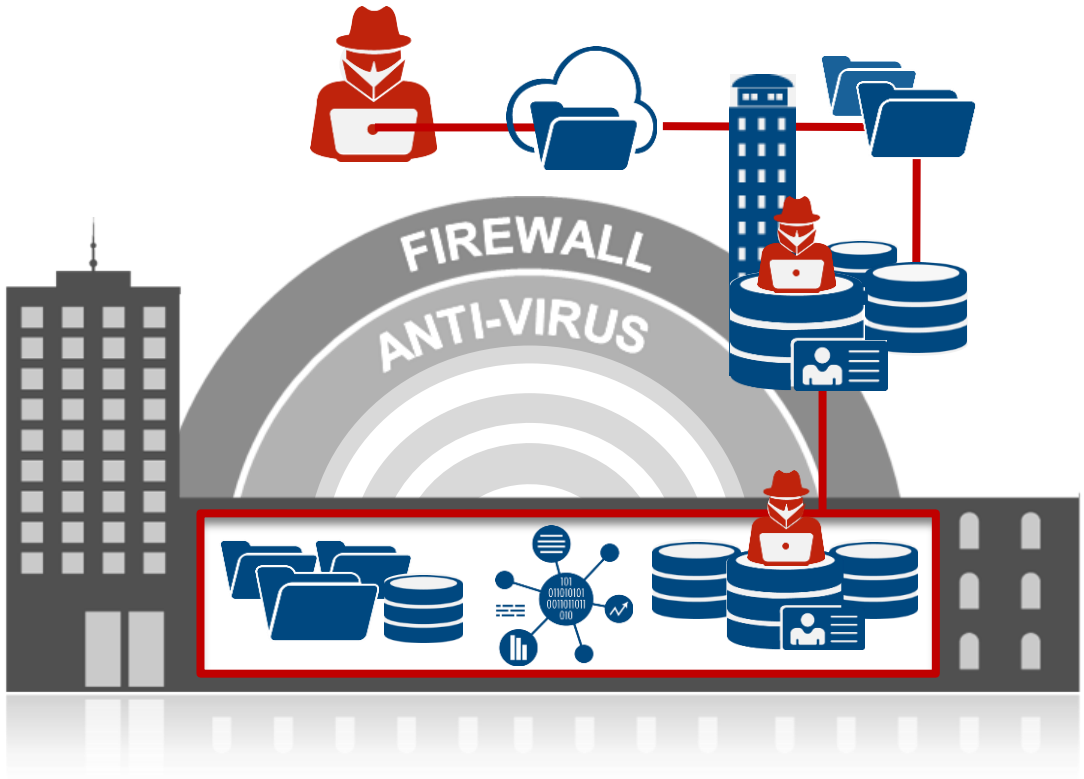
IBM Security

Intelligence. Integration. Expertise.

IBM

Security Starts from the Inside

What's on the inside counts



55% of all attacks are caused by insider threats**

Damaging security incidents involve loss or illicit modification or destruction of sensitive data

Many security programs only focus on what's happening beyond the perimeter

**Source: 2Q15 X-Force Report

Who is an Insider?

Unsuspecting Employees

Attackers

Frequent threats

81%

used someone else's credentials to bypass controls or gain elevated rights

Disgruntled/Malicious Employees

Enterprise users

Evasive perpetrators

79%

of the time a privileged user altered and then reset application controls to avoid detection

Partners/Contractors

Third-party actors

Long response times

87 days

on average to recognize that insider fraud has occurred

Insider Risk can also be business risk

Volkswagen Emissions Scandal: German Carmaker Faces Legal Action In China, India

DraftKings, FanDuel Sued Over Fantasy Sports Scandal

The class-action suit accuses the two companies of fraud and negligence, among other charges.

Sources: International Business Times (VW) and Huffington Post (DK and F)

How are most companies combating insider threats today?

62% **of organizations do not monitor and audit the actions of users with privileges more closely than non-privileged users***

57% **of organizations do not have a data security solution that supports entitlement reporting**

Stop the madness!!

**According to a 2015 UBM study of more than 200 organizations*

Getting Started: Know your users, know your data

Know your users

1. Who has access to sensitive data?
2. Who should have access?
3. What are end users doing with data?
4. What are administrators doing with data?

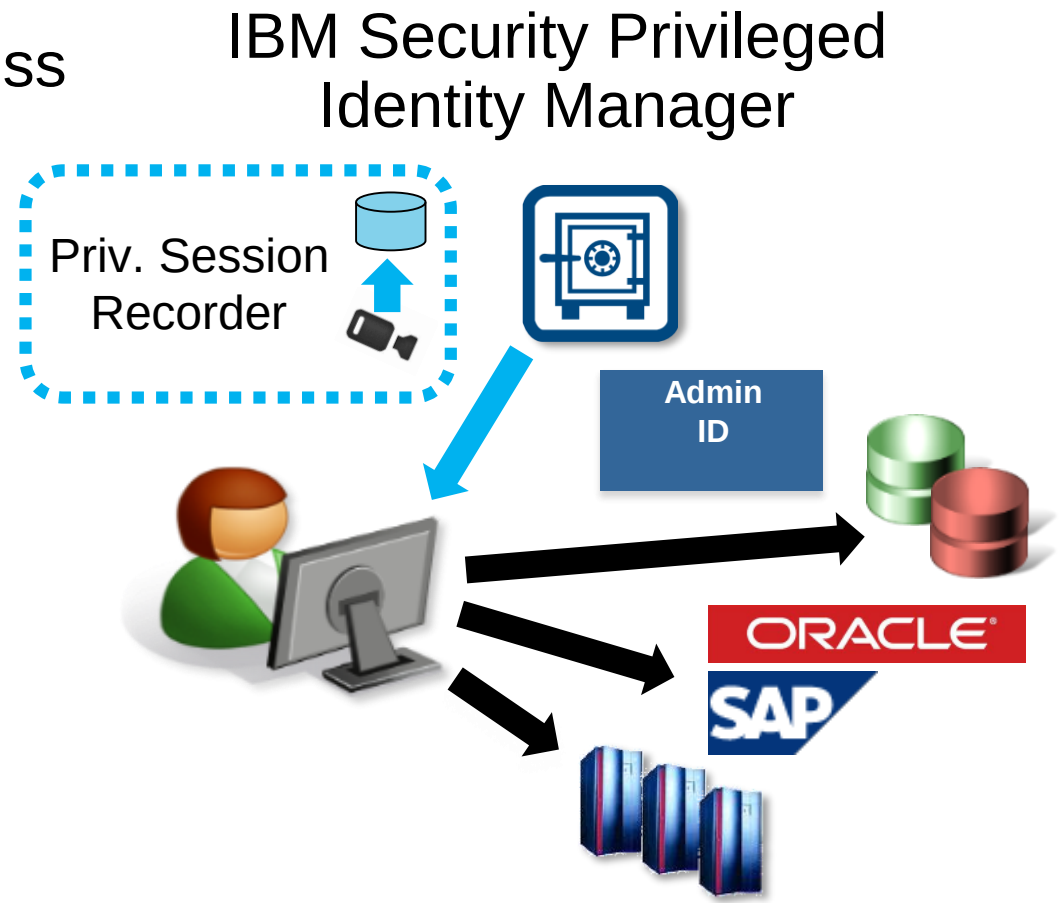
Know your data

1. What data is sensitive?
2. Is the right sensitive data being exposed?
3. What risk is associated with sensitive data?
4. Can you control privileged user access to sensitive data?

Know your Privileged Users

Manage shared access and session recording for compliance

Record monitor what privileged users are doing

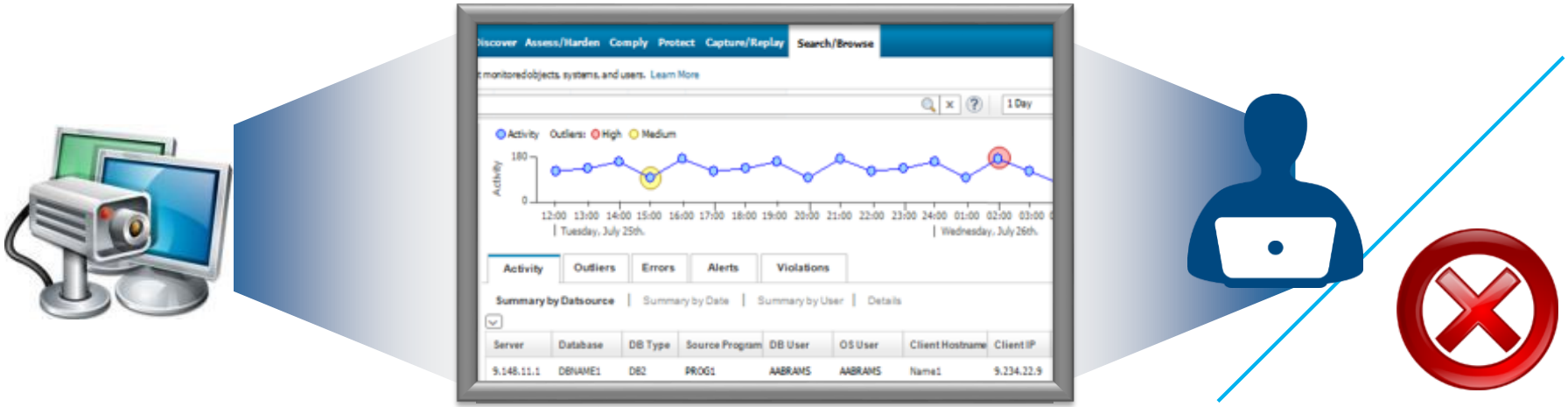


Identity & Access Management – Know your regular users

Govern and administer users and their access

Know your data – IBM Guardium

Apply machine learning & intelligence to uncover behavioral changes and risks



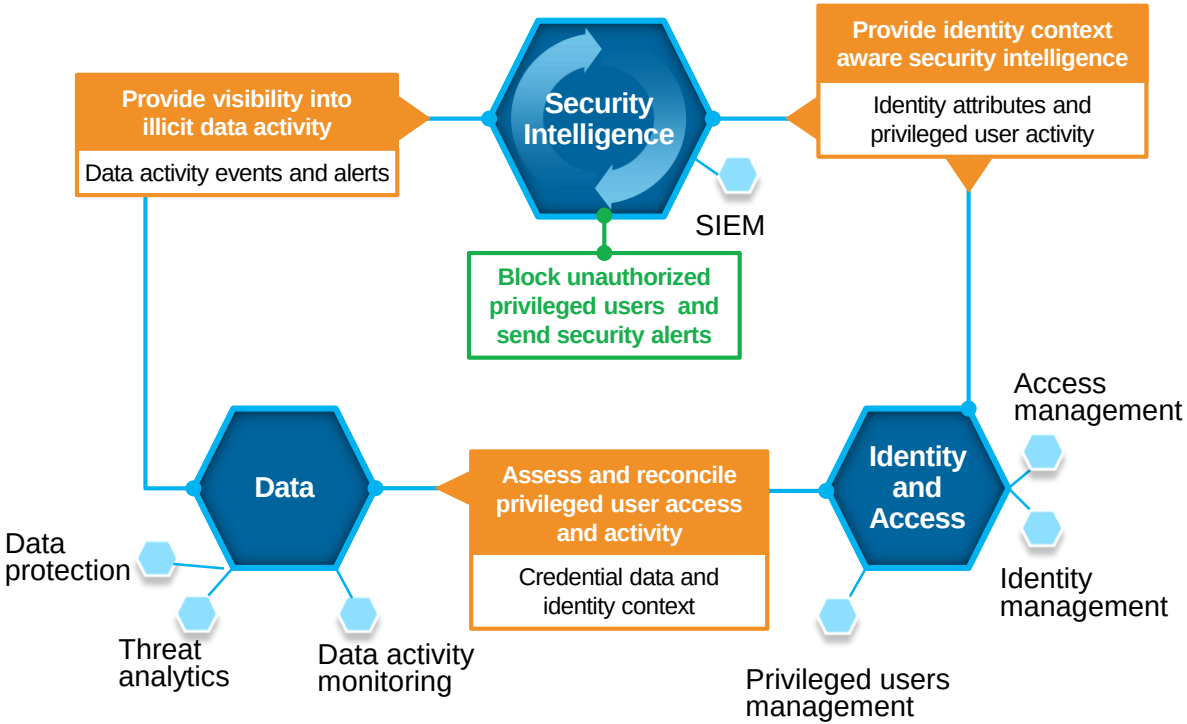
1. Policy-based, real-time monitoring* reveals behavior patterns over time

2. Analytics run and anomalies are surfaced

3. Anomalies are sent for manual review OR triggers action

**including tions by privileged users*

A connected environment helps stop insider threats



Integrated Value

- Provide privileged user information and manage user credentials
- Understand what, where and when sensitive data is accessed
- Detect unusual activity and make corrections to block and prevent

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM Security

Intelligence. Integration. Expertise.