GET YOU ENTERPRISE READY FOR GDPR WITH CYBERARK

David Kellerman

Customer Success Technical Advisor

CYBERARK - TRUSTED ADVISOR

salesforce

ING

vodafone

BT

AEP AMERICAN ELECTRIC POWER

Union Bank
Banking. Simplified.

ANZ

Manulife Financial
For your future

ConAgra Foods
Food you love

3,400+ Global Customers
More than 50% of Fortune 100
More than 25% of Global 2000

THE BUSINESS CHALLENGES OF GDPR COMPLIANCE

CHALLENGES

Structured and unstructured data is growing exponentially

Threat surface continues to grow and evolve

Attackers are becoming more sophisticated

Controllers and Processors *(3rd Party Vendors)* share equal responsibility

KEY GDPR REQUIREMENTS – WHAT YOU NEED TO DO

Article 25 **Article 32 (2)**	Data protection by design and by default	**PROTECT ACCESS** to sensitive personal data
Article 33	Notification of a personal data breach	Detect and **RESPOND RAPIDLY** to breaches early in the attack lifecycle
Article 35	Data protection impact assessment	**ASSESS RISK** and test the effectiveness of data protection processes
Article 82	Protection from non-compliance	**DEMONSTRATE COMPLIANCE** and prove you have the necessary security controls in place

KEY GDPR REQUIREMENTS – WHAT YOU NEED TO DO

Article 25 **Article 32 (2)**	Data protection by design and by default	**PROTECT ACCESS** to sensitive personal data
Article 33	Notification of a personal data breach	Detect and **RESPOND RAPIDLY** to breaches early in the attack lifecycle
Article 35	Data protection impact assessment	**ASSESS RISK** and test the effectiveness of data protection processes
Article 82	Protection from non-compliance	**DEMONSTRATE COMPLIANCE** and prove you have the necessary security controls in place

AN ATTACKER MUST OBTAIN INSIDER CREDENTIALS

"…100% of breaches involved stolen credentials."

"APT intruders…prefer to leverage privileged accounts where possible, such as Domain Administrators, service accounts with Domain privileges, local Administrator accounts, and privileged user accounts."

Mandiant, M-Trends and APT1 Report

DEFAULT PROTECTION PERSONAL DATA

Lock Down Credentials

Protect privileged passwords and SSH keys

Isolate & Control Sessions

Prevent malware attacks and control privileged access

Continuously Monitor

Implement continuous monitoring across all privileged accounts

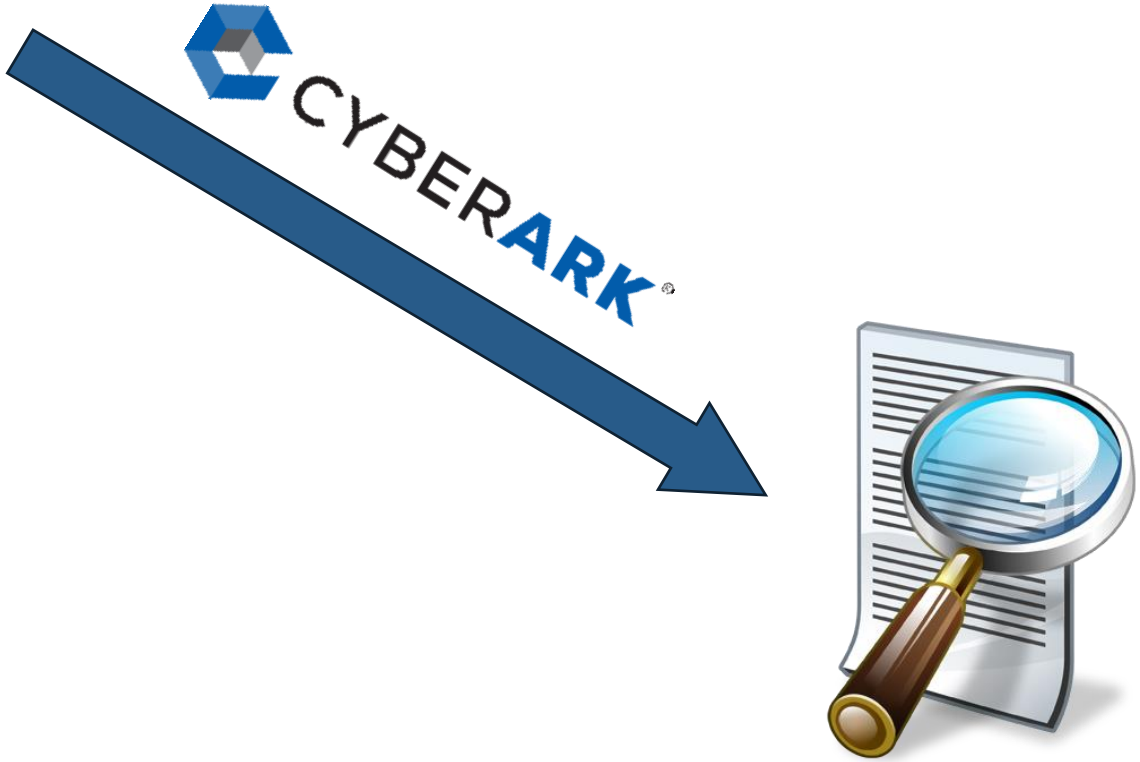
KEY GDPR REQUIREMENTS – WHAT YOU NEED TO DO

Article 25 Article 32 (2)	Data protection by design and by default	**PROTECT ACCESS** to sensitive personal data
Article 33	Notification of a personal data breach	Detect and **RESPOND RAPIDLY** to breaches early in the attack lifecycle
Article 35	Data protection impact assessment	**ASSESS RISK** and test the effectiveness of data protection processes
Article 82	Protection from non-compliance	**DEMONSTRATE COMPLIANCE** and prove you have the necessary security controls in place

“ p3 (a) Nature of personal data breach

(c) Consequences of the breach

(d) Measures Taken to address the breach “



COLLECT AND ANALYZE THE **RIGHT** DATA

CYBERARK®

Microsoft Active Directory

CYBERARK®

PRIVILEGED THREAT ANALYTICS

SIEM

splunk> IBM Radar ArcSight An HP Company

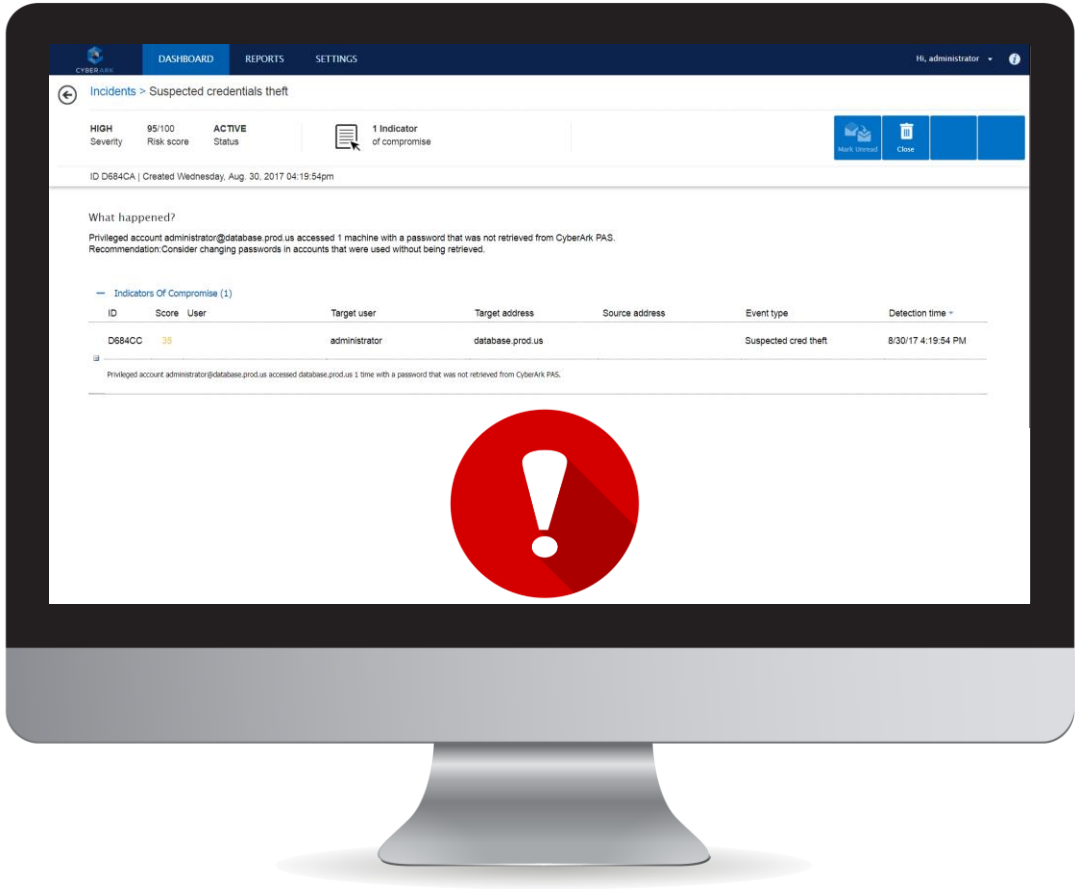
intel Security RSA

NETWORK TRAFFIC

ALERT & RESPONSE
ON SUSPICIOUS ACTIVITY AND BEHAVIOR

- Enable Security teams to prioritize alerts:
  - ✓ Score based risk severity
  - ✓ Granular details about the specific attack
  - ✓ Easy to review by dashboard, email or SIEM

- Automatic response improves security posture and mitigates the risk:
  - ✓ Auto credential rotation
  - ✓ Auto on-boarding of privileged accounts
  - ✓ Minimize damage by stopping attack early
  - ✓ High risk session termination (Auto or Manual)



KEY GDPR REQUIREMENTS – WHAT YOU NEED TO DO

Article 25 Article 32 (2)	Data protection by design and by default	**PROTECT ACCESS** to sensitive personal data
Article 33	Notification of a personal data breach	Detect and **RESPOND RAPIDLY** to breaches early in the attack lifecycle
Article 35	Data protection impact assessment	**ASSESS RISK** and test the effectiveness of data protection processes
Article 82	Protection from non-compliance	**DEMONSTRATE COMPLIANCE** and prove you have the necessary security controls in place

COMMON TYPES OF RISK ASSESSMENT

VULNERABILITY ASSESMENTS

PENETRATION TESTING

RED TEAMING

BENEFITS OF CYBERARK RISK ASSESSMENT

Measure the Risk of Critical Assets

Uncover Known Vulnerabilities

Identify Strengths and Weaknesses

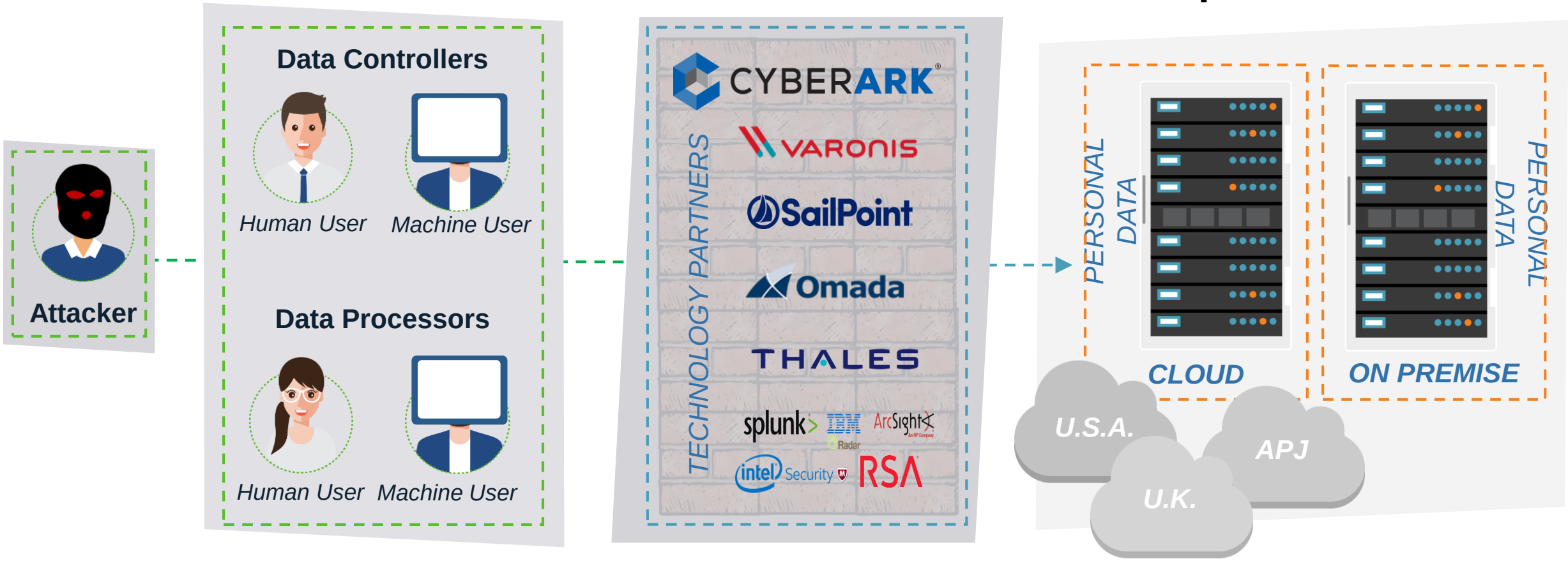
Measure Improvement Over Time

KEY GDPR REQUIREMENTS – WHAT YOU NEED TO DO

Article 25 **Article 32 (2)**	Data protection by design and by default	**PROTECT ACCESS** to sensitive personal data
Article 33	Notification of a personal data breach	Detect and **RESPOND RAPIDLY** to breaches early in the attack lifecycle
Article 35	Data protection impact assessment	**ASSESS RISK** and test the effectiveness of data protection processes
Article 82	Protection from non-compliance	**DEMONSTRATE COMPLIANCE** and prove you have the necessary security controls in place

PRIVILEGED ACCESS SECURITY (PAS) IS KEY TO COMPLIANCE

1. Protect Access
2. Respond Rapidly
3. Assess Risk
4. Demonstrate Compliance



Security works as a Team

CYBERARK

C³ Alliance

+70 Certified Parters

aqua, CHEF, Devolutions, ForeScout, illusive, Omada, RADIANT LOGIC, STEALTHbits TECHNOLOGIES, UiPath, docker, FORTINET, Informatica, onelogin, RAPID7, SyferLock, utimaco, Atos, cloudbees, DUO, GE Power, intel, paloalto NETWORKS, redhat, Symantec, VARONIS, AUTOMATION ANYWHERE, CyberX, Eracent, gemalto, IP SOFT, PHANTOM Technology Solutions, RSA, VENAFI, blueprism, evidian, iQuate, talend, VISTARA, datablink, HEXADITE, proofpoint, SailPoint, bmc, EZMCOM, SONAR, tenable, WATERFALL, SECUREAUTH, cavirin, NETWORKS, Hewlett Packard Enterprise, puppet, THALES, WorkFusion, FireEye, LogRhythm, servicenow, Check Point, DBmaestro, Flexera, IBM, okta, Qualys, splunk>, tripwire, yubico

+100 Certified Joint Solutions

Analytics	Authentication	Detection	DevOps	Discovery	Governance	HSM
ICS	Identity & Access Management	ITSM	Orchestration & Response	Robotic Process Automation	SIEM	Vulnerability Management

+200 Plug-ins

CPM Plug-ins	PSM Plug-ins

KEY GDPR REQUIREMENTS – WHAT YOU NEED TO DO

Article 25 **Article 32 (2)**	Data protection by design and by default	**PROTECT ACCESS** to sensitive personal data
Article 33	Notification of a personal data breach	Detect and **RESPOND RAPIDLY** to breaches early in the attack lifecycle
Article 35	Data protection impact assessment	**ASSESS RISK** and test the effectiveness of data protection processes
Article 82	Protection from non-compliance	**DEMONSTRATE COMPLIANCE** and prove you have the necessary security controls in place

THANK YOU!