IBM Security Access Manager

Take back control of access management with an integrated platform for web, mobile & cloud

Highlights

- Allows organizations to bridge the access control gap between on-premise and cloud environments.
- Enables the mobile enterprise with mobile access control policies that integrate with mobile device management, application development and malware detection solutions.
- Protects critical assets using access control policies, including risk-based and multi-factor authentication.
- Delivers simplified and secure user experiences with single sign-on across applications, irrespective of whether applications are hosted on-premise or in the cloud.
- Reduces cost and time to value by helping secure access to applications and workloads, including web, mobile, cloud, and APIs, with a single integrated appliance.
- Provides access control for external applications by scaling for large user bases, and delivering built-in protection against application threats.

Many organizations face access management chaos. As applications and resources have spread across on-premise datacenters and multiple cloud providers, users are often accessing these resources from anywhere and on multiple devices. These simultaneous trends have left access management systems fragmented and access polices inconsistent, resulting in an environment that is expensive to maintain and challenging to secure.

IBM® Security Access Manager allows organization to take back control of their access management system with a single integrated platform that manages access across many common scenarios. Access Manager helps secure access points into the corporate network and enforce risk-based access policies that define who and what can access protected resources. The solution is a modular platform for web access management, web application protection, mobile access management, cloud access management, risk-based access and identity federation. The integrated appliance form factor allows for easy and flexible deployment and maintenance.

Access Manager helps centrally secure internal and external user access points into the corporate network from web and mobile channels. Highly scalable and configurable, the solution is designed to provide a policy-based user authentication and authorization system that helps defend against the latest web-based security threats.

IBM Security Access Manager delivers a security appliance that helps secure user access and protect content against common web attacks. Key benefits include:

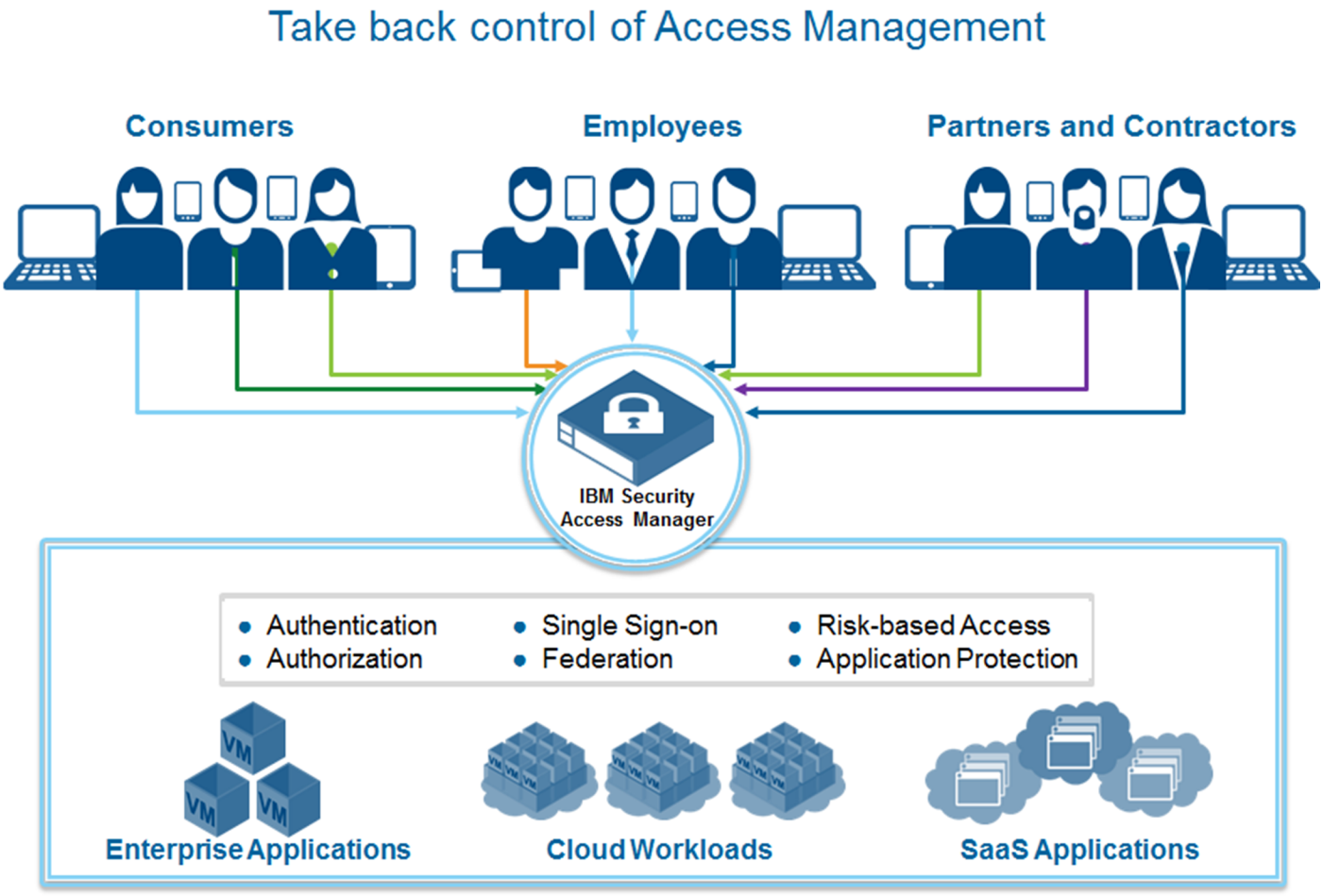
- Enhanced user productivity while ensuring secure user access to web and mobile applications through single sign-on (SSO), session management, strong authentication, and context-based access policy enforcement.
- Federated single sign-on (SSO), which helps enhance user productivity and facilitates trust through the delivery of SSO across separately managed domains, including easily configurable connections to popular software as a service

(SaaS) applications.

- Integration with IBM MobileFirst Platform, IBM MobileFirst Protect (formerly, MaaS360 by Fiberlink, an IBM company), IBM Security Trusteer Fraud Protection for easier mobile access development and rich mobile context for access decisions.
- Better protection from advanced threats including OWASP top 10 web application risks.

Access Manager is structured as a platform with two optional add-on modules as detailed below. All required code is included with the base appliance and customers enable add-on module functionality by entering the appropriate activation keys. This allows users the flexibility to more easily support many usage scenarios while minimizing the additional software required.

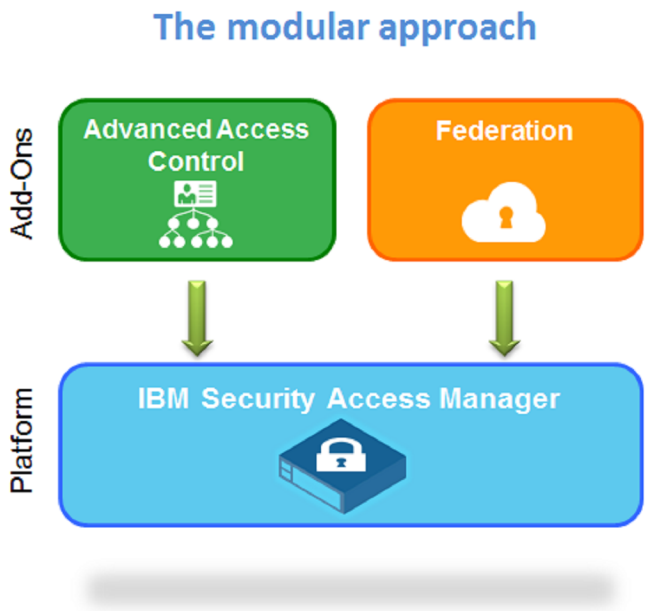
Web applications are often subject to repeated attacks by external and internal attackers seeking to acquire valuable content.



One platform offering, with easily consumable add-on modules

IBM Security Access Manager is a modular, integrated access management appliance that helps secure access to web, mobile, and cloud workloads. The integrated appliance form factor allows for easier and more flexible deployment and maintenance. It is offered both as a physical appliance and as a virtual appliance image that runs on a number of popular hypervisors.

According to the Open Web Application Security Project (OWASP) top 10 list of web vulnerabilities, external hackers use SQL injections, broken authentication, and cross-site scripting (XSS) as common methods to gain unauthorized access into the web applications. By utilizing research from the IBM X-Force threat research team, Access Manager delivers the ability to help block OWASP top 10 web vulnerabilities before they reach the targeted application.



Access Manager Advanced Access Control Module

According to the IBM X-Force Security and Risk trend report, attackers use phishing attacks and social engineering to compromise end-user access to gain unauthorized access into corporate applications. Identity fraud and bring your own device (BYOD) are growing concerns for enterprises, as they expand their web application reach into mobile, business partner, and social collaborations.

In the face of these challenges, it is important to bring increased intelligence to authentication and authorization. The Advanced Access Control Module allows Access Manager to use detailed contextual information (for example, geographic location, device fingerprint, browser type, application data, and so forth) about the user making the access request when making access decisions.

Advanced Access Control Module key capabilities:

- Risk scoring engine to enforce context-aware authorization using information about the users, their mobile devices, and other transactions-based information.
- Mobile sign-on, session management, and an authentication service for supporting multiple strong authentication schemes, for example, one-time password, and Short Message Service (SMS) verification codes.
- Helps provide more secure mobile transactions with a graded level of trust to allow and deny access using mobile device fingerprinting, geographic location awareness, and IP reputation.
- Integration with the IBM MobileFirst Platform and IBM MobileFirst Protect (formerly, MaaS360 by Fiberlink, an IBM company) lets mobile application developers easily incorporate access security.
- Integration with IBM Security Trusteer Fraud Protection lets Access Manager use device fraud and malware indicators in access decisions.
- Provides a graphical policy management interface that supports authoring complex policies.

Access Manager Federation Module

Collaboration between organizations is a central tenant of business. Users from collaborating organizations often require secure access to each other's applications. Additionally, internal users increasingly need access to externally hosted services, including cloud-based SaaS and business partner applications.

Federated access helps enable these scenarios by delivering a secure, seamless sign-on experience to external applications, helping eliminate the need for providing multiple user IDs and passwords. This may lead to gains in user productivity, user experience, and reductions in administration cost. Users authenticate once, and then obtain access to federated applications inside and outside their network infrastructure.

The Federation Module accelerates the adoption of third party enterprise SaaS applications within an organization by enabling out of the box connectors to popular applications. By using these connectors the organization can rapidly give users access to an application without creating an additional set of logins. This also increases security and visibility by linking a user’s enterprise identity to the identity at the third party application provider.

Access Manager Federation Module key capabilities:

- Federated single sign-on (SSO) for users across multiple applications.
- Support for SAML 2.0 and OpenID Connect protocols for federated access.
- Preintegrated federation connectors to popular cloud applications.

IBM Security Access Manager at a glance
Physical characteristics of hardware appliance:
- 1U form factor
- H x W x D: 44.2 mm x 430.2 mm x 533.7 mm (1.74 in. x 17 in. x 21 in.)
- Management interface: 10/100/1000
- Application interface: 10/100/1000 (IPv6 supported)
- Supported physical media types: RJ-45
- Redundant power supplies
- Solid-state storage
- 100 – 240 V, full range
Machine specifications for hardware appliance:
- Intel Core i7-2600 processor
- 32 GB memory
- 800 GB solid-state drive
- 6 network ports*
Platform support for virtual appliance:
- VMware ESX environment
- SoftLayer Bare Metal
- Amazon Web Services (AWS)
- Citrix XenServer
- Kernel-based Virtual Machine (KVM)
Supported web browsers:
- Google Chrome
- Microsoft Internet Explorer
- Mozilla Firefox
Performance data:**
- Throughput: Up to 1.2 Gbps or 25,000 requests per second
- Latency: Down to 0.8 ms
- Large-packet throughput: Up to 1.2 Gbps
- Small-packet throughput: Up to 25,000 requests per second
- Authentication throughput: Up to 1,500 logins per second
- Concurrent connections: Up to 30,000

Why IBM?

IBM Security solutions are trusted by organizations worldwide for identity and access management. The proven technologies enable organizations to protect their most business-critical resources from the latest security threats.

Going beyond traditional point solutions, Security Access Manager integrates with many other IBM Security solutions to provide next-generation access management for a multi-perimeter world. Organizations can use IBM QRadar Security Intelligence Platform to get actionable insights for staying a step ahead of new types of attacks, while also helping facilitate compliance. Out-of-the-box consumption of IBM Trusteer Mobile SDK and Secure Browser context data enables users to create comprehensive access policies that include fraud and malware detection without modifying applications. Security Access Manager also provides built-in support for IBM MobileFirst Platform developed mobile applications by enabling seamless authentication and authorization of users along with risk based access enforcement.

As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: ibm.com/financing

For more information

To learn more about IBM Security Access Manager contact your IBM representative or IBM Business Partner, or visit: ibm.com/identity-access-management

IBM Corporation

Software Group

Route 100

Somers, NY 10589

Produced in the United States of America

September 2015

* Two of these ports are dedicated to appliance management.

**Performance data quoted for IBM Security Access Manager for Web is based on testing with HTTP and HTTPS traffic that is intended to be reflective of typical live traffic. Environmental factors such as protocol mix and average packet size will vary in each network, and measured performance results will vary accordingly. IBM Security Access Manager for Web throughput was determined by pushing traffic through the appliance and measuring how much throughput was achieved with zero packet loss and low response times. For benchmark testing, IBM Security Access Manager for Web appliances were configured with worker-threads = 300 and maximum-cached-persistent-connections = 300; large-file throughput was measured with multiple clients requesting 50 Kb