



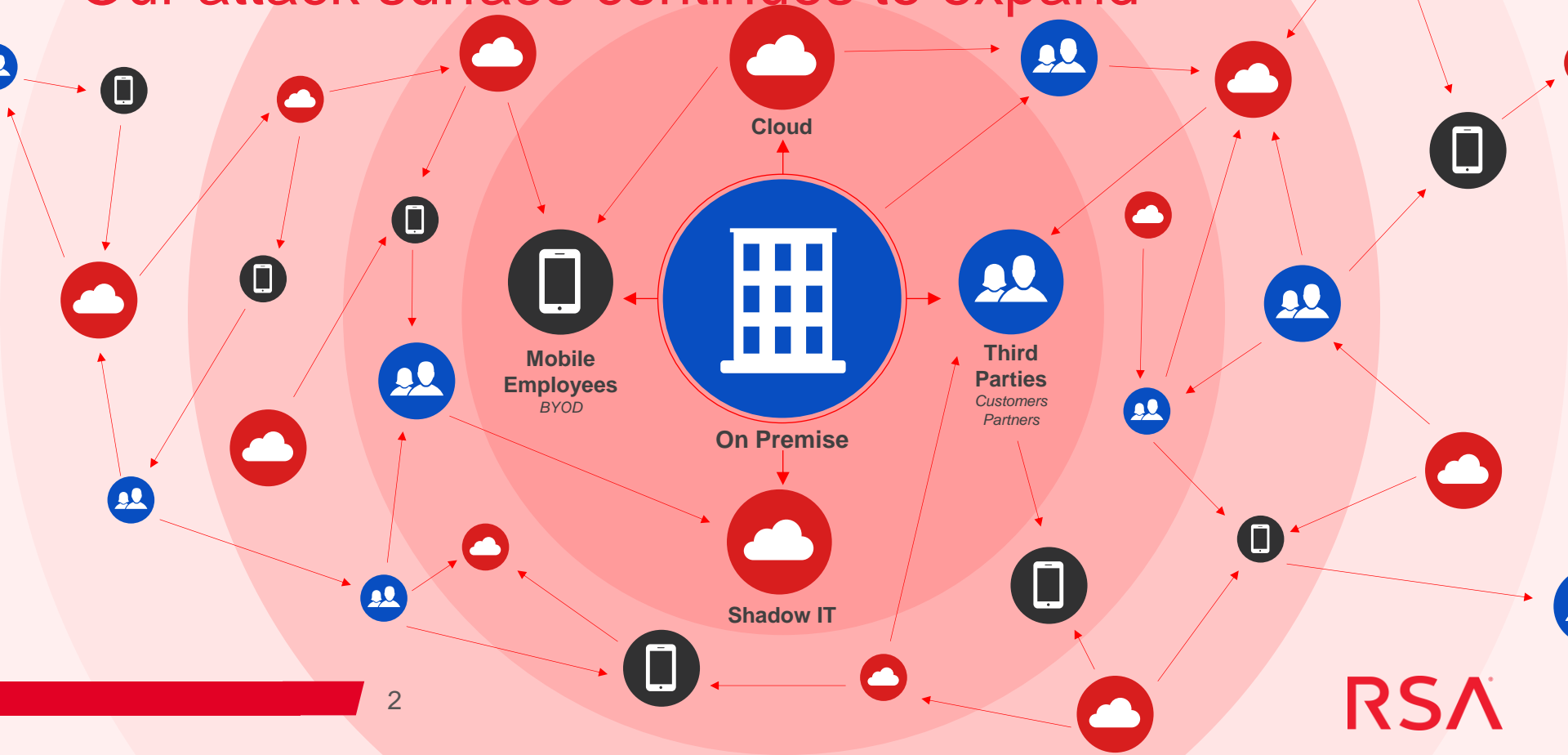
Effective Cyber Security: the strategy of detection, analysis and response

DR. ROBERT W. GRIFFIN
CHIEF SECURITY ARCHITECT
RSA, THE SECURITY DIVISION OF EMC



RSA

Our attack surface continues to expand



The capabilities that matter most now



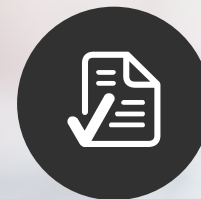
Visibility & Analytics

*establish foundation /
make responders
faster & smarter*



Identity Assurance & Governance

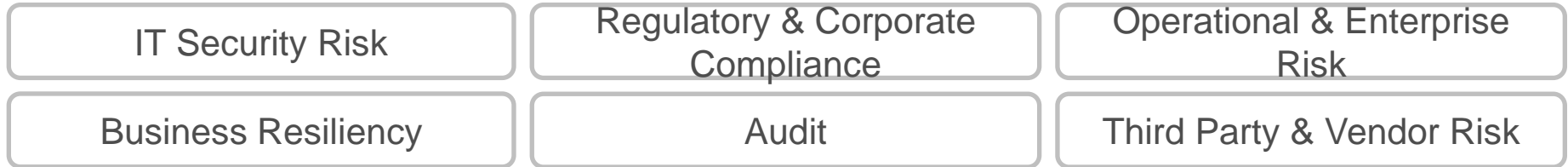
*address the
most consequential
attack vector*



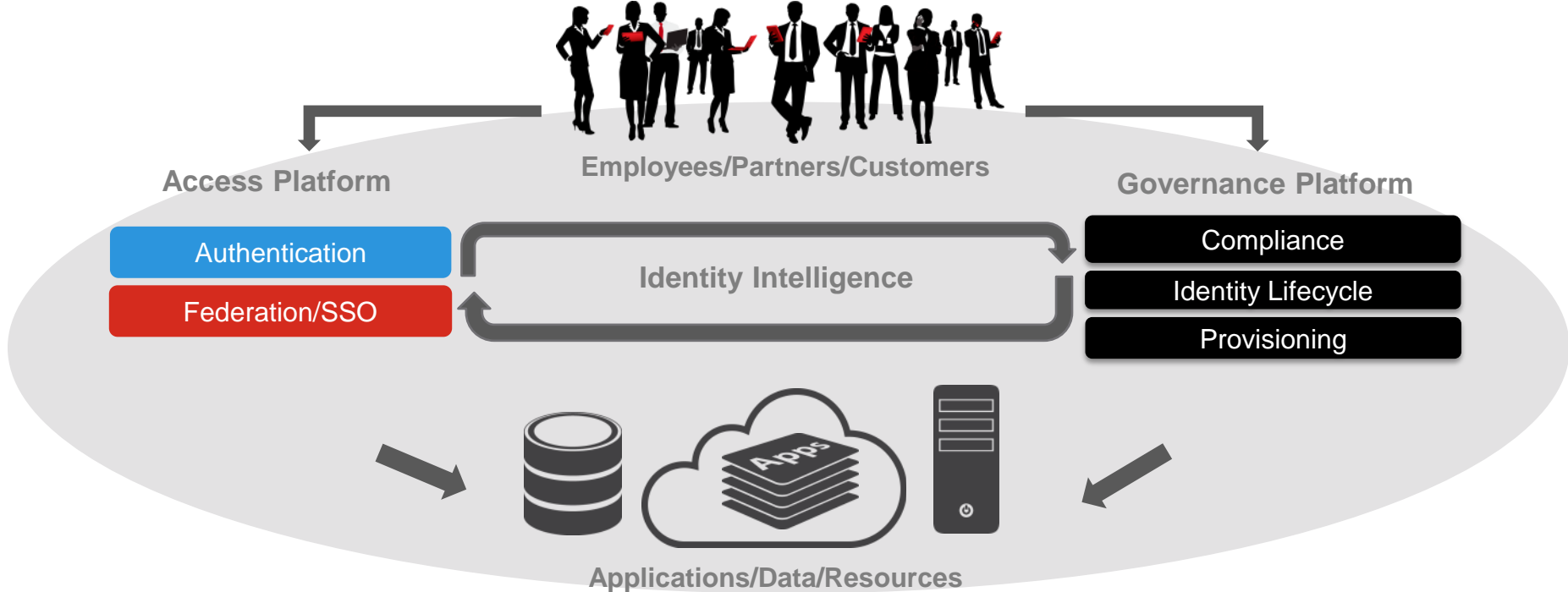
Risk Intelligence

*prioritize
effectively*

Risk Intelligence across the Organization



Identity Assurance and Governance



Visibility and Analytics

PACKETS



LOGS



ENDPOINT

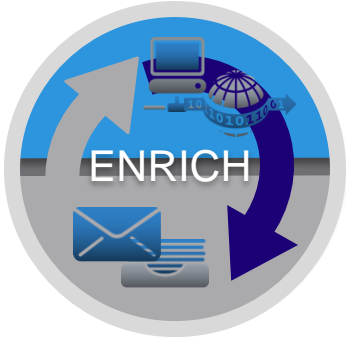


NETFLOW



VISIBILITY

Capture Time
Meta-Data Enrichment



ANALYSIS



Hadoop-based Analytics



Archiving

ACTION



Incident Management



Compliance



Investigation



Session
Reconstruction



Advanced Analytics



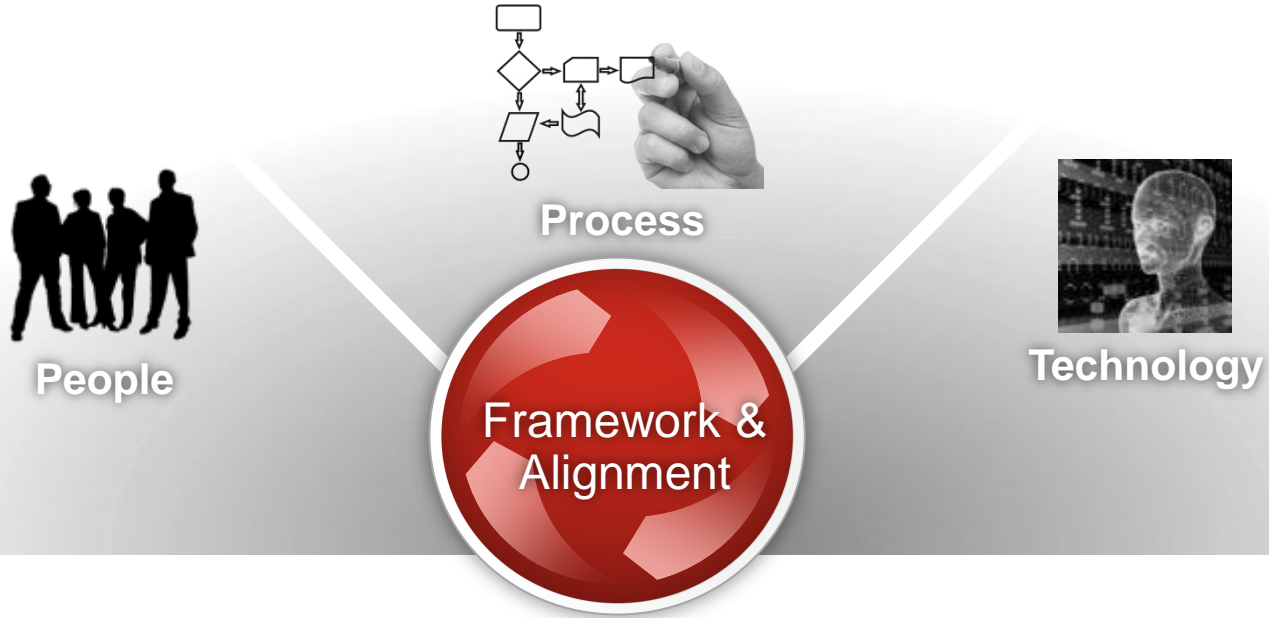
Endpoint Analysis

INTELLIGENCE



Threat Intelligence | Rules | Parsers | Feeds | Reports | Research

Advanced Security Operations Center



**Incident
Response**

**Breach
Response**

**ASOC Program
Management**

Thank You!

robert.griffin@rsa.com

[*blogs.rsa.com/author/griffin*](https://blogs.rsa.com/author/griffin)
[*project-sparks.eu/blog/*](https://project-sparks.eu/blog/)

[*@RobtWesGriffin*](#)

[*www.linkedin.com/pub/robert-griffin/0/4a1/608*](https://www.linkedin.com/pub/robert-griffin/0/4a1/608)