycle. These are a few highlights.

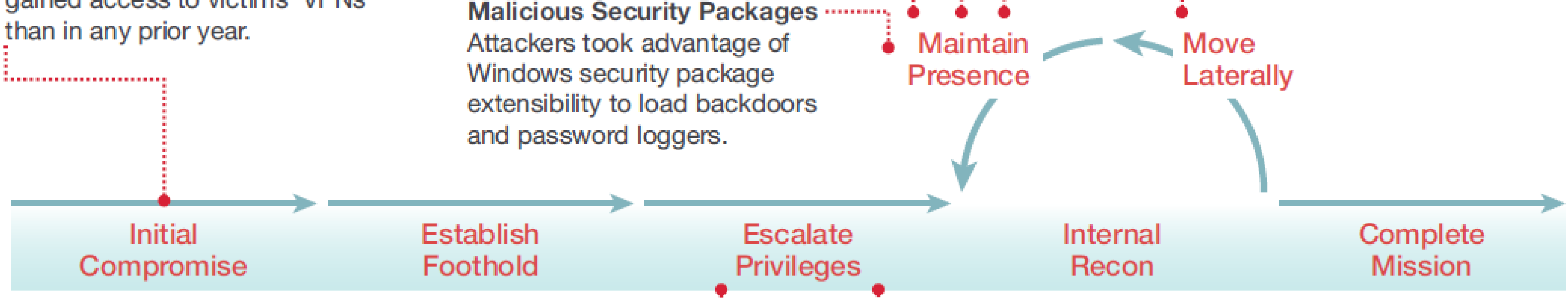
Hiding Webshells
Attackers continued to use novel techniques to deploy and hide web-based malware. Mandiant saw several stealthy techniques, including the following:

- Shells planted on servers that used SSL encryption to evade network monitoring
- Single-line "eval" shells embedded in legitimate web pages
- Server configuration files that were modified to load malicious DLLs

Leveraging WMI and PowerShell
Attackers increasingly adopted WMI and PowerShell, two powerful built-in components of Windows, to maintain a presence, gather data, and move laterally.

Hijacking the VPN
Mandiant witnessed more cases in which attackers successfully gained access to victims' VPNs than in any prior year.

Malicious Security Packages
Attackers took advantage of Windows security package extensibility to load backdoors and password loggers.



Maintain Presence

Move Laterally

Initial Compromise

Establish Foothold

Escalate Privileges

Internal Recon

Complete Mission

Plaintext Passwords
Attackers used recompiled variants of the Mimikatz utility to steal plaintext passwords from memory while evading anti-virus detection.

Kerberos Attacks
After gaining domain administrator privileges, attackers used the Kerberos golden ticket attack to authenticate as any privileged account—even after domain password resets.

Intrusion phases

- Reconnaissance
- Initial Exploitation
- Establish Persistence
- Install tools
- Move Laterally
- Collect Exfil and Exploit

Intrusion phases

- Reconnaissance – **(Business user privileges, Application credentials, System accounts etc.)**
- Initial Exploitation – **(End-user workstation privileges)**
- Establish Persistence – **(Privileged accounts credentials, Kerberos tickets)**
- Install tools – (**End-user workstation privileges, Privileged accounts credentials**)
- Move Laterally – **(Any credentials, SSH keys, Password hashes, KrbTGT)**
- Collect Exfil and Exploit

Intrusion phases

- Reconnaissance
- Initial Exploitation
- **Establish Persistence**
- Install tools
- Move Laterally
- Collect Exfil and Exploit

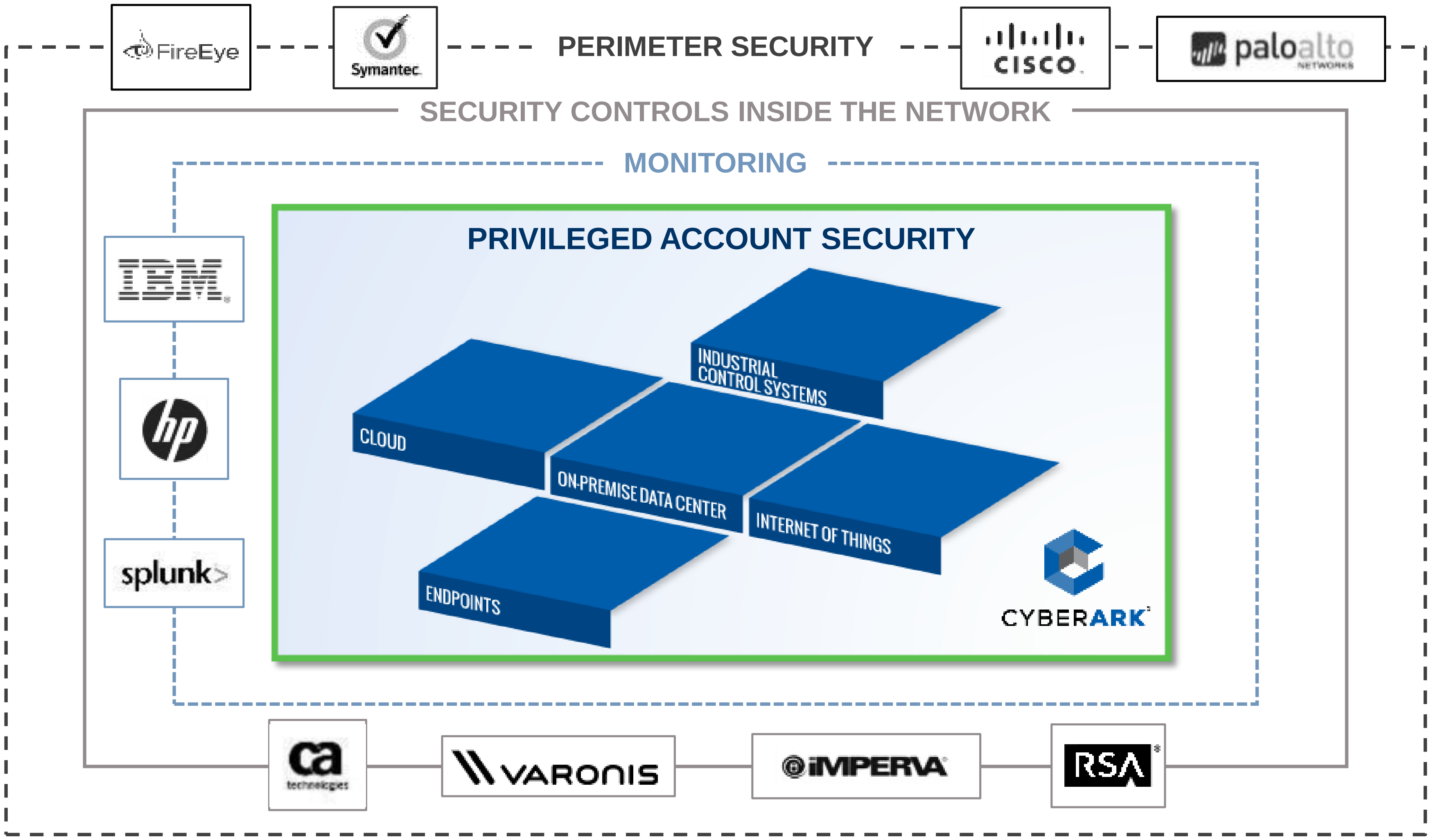
Just an idea

IF YOU’VE BEEN HACKED

MEANS YOU GAVE HACKER PRIVILEGES

TO ATTACK

Heart of the enterprise



PERIMETER SECURITY

SECURITY CONTROLS INSIDE THE NETWORK

MONITORING

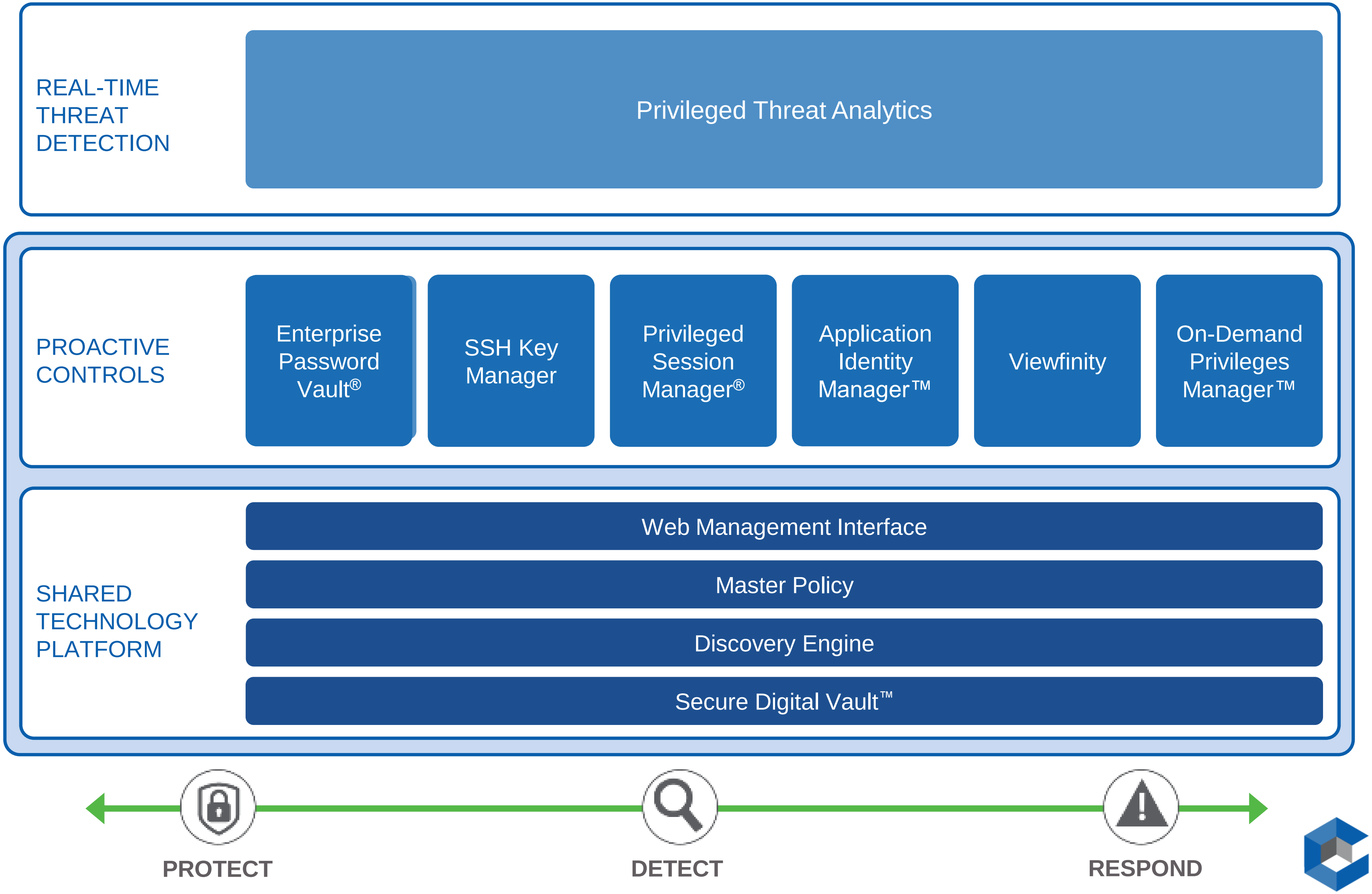
PRIVILEGED ACCOUNT SECURITY

What to do?

- Detect privileges in your company
- Protect privileges in a secure place and control access to them
- Implement and automate password policies for all privileged account types
- Isolate critical assets from the target access
- Control user sessions to critical assets
- Control application sessions to critical assets
- Implement least privileges principle in your company
- Manage and control end-user applications and commands
- Analyze user behavior and react in real time on suspicious activity

- Protect your PRIVILEGES and stop the attack in the beginning

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

THANK YOU

Anton Fridrikh
Anton.Fridrikh@cyberark.com