



Highlights

- Reduces your exposure by helping to secure your data and govern your user identities
 - Helps anticipate the risk of malicious user actions before they occur with behavior analytics
 - Delivers actionable intelligence to help you respond promptly if there is a breach and recover the compromised data
-

Insider threat protection services from IBM

Gain an edge over insider threats with actionable intelligence

To protect your organization from information theft, IT sabotage or fraud, it is critical to address security gaps that could be exploited. Insiders in particular can take advantage of their easy access to your most valuable information, which can cause irreparable harm to your organization. In fact, 60 percent of attacks against enterprises in 2015 were committed by insiders.¹

IBM® Identity and Access Management Services for insider threat protection offer an integrated approach to your organization's defense. The offering grants greater insight into how and why insider attacks occur by focusing on the identities and behaviors of your users as they access your most valuable data. This helps ensure you are adequately protecting your data, governing user identities and understanding users who hold the potential for the greatest damage. As a result, our experts help predict malicious user behavior before it occurs, and you can act before any data is lost. Guarding against insider threat means preserving brand value and customer trust, defending your business from financial losses and costly interruptions.

Reducing your exposure by helping to secure your data and govern your identities

Gaining visibility into security gaps you might have is crucial to safeguarding your most valuable information. An IBM advisor works with you to help identify where your most valuable data is located, how it is accessed and by whom, creating a robust map of its access pathways. This helps you verify that you have protected critical information with the appropriate access controls, and adequately governed your privileged and golden users, such as executives, brokers or other critical individuals.



Anticipating malicious actions before they occur with behavior analytics

Identifying the privileged or golden users who have access to your data is just the first step in your defense against insider threats. Once users are identified, available corporate data is analyzed to determine whether a user is at-risk of becoming a malicious insider. When coupled with the user's transaction patterns, suspicious activity that might be indicative of an inappropriate action by an insider can be detected. Your trusted IBM advisor can help identify individual transactions or individual users that exhibit unusual behavioral patterns, prioritizing which elements merit further investigation.

Responding promptly in case of a breach to help recover compromised data

Collecting intelligence on insiders who have access to your most valuable information is necessary to determine when a breach occurs and by whom. Knowing who your users are and their typical behavior helps you pinpoint when an insider takes an inappropriate and harmful action against your organization. This program helps provide the information you need to protect your organization against insiders who might cause irreparable harm to your organization.

Why IBM?

With virtually unparalleled identity and access management (IAM) and data security expertise, IBM can provide the benefits of a trusted advisor to augment your security staff. Backed by IBM research and development resources, the large data set of IBM X-Force® command centers and managed security services clients, IBM Security specialists can offer the business, data and IAM security experience to help you evaluate intelligence, draw more meaningful conclusions and prepare for next steps.

For more information

To learn more about insider threat protection services from IBM, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security/insider-threat-protection

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing



© Copyright IBM Corporation 2016

IBM Global Services
Route 100
Somers, NY 10589

Produced in the United States of America
November 2016

IBM, the IBM logo, ibm.com, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

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 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.

¹ [IBM X-Force Research 2016 Cyber Security Intelligence Index report](#)



Please Recycle