CYBERARK®

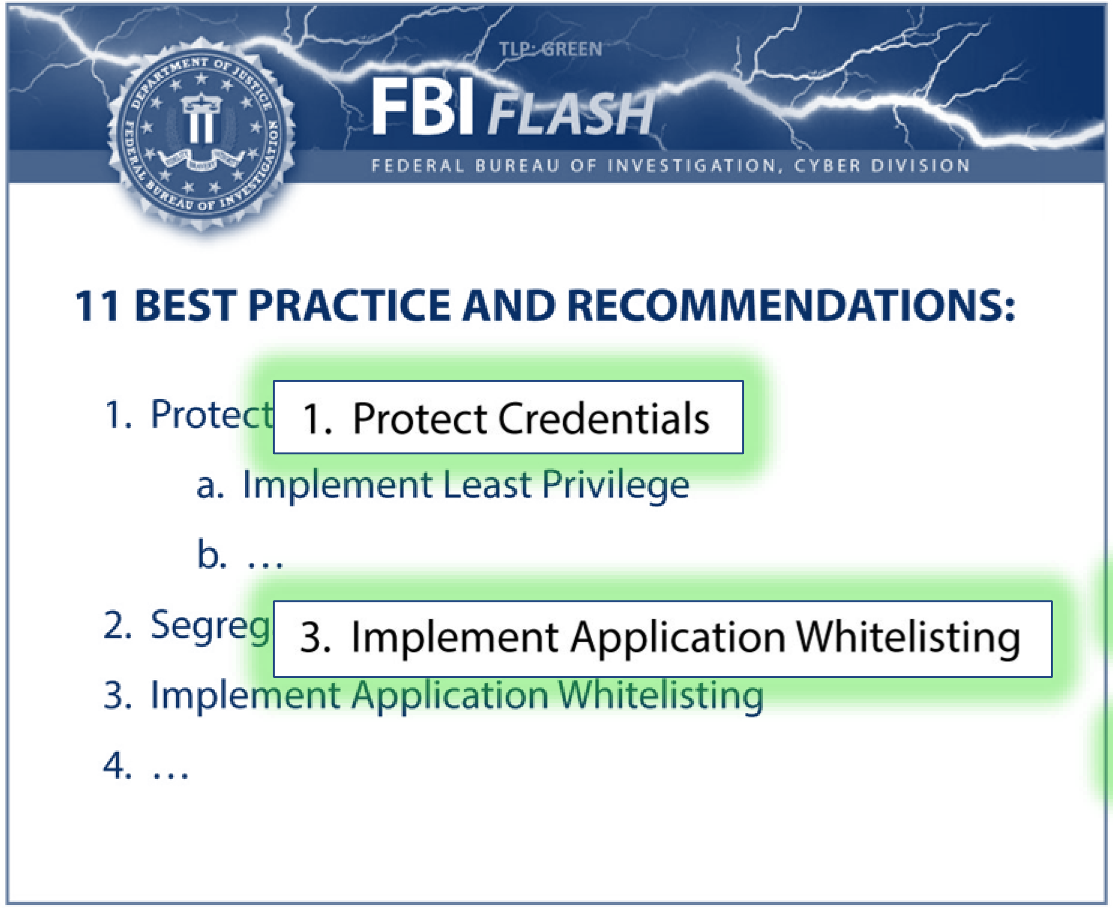
Endpoint Privilege Manager

Managing local administrator privileges and mitigating the risk of malicious software

The Dilemma – Security vs Operational impact

	Users **have** local admin rights	Local admin rights are **removed**
Operations Impact	*Happy, productive users*	*Increased burden on the support team* *Increased calls and costs*
Security Impact	*Increased security incidents*	*Contain attacks on the endpoint*

Three Crucial Capabilities - Top Priority



TLP: GREEN

FBI FLASH

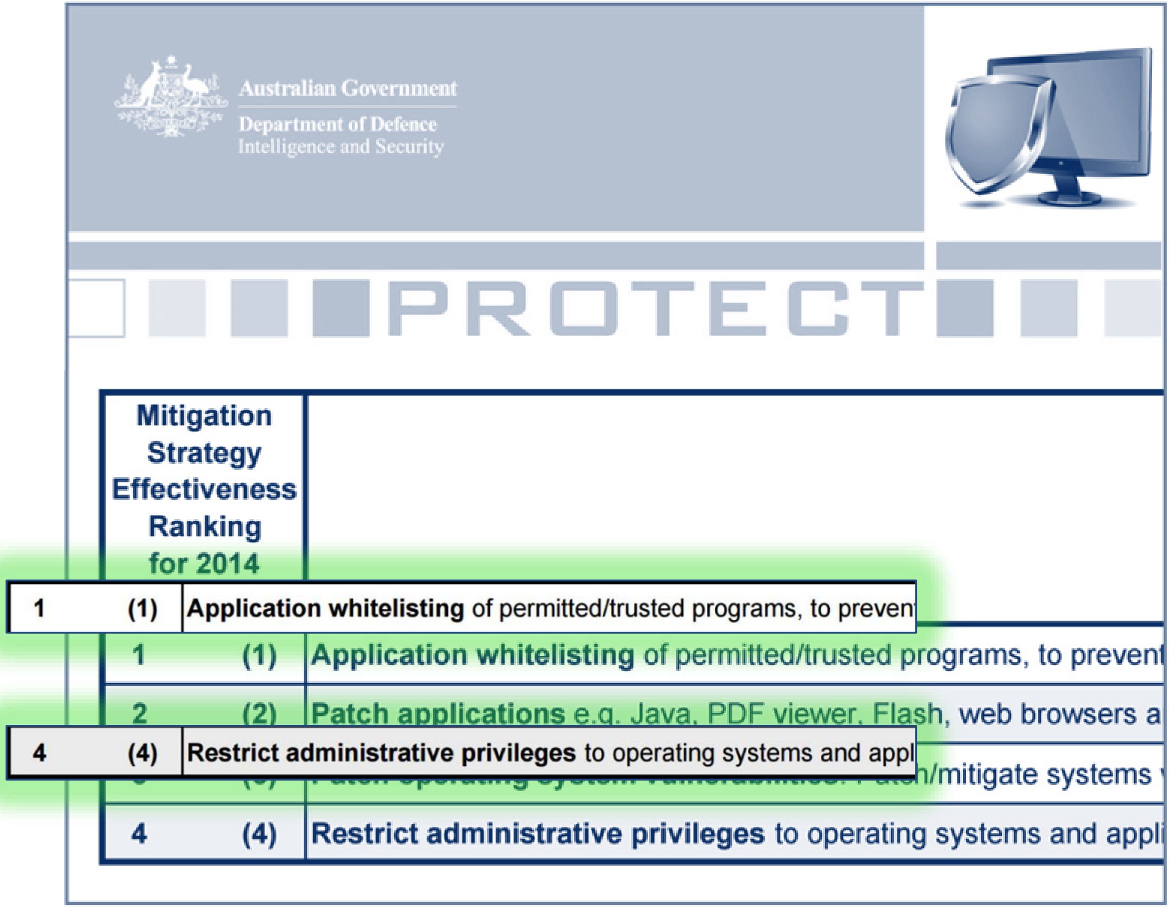
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

11 BEST PRACTICE AND RECOMMENDATIONS:

1. Protect
   a. Implement Least Privilege
   b. …
2. Segreg
3. Implement Application Whitelisting
4. …

1. Protect Credentials

3. Implement Application Whitelisting



Australian Government
Department of Defence
Intelligence and Security

PROTECT

Mitigation Strategy Effectiveness Ranking for 2014		
1	(1)	**Application whitelisting** of permitted/trusted programs, to prevent
2	(2)	**Patch applications** e.g. Java, PDF viewer, Flash, web browsers a
	(3)	**Patch operating system vulnerabilities.** Patch/mitigate systems
4	(4)	**Restrict administrative privileges** to operating systems and appli

1	(1)	**Application whitelisting** of permitted/trusted programs, to preven
4	(4)	**Restrict administrative privileges** to operating systems and appl

Vulnerable Privileges Lead to Compromised Endpoints

CYBERARK®

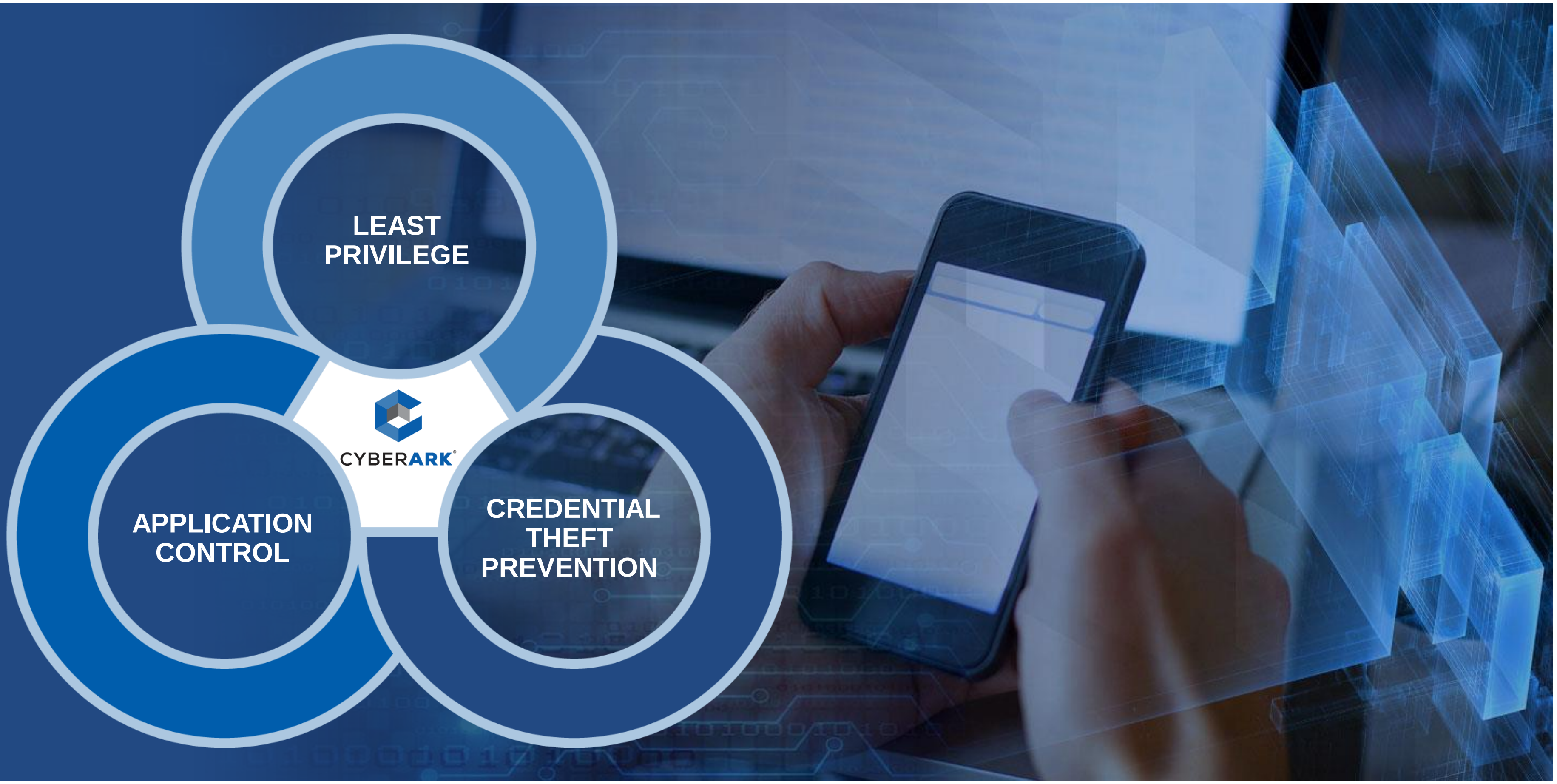
CyberArk Endpoint Privilege Manager

Elevation

Whitelisting

Detection

Prevention



LEAST PRIVILEGE

APPLICATION CONTROL

CREDENTIAL THEFT PREVENTION

CyberArk Labs Ransomware Research

CyberArk Labs tests ~2000 Ransomware samples daily.
Endpoint Privilege Manager has a success rate of:

100%!

The combined solution of

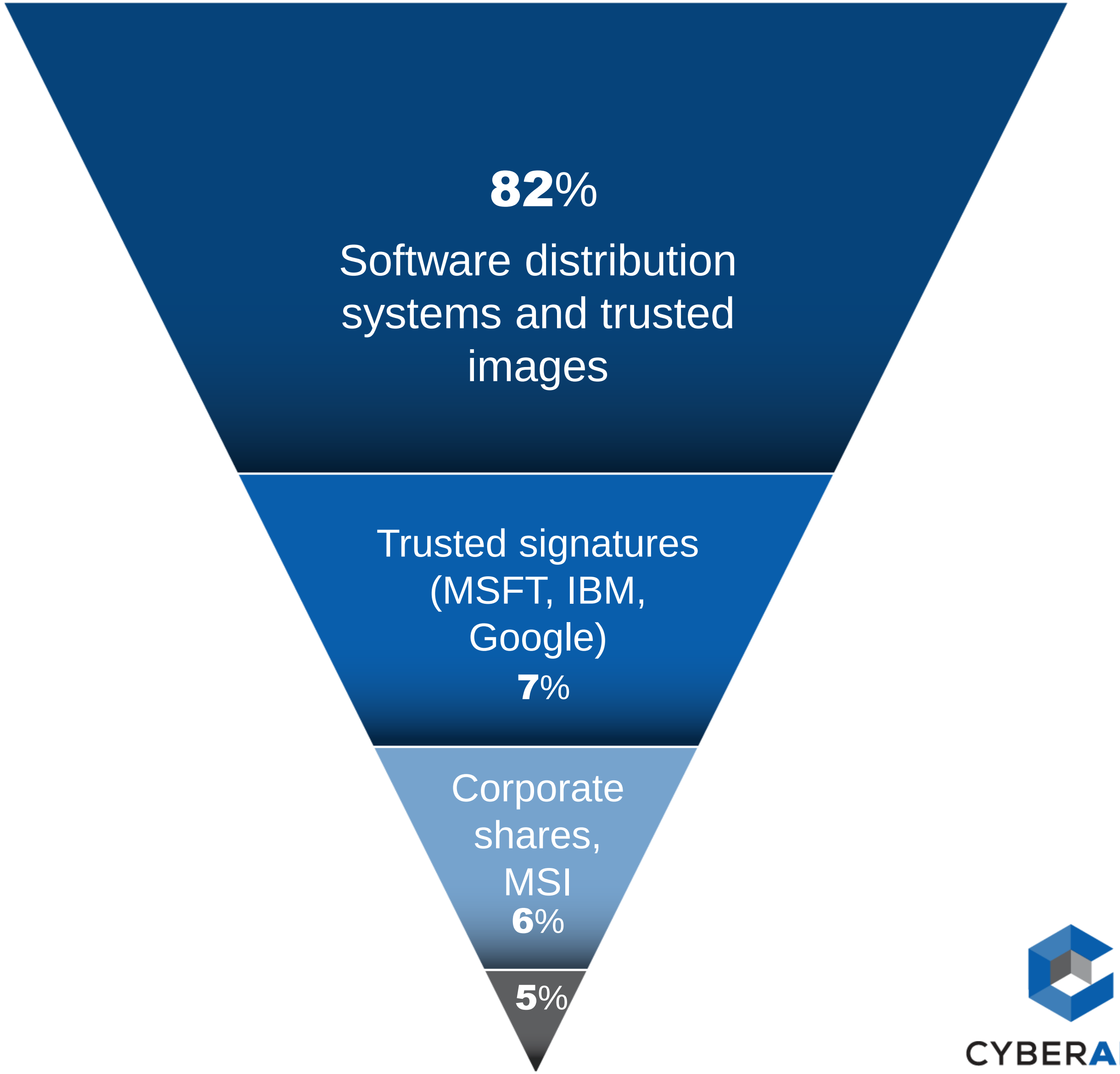
Least Privilege, Application Control, and Credential Theft Prevention

in CyberArk EPM is able to protect sensitive data against **>600,000** out of **>600,000** strains of Ransomware

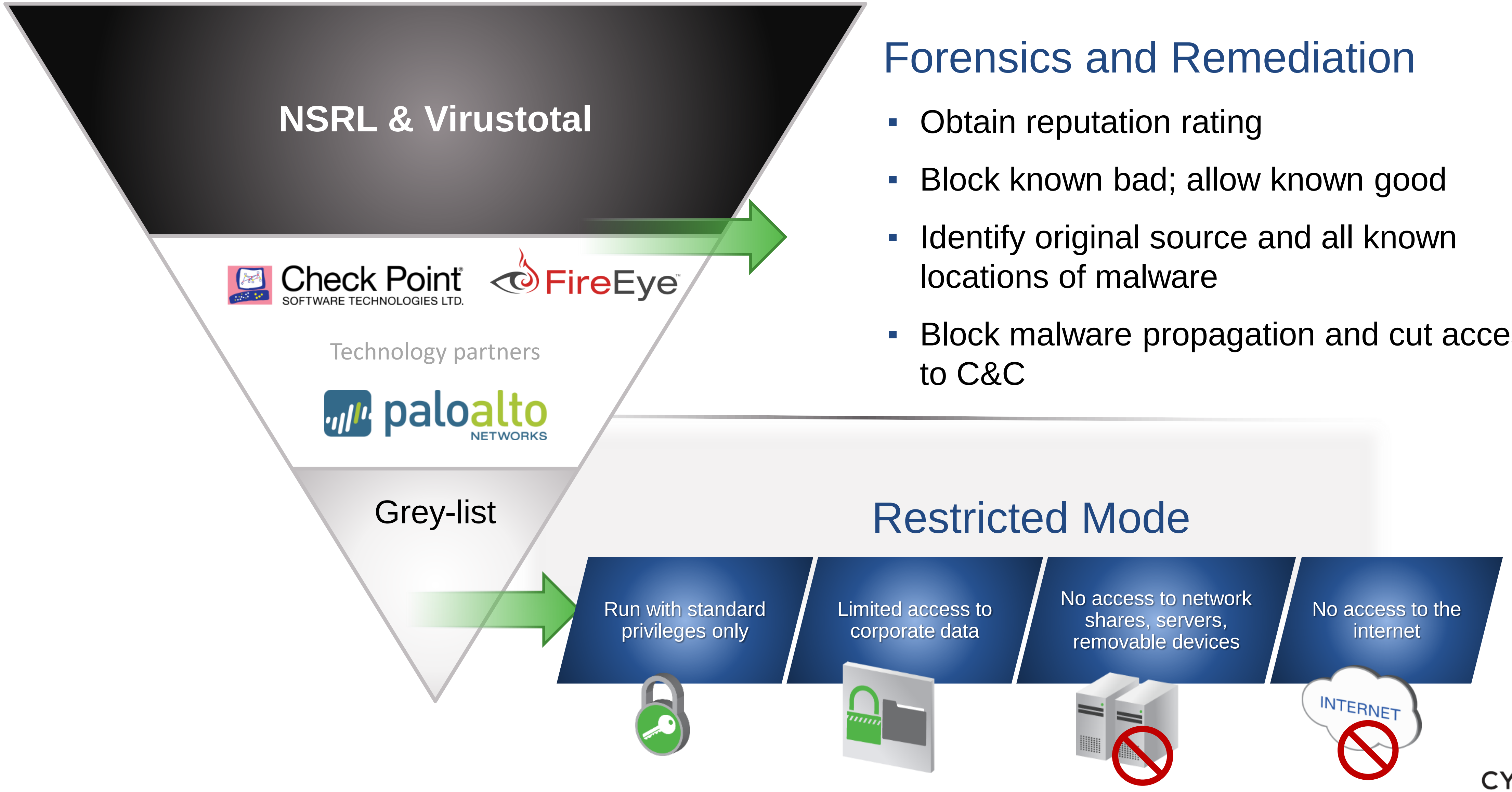
Automated policy creation reduces overhead

Trusted Sources:
policies for **over 95%** of applications can be created and enforced automatically.

- Non-disruptive to end users
- Streamlined deployment
- Efficient on-going management
- Accurate and reliable



What happens to everything else?


NSRL & Virustotal

Technology partners

Grey-list

Forensics and Remediation

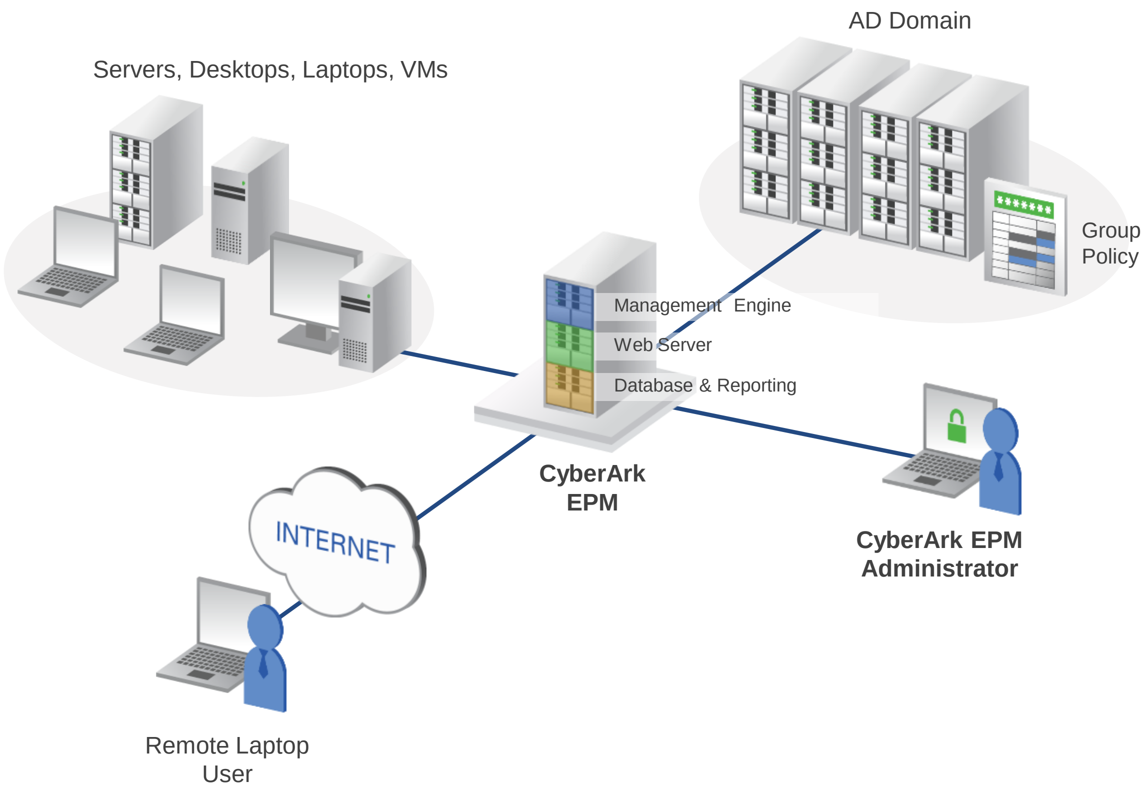
- Obtain reputation rating
- Block known bad; allow known good
- Identify original source and all known locations of malware
- Block malware propagation and cut access to C&C

Restricted Mode

- Run with standard privileges only
- Limited access to corporate data
- No access to network shares, servers, removable devices
- No access to the internet

Flexible Delivery Methods

SERVER-BASED

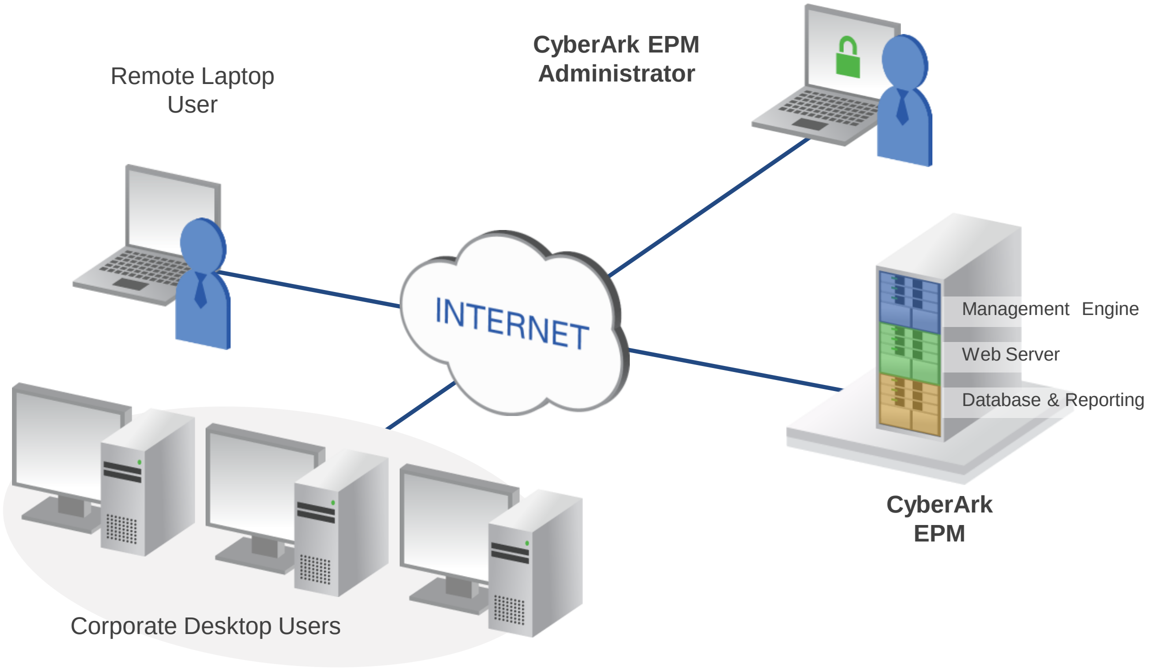


- LDAP-based authentication option to EPM admin console
- Simplified SIEM integration
- FireEye AX integration
- Enhanced integration with other components of the CyberArk suite

Flexible Delivery Methods

- Avoid infrastructure costs and maintenance
- Avoid software costs (SQL, etc.)
- Includes CyberArk Application Risk Analysis Service
- SAML-based authentication option to EPM admin console
- Upgrades are performed automatically – eliminate conversations about features that are not available on outdated versions

PUBLIC CLOUD (SaaS)


Remote Laptop User
CyberArk EPM Administrator
INTERNET
Management Engine
Web Server
Database & Reporting
CyberArk EPM
Corporate Desktop Users