Identity and Access Management in IBM Security Solutions

مدیریت هویت و دسترسی در استراتژی و سبد محصولات شرکت IBM

شرکت IBM با هدف ارائه راهکارهای جامع امنیتی، زیربنای امنیتی خود را تحت عنوان IBM Security Framework ارائه کرده است که مشتمل بر سخت‌افزارها، نرم‌افزارها و خدمات امنیتی است تا از این راه با کمترین هزینه، نیازمندی‌های امنیتی سازمان‌ها به‌صورت جامع‌نگر تأمین شود. یکی از حوزه‌های فعالیت شرکت IBM تأمین امنیت کاربران است تا امنیت سازمان و امنیت کاربران به‌صورت دوطرفه حاصل شود. این معماری امنیتی در شکل-۱ قابل مشاهده است.

شکل ۱- Framework امنیتی شرکت IBM

برای رسیدن به این هدف در دامنه People از معماری معرفی شده، شرکت IBM محصولات مختلف و مکملی را ارائه داده که شاخص‌ترین آن مجموعه نرم‌افزاری IBM Security Identity and Access Assurance می‌باشد. این مجموعه نرم‌افزاری، شامل پنج محصول امنیتی مرتبط شرکت IBM است که چرخه حیات کاربران را همراه با مدیریت، حفاظت و پایش دسترسی آن‌ها به منابع، داده‌ها و برنامه‌های کاربردی سازمان فراهم می‌کنند. این مجموعه نرم‌افزاری، مدیریت پروفایل کاربران، احراز هویت، مجوزهای دسترسی و بازرسی خط‌مشی‌های امنیتی را به‌صورت خودکار و متمرکز فراهم می‌کند؛ ضمن اینکه قابلیت پایش کاربر و گزارش‌هایی از فعالیت کاربران برای شناسایی وضعیت انطباق با خط‌مشی‌ها و استانداردهای امنیتی را ارائه کرده است. بنابراین با به‌کارگیری این راهکار جامع، می‌توان شناسایی هویت‌ها را تضمین کرد، مخاطرات امنیتی را کاهش داد و از منابع زیرساختی فناوری اطلاعات سازمان حفاظت کرد.

برای اطمینان از کیفیت و کارایی این مجموعه محصول، مناسب است تا گزارش رده‌بندی محصول مؤسسه مرجع بین‌المللی بسیار معتبر Gartner در سال جاری میلادی را مرور نموده تا جایگاه راهکار IBM نسبت به سایر رقبای آن معین گردد. همان‌طور که مشخص است IBM در گروه Leader این حوزه از محصولات معرفی شده است که در شکل-۲ مشاهده می‌شود.

شکل ۲- نمودار اختصاصی مؤسسه مرجع بین‌المللی Gartner در رده‌بندی محصولات IAM در سال ۲۰۱۵ میلادی

معرفی مجموعه محصول IBM Security Identity and Access Assurance

در یک نگاه کلان، مجموعه نرم‌افزاری IBM Security Identity and Access Assurance امکانات و قابلیت‌های زیر را برای زیرساخت فناوری اطلاعات سازمان فراهم می‌نماید:

- ✓ مدیریت کامل هویت کاربران در چرخه حیات سازمانی شامل پرسنل و کاربران داخلی و خارجی و مشتریان
- ✓ مدیریت و کنترل دسترسی به منابع و برنامه‌ها بر پایه خط‌مشی‌های امنیتی به‌صورت خودکار
- ✓ فراهم کردن قابلیت ورود یک‌مرحله‌ای (SSO) کاربران به برنامه‌های کاربردی به‌صورت امن
- ✓ پشتیبانی و ارائه خدمات مدیریت هویت و دسترسی به منابع و برنامه‌های کاربردی سازمانی مستقر در محیط‌های پردازش ابری یا مراکز داده توزیع شده و راه دور
- ✓ رخداد نگاری و تحلیل رویدادها و وقایع جمع‌آوری شده از همه زیرسیستم‌های این مجموعه جهت تولید گزارش‌های مدیریتی و بررسی و ممیزی انطباق با استانداردهای امنیتی

- ✓ ایجاد یکپارچگی در سطح بالاتر و فرا سازمانی (Federation) برای مدیریت یکپارچه دسترسی‌های متقابل کاربران مابین سازمان‌های شریک یا همکار
- ✓ محافظت سرویس‌ها و برنامه‌های کاربردی مبتنی بر وب در برابر انواع حملات و تهدیدات امنیتی
- ✓ قابلیت پشتیبانی برنامه‌های تجاری و سازمانی در محیط IBM Mainframe
- ✓ ایجاد یکپارچگی و تعامل ارتباط سیستمی مابین سیستم‌ها و Platformهای متنوع دارای بانک اطلاعاتی کاربران
- ✓ بهبود مدیریت امنیت و سازگاری از راه کسب اطمینان از رعایت خط‌مشی‌ها و استانداردهای امنیتی
- ✓ ایجاد سیستم هوشمند مدیریت Password به‌صورت خودکار برای کلیه دسترسی‌های کاربران در سطح سازمان

شکل ۳- مدیریت یکپارچه هویت و دسترسی

مجموعه نرم‌افزاری IBM Security Identity and Access Assurance خود از پنج نرم‌افزار زیر تشکیل شده است:

- IBM Security Identity Manager
- IBM Security Access Manager for Enterprise Single Sign-on
- IBM Security Access Manager for Web
- IBM Tivoli Federated Identity Manager
- IBM Security QRadar Log Manager

این پنج نرم‌افزار که هریک عهده‌دار تأمین بخشی از امکانات و قابلیت‌های اشاره شده هستند، در نهایت در پیاده‌سازی یکپارچه با یکدیگر و نیز در همگام‌سازی با پایگاه‌های داده و برنامه‌های کاربردی مرتبط در سطح سازمان، مدیریت فراسازمانی کاربران و هویت‌ها و دسترسی‌های آن‌ها را در سطح یک سازمان یا به‌صورت فرا سازمانی با طرف‌های تجاری و خدماتی ایشان به انجام می‌رسانند.

شکل ۴- عناصر مجموعه نرم‌افزاری IBM Security Identity and Access Assurance

ابزار مدیریت هویت IBM Security Identity Manager

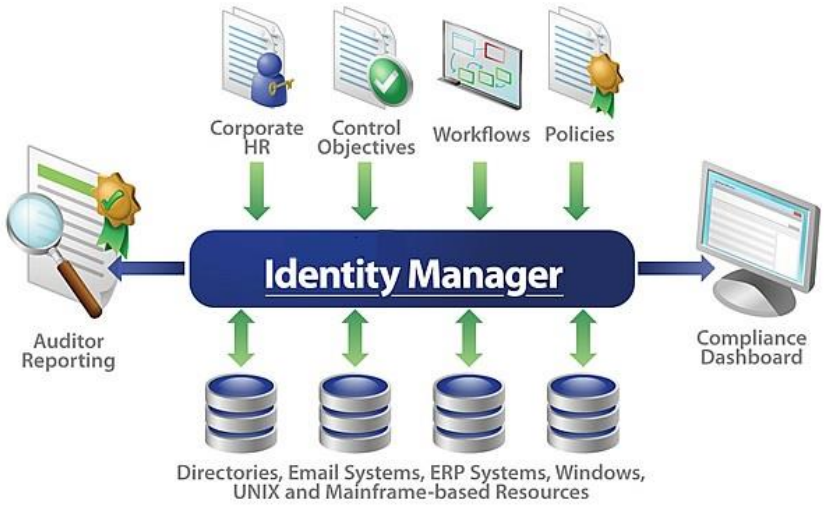
این ابزار یکی از مهم‌ترین اجزای مجموعه نرم‌افزاری IBM Security Identity and Access Assurance بوده و به‌عنوان راهکار جامع مدیریت چرخه حیات سازمانی کاربران و مدیریت نقش‌ها و دسترسی‌های آن‌ها، این امکان را فراهم می‌کند تا سازمان‌ها به‌طور مؤثر مدیریت هویت کاربران را به‌منظور ارتقاء امنیت و انطباق با استانداردهای موجود انجام دهند. این ابزار، راهکاری مبتنی بر خط‌مشی‌های امنیتی است که مجوزهای دسترسی کاربر را به منابع مدیریت شده کنترل می‌کند. همچنین، با استفاده از این ابزار، امکان ایجاد، تغییر، تجدید گواهی[۱] و پایان دادن هویت کاربران در چرخه حیاتی که برای هر کاربر و نقش در سازمان تعریف شده است، به‌صورت خودکار فراهم می‌شود. اهم قابلیت‌هایی که این ابزار فراهم می‌کند عبارت‌اند از:

- دسترسی کاربران به مدیریت رمز عبور خود و یا بازیابی[۲] آن در صورت نیاز
- کاهش هزینه‌های مربوط به نیروی میز امداد[۳]
- نظارت و ممیزی بر سطح دسترسی کاربران
- مدیریت متمرکز تجهیزات و منابع سازمانی
- افزایش امنیت دسترسی توسط کاهش حساب‌های کاربری زائد و بدون استفاده
- تعریف چرخه‌های کاری[۴] به‌منظور خودکارسازی دسترسی کاربران سازمان به منابع و در نهایت کاهش زمان انجام کار و همچنین هزینه‌های مدیریتی

---

۱ Recertification
۲ Rest Password
۳ Help Desk
۴ Work flow

- کاهش پیچیدگی در مدیریت هویت کاربران از راه خط‌مشی‌های متمرکز، مدیریت چرخه حیات هویت کاربران به‌صورت یکپارچه و پشتیبانی از ابزارهای شرکت‌های ثالث
- ارتقاء سطح اطمینان به کاربر از راه یکپارچه‌سازی با روش‌های احراز هویت سخت‌گیرانه
- تولید گزارش‌های ممیزی و پایش فعالیت‌های کاربر
- انطباق‌پذیری مؤثر و عملی از راه مدیریت هویت و دسترسی به‌صورت متمرکز



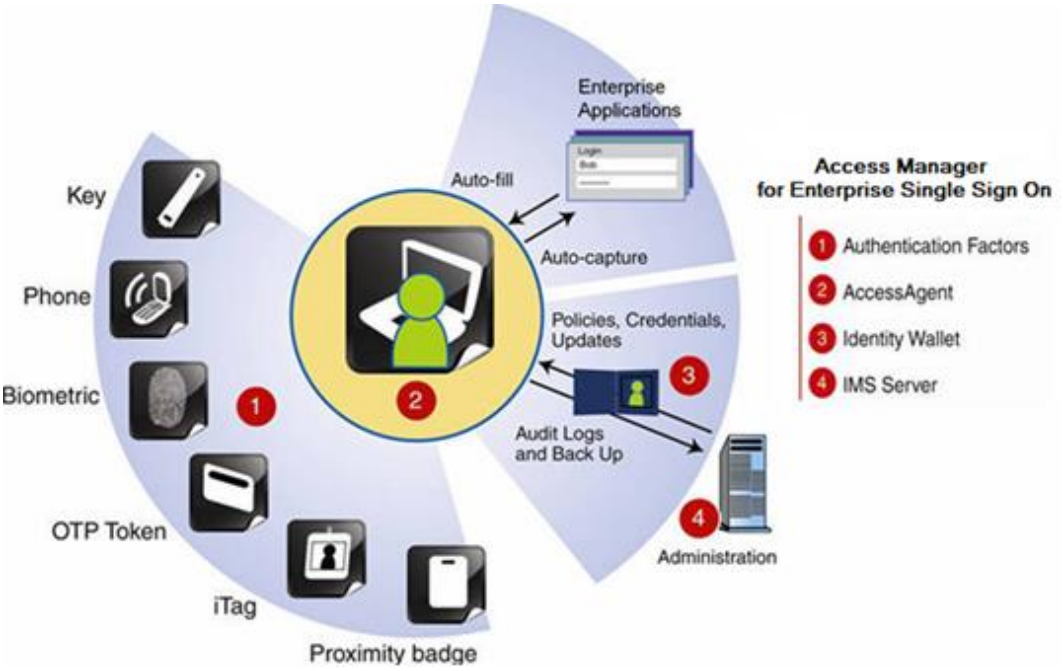
شکل ۵- مدیریت هویت توسط IBM Security Identity Manager

ابزار مدیریت دسترسی یک مرحله‌ای IBM Security Access Manager for Enterprise SSO

این نرم‌افزار یکی دیگر از مهم‌ترین اجزای این مجموعه بوده و مدیریت کلمه‌های عبور و روش‌ها و تجهیزات مختلف احراز هویت کاربران را در دسترسی به همه منابع IT از رایانه‌های شخصی و کاری گرفته تا انواع برنامه‌های کاربردی سازمان انجام می‌دهد. مدیریت کلمه‌های عبور و نیز دسترسی یک مرحله‌ای (Single Sign-on) از جمله قابلیت‌هایی است که این نرم‌افزار در مجموعه مدیریت هویت و دسترسی کاربران بر عهده دارد. این ابزار ضمن اینکه کمک قابل‌توجهی برای مدیریت کلمه‌های عبور متنوع کاربران و سربار ناشی از آن می‌باشد، از طریق جمع‌آوری رویدادها و سابقه فعالیت‌های کاربران و ارسال آن‌ها به یک سرور مرکزی، ممیزی و تحلیل‌های لازم را انجام داده و دسترسی کاربران به اطلاعات را پیگیری و ارزیابی می‌کند تا درنهایت از طریق آن‌ها، بتوان به گزارش‌های انطباق نیز دست یافت. در حوزه احراز هویت کاربران، این نرم‌افزار علاوه بر کلمه عبور از تجهیزات و روش‌های سخت‌گیرانه‌تری نیز از قبیل کارت‌های هوشمند و بیومتریک نیز پشتیبانی می‌کند. به‌طور خلاصه اهم قابلیت‌هایی را که این ابزار فراهم می‌کند می‌توان به شرح ذیل برشمرد:

- مدیریت کلمات عبور کاربران به‌طور متمرکز جهت کاهش سربار حاصل از مدیریت و راهبری آن‌ها از قبیل فراموشی کلمه عبور و ارائه کنسول مناسب جهت مدیریت کلمات عبور توسط خود کاربران
- ارائه مکانیسم Single Sign-on و Single Sign-off در دسترسی به برنامه‌های کاربردی سازمان و برنامه‌های کاربردی مبتنی بر وب
- کنترل دسترسی سخت‌گیرانه از راه ورود یک مرحله‌ای به برنامه‌های مختلف

- یکپارچگی با نرم‌افزار IBM Security Identity Manager جهت دسترسی به فهرست کاربران و نقش‌های آن‌ها به‌منظور مدیریت کلمات عبور، ارائه قابلیت SSO، کنترل دسترسی به برنامه‌ها و منابع IT توسط ایشان و نیز ممیزی فعالیت‌های آن‌ها
- بهبود کارایی از راه حذف چندین کلمه عبور
- افزایش قابلیت بازرسی و انطباق از طریق جمع‌آوری، ردیابی و ممیزی جزئیات دسترسی کاربر به اطلاعات
- امکان نصب و راه‌اندازی به‌صورت گسترده و توزیع شده از نظر وسعت جغرافیایی و راهکارهای افزونگی اجزای مختلف نرم‌افزار
- برخورداری از یک زیرساخت باز جهت پشتیبانی از طیف وسیعی از تجهیزات احراز هویت از قبیل کارت هوشمند، توکن، RFID، اثر انگشت و سایر مکانیسم‌های بیومتریک و ...

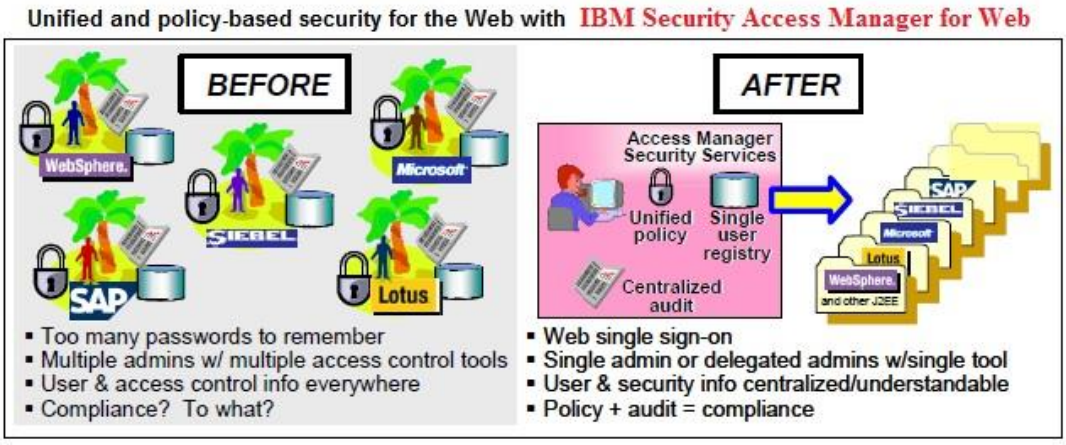


شکل ۶- مدیریت ورود یک مرحله‌ای دسترسی توسط IBM Security Access Manager for Enterprise Single Sign-On

ابزار مدیریت دسترسی به خدمات مبتنی بر وب IBM Security Access Manager for Web

این ابزار مؤثر و پرقابلیت شرکت IBM به‌صورت هم‌زمان مدیریت دسترسی امن کاربران و حفاظت از برنامه‌های کاربردی مبتنی بر وب را با بهره‌گیری از مکانیسم‌های متنوع امنیتی و شبکه‌ای فراهم می‌نماید. از جمله این مکانیسم‌ها می‌توان به احراز هویت، احراز صلاحیت، ورود یک مرحله‌ای (SSO)، تقسیم بار و کنترل امنیتی ترافیک عبوری به سمت سرویس‌ها و نرم‌افزارهای مبتنی بر وب اشاره نمود؛ بنابراین این ابزار ضمن کنترل دسترسی هوشمند کاربر به برنامه‌های کاربردی مختلف، از برنامه‌های کاربردی در برابر تهدیدات وب پیشرفته در سطح شبکه نیز حفاظت می‌کند.

از آنجا که این ابزار شامل بر ماژول‌های نرم‌افزار و میان‌افزارهای سرویس‌دهنده متعددی می‌باشد، شرکت IBM در راستای سیاست‌های ساده‌سازی محصولات خود، آن را به‌صورت یکپارچه و آماده در دو قالب سخت‌افزاری Appliance و نرم‌افزاری Virtual Machine ارائه می‌دهد. قابلیت‌هایی که این ابزار فراهم می‌کند عبارت‌اند از:



شکل ۷- مدیریت دسترسی به خدمات وب توسط IBM Security Access Manager for Web

- ایجاد بستر مدیریت متمرکز در امن سازی و دسترسی امن به سرویس‌های وب سازمان به‌صورت مبتنی بر قواعد[۱]
- احراز هویت و احراز صلاحیت کاربران به‌صورت امن در دسترسی به برنامه‌های کاربردی وب با قابلیت‌های هوشمند و تصمیم‌گیری اجازه دسترسی مبتنی بر ریسک
- حفاظت برنامه‌های کاربردی مبتنی بر وب در برابر تهدیدات پیشرفته با به‌کارگیری فایروال لایه وب
- پیاده‌سازی Reverse Proxy در دسترسی سریع به برنامه‌های کاربردی مبتنی بر وب
- سازگاری با انواع برنامه‌های کاربردی مبتنی بر وب شامل IBM WebSphere، Microsoft و SAP
- ثبت دسترسی‌ها و رویدادهای امنیتی و امکان ارائه گزارش‌های ویژه نظارت و ممیزی در یکپارچگی با سری محصول IBM QRadar SIEM
- سازگاری با انواع برنامه‌های کاربردی مبتنی بر وب شامل IBM WebSphere، Microsoft و SAP

شکل ۸- مدیریت دسترسی به خدمات وب توسط IBM Security Access Manager for Web

[۱] Policy-based

ابزار مدیریت و نگهداری رویدادها — IBM Security QRadar Log Manager

این ابزار، امکان جمع‌آوری، تجزیه و تحلیل، بایگانی و ذخیره‌سازی حجم زیادی از رویدادهای[۱] امنیتی و شبکه‌ای را به‌صورت جامع فراهم می‌سازد. این ابزار با تجزیه و تحلیل داده‌هایی که از تجهیزات شبکه و امنیتی، سرویس‌دهنده‌ها، سیستم‌های عامل، برنامه‌های کاربردی، کاربران انتهایی و غیره جمع‌آوری شده است، نگرشی بلادرنگ از تهدیدات فراهم می‌کند.

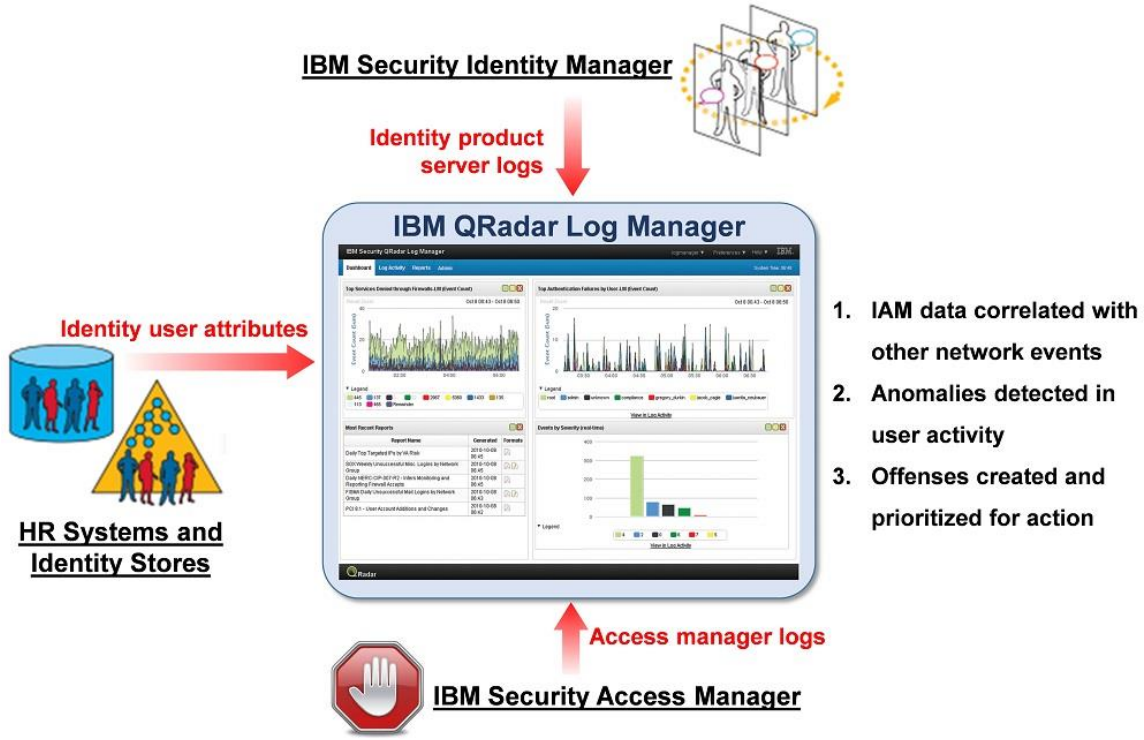
به بیان دقیق‌تر، نقش این مؤلفه در مجموعه نرم‌افزاری IBM Security Identity and Access Assurance جمع‌آوری، نگهداشت و تحلیل رخدادهای این مجموعه و سوابق فعالیت‌های کاربران و دسترسی‌های آن‌ها به منابع تحت مدیریت و نیز رخدادهای مربوط به مؤلفه WAF موجود در سیستم Access Manager for Web این مجموعه است تا در نهایت بتوان بازنگری و بهبودهای لازم را در خط‌مشی‌ها و دسترسی‌های تعریف شده در این مجموعه ایجاد نمود به‌نحوی که به بیشترین انطباق با استانداردهای امنیتی موجود دست پیدا کرد.

از اهم قابلیت‌های این ابزار می‌توان موارد زیر را برشمرد:

- دارای رابط کاربری برای مشاهده بلادرنگ رخدادها، گزارش‌ها و انجام کارهای مدیریتی
- نرمال‌سازی[۲] رویدادهای خام دریافتی از تجهیزات و یا نرم‌افزارها و تبدیل آن به قالب یکسان
- قابلیت همبستگی[۳] رویدادهای دریافتی
- دارای موتور تحلیل‌گر ترافیک شبکه و رخدادهای امنیتی
- ساخت قواعد مختلف در برخورد با یک رخداد خاص (به‌طور مثال ایجاد یک هشدار در زمان وقوع یک ورود ناموفق به سیستم)
- ترسیم شکل سلسله مراتبی[۴] شبکه
- قابلیت ارسال رویدادها به یک سیستم Ticketing برای انجام اقدامات لازم
- قابلیت رمزنگاری بر روی بسته‌های حاوی نام کاربری، یا شماره کارت بانکی و یا اطلاعات مشابه
- قابلیت بسته‌بندی رویدادها در مجموعه‌های مختلف به‌منظور جستجوی آسان
- ضبط و پردازش حجم زیادی از داده‌های مربوط به رویدادها
- گزارش‌گیری از انطباق‌پذیری با الزامات و استانداردها

---

[۱] Log
[۲] Normalization
[۳] Correlation
[۴] Network Hierarchy

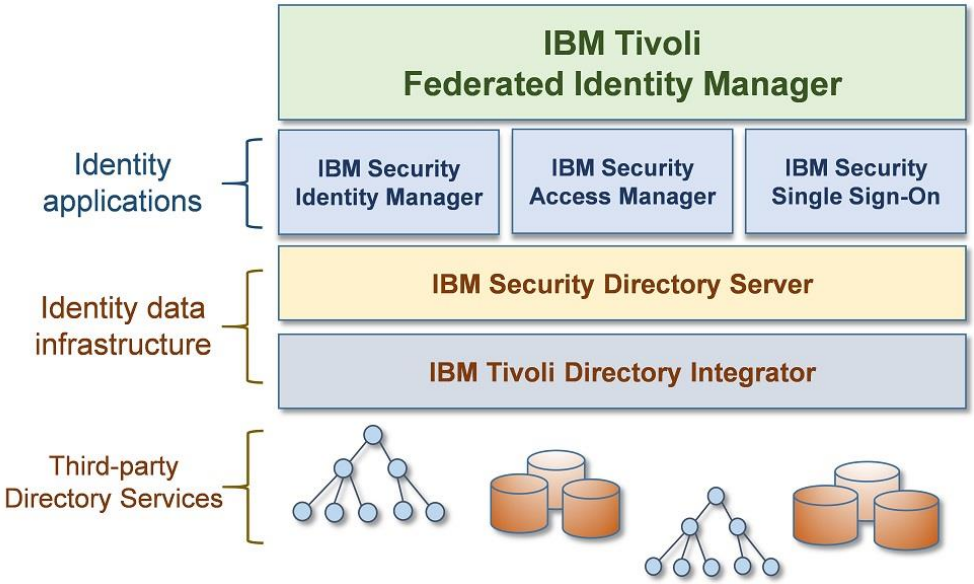


شکل ۹- مدیریت رویدادها توسط IBM Security QRadar Log Manager

ابزار مدیریت هویت فراسازمانی IBM Tivoli Federated Identity Manager

این ابزار امکان همکاری بین دو کسب‌وکار[۱] و یا یک کسب‌وکار و یک مشتری[۲] را به‌صورت متمرکز با استفاده از مدیریت دسترسی کاربر و از طریق یکپارچه‌سازی و احراز هویت امن به‌صورت کلان و فراسازمانی فراهم می‌کند. بنابراین به کمک این ابزار، کاربران یک سازمان می‌توانند ورود یک مرحله‌ای و یکپارچه به برنامه‌های کاربردی سازمان دیگر داشته باشند بدون اینکه نیازی به چندین شناسه کاربری و کلمه عبور باشد. این ابزار یک راهکار مدیریت دسترسی است که SSO را به‌صورت فراسازمانی برای کاربران فراهم می‌کند. به بیان دیگر، این نرم‌افزار به‌عنوان یک لایه مجتمع‌سازی بالاتر، عملیات مدیریت هویت و دسترسی و نیز SSO را در سطح بالاتری میان چندین مجموعه برخوردار از راهکار Identity and Access Manager میسر می‌سازد.

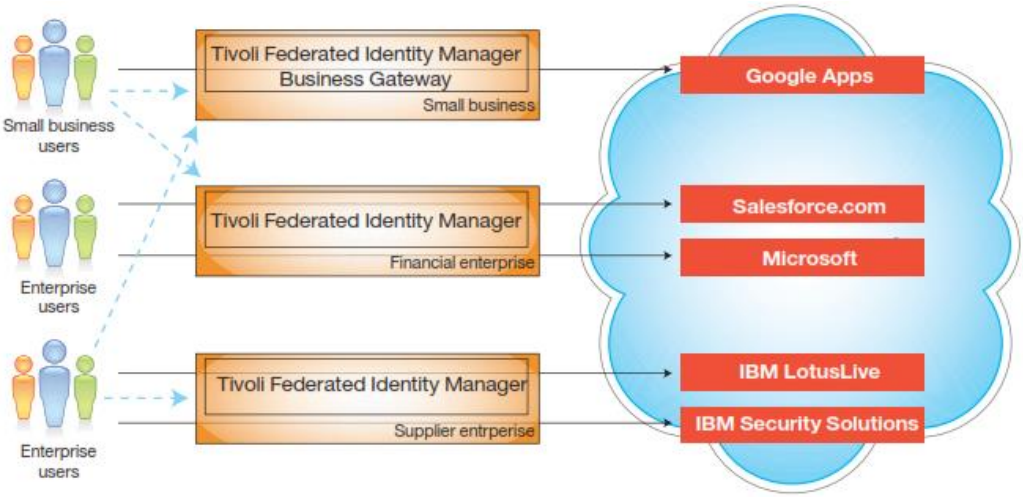
[۱] Business-to-Business
[۲] Business-to-Consumer



شکل ۱۰- معماری و ساختار IBM Tivoli Federated Identity Manager

از قابلیت‌هایی که این ابزار فراهم می‌کند، می‌توان به موارد ذیل اشاره کرد:

- کمک به همکاری و تعامل میان کسب‌وکارها و سازمان‌های به‌صورت امن با استفاده از فراهم کردن خدمات واسطه‌ای و قابلیت SSO
- ارائه SSO برای کاربران خارج از سازمان به برنامه‌های کاربردی داخل سازمان و نیز ارائه قابلیت SSO به کاربران داخلی جهت دسترسی به برنامه‌های کاربردی خارجی مبتنی بر رایانش ابری
- پشتیبانی از استانداردهای باز برای دسترسی کاربران به برنامه‌های کاربردی مبتنی بر رایانش ابری
- ارائه راهکارهای مدیریت هویت
- ارائه یک ساختار ماژولار جهت پشتیبانی محیط‌های IBM z/OS



شکل ۸۱- مدیریت SSO توسط IBM Tivoli Federated Identity Manager

پیشنهاد شرکت داده‌پردازی ایران

شرکت داده‌پردازی ایران به‌عنوان پرقدمت‌ترین شرکت در صنعت فناوری اطلاعات کشور و یکی از شرکت‌های با توان و اعتبار رده اول در بازار و نیز با توجه به سابقه فعالیت تحت مالکیت مستقیم شرکت بزرگ IBM ، در این دوره زمانی، فعالیت تجاری و فنی در زمینه راهکارها و محصولات حیطه امنیتی شرکت IBM با اولویت جاری در دامنه Identity and Access Management را به‌عنوان یکی از راهبردهای عملیاتی خود برگزیده است و بدین ترتیب محصولات مرتبط IBM را به سبد متنوعی از محصولات سخت‌افزاری و نرم‌افزاری IBM که سال‌هاست برای مشتریان سازمانی خود در کشور ارائه می‌نماید اضافه نموده است.

طبق دیدگاه حاکم در شرکت داده‌پردازی ایران، فعالیت موفق و مؤثر در حیطه‌های امنیت یا مدیریت در فناوری اطلاعات، نیازمند نگرشی فراتر از فرایندهای معمول فروش و نصب سخت‌افزار و نرم‌افزار بوده و مستلزم نگرش سیستمی و پروژه–محور با ابعاد چندوجهی سازمانی/فنی می‌باشد. مطابق این دیدگاه، پیشنهاد شرکت داده‌پردازی ایران در استفاده از راهکارهای مطمئن شرکت IBM در زمینه مدیریت هویت و دسترسی نیز یک فرایند چندمرحله‌ای شامل شناخت و تعیین استراتژی، تعیین معماری سرویس و انتخاب محصولات متناسب، تأمین و نصب و راه‌اندازی، پیکربندی و پیاده‌سازی و یکپارچه‌سازی عملیاتی، نظارت و بهبود مستمر و در نهایت پشتیبانی فنی می‌باشد.

بدیهی است که به‌کارگیری این راهکارهای جامع امنیت اطلاعات به‌صورت عمده متناسب با نیازهای گسترده سازمان‌های بزرگ می‌باشد که در کشور ایران، بانک‌ها و مؤسسات حوزه مالی و اقتصادی در کنار شرکت‌های بزرگ صنعت و انرژی و برخی نهادهای دولتی، مخاطب ویژه این پیشنهادهای نوین می‌باشند.

هم‌اکنون اولین پروژه بزرگ پیاده‌سازی راهکار جامع سازمانی مدیریت هویت و دسترسی در سطح کشور، با استفاده از محصولات شرکت IBM و در یکی از بزرگ‌ترین بانک‌های کشور توسط شرکت داده‌پردازی ایران در دست اجرا می‌باشد. برای کسب اطلاعات بیشتر و ارتباط با بخش مرتبط در شرکت داده‌پردازی ایران، از نشانی اینترنتی ذیل استفاده نمایید:

⇨ http://www.dpi.ir/fa/products/security/iam