بسم الله الرحمن الرحیم

مشخصات فنی

راهکار امن سازی و پایش دسترسی های سطح بالا (PAM)

رایمون

نسخه ۲.۳

خرداد ماه ۱۴۰۲

فهرست مطالب

۱- مقدمه

امروزه با گسترش فناوری اطلاعات، هر سازمان کوچك یا بزرگی دارای یك شبکه کامپیوتری است. در این شبکه‌ها معمولا سرویس‌دهنده های مختلف همچون پایگاه داده، HTTP، FTP، برنامه‌های کاربردی تحت شبکه و ... بر روی یك LAN در مرکز شبکه قرار می‌گیرند. در حال حاضر بسیاری از سازمانهای کشور، جهت مدیریت و نگهداری این سرویس‌دهنده‌ها از پروتکلهای دسترسی راه دور نظیر Remote Desktop، SSH، HTTP(S)، Telnet و VNC برای دسترسی و اعمال تنظیمات به تجهیزات شبکه سازمان (واقع در مرکز داده) مانند سرورها، سوییچ‌ها و روترها استفاده می‌نمایند. متأسفانه از آنجا که این پروتکل‌ها فاقد فرآیندهای رویدادنگاری با جزئیات مناسب هستند می‌توانند امنیت اطلاعات سازمانی را به صورت جدی به مخاطره بیندازند. این در حالیست که دسترسی‌های راه دور عموما بالاترین نوع دسترسی به شبکه سازمان محسوب می‌شود و از این رو نیاز است تا رویدادنگاری کاملا جزیی و نیز غیر قابل انکاری از ارتباطات انجام گرفته صورت پذیرد.

سامانه رایمون محصولی است در حوزه Privilege Access Management (PAM) که با هدف ایجاد رویدادنگاری از تمامی جزئیات پروتکل‌های دسترسی راه دور و نیز دیواره آتش لایه کاربرد توسعه یافته است. این محصول به دو صورت کاملا شفاف و یا غیر شفاف می‌تواند در شبکه سازمان مستقر شود. شکل ۱ به صورت نمادین نحوه فعالیت سامانه رایمون را نشان می‌دهد.

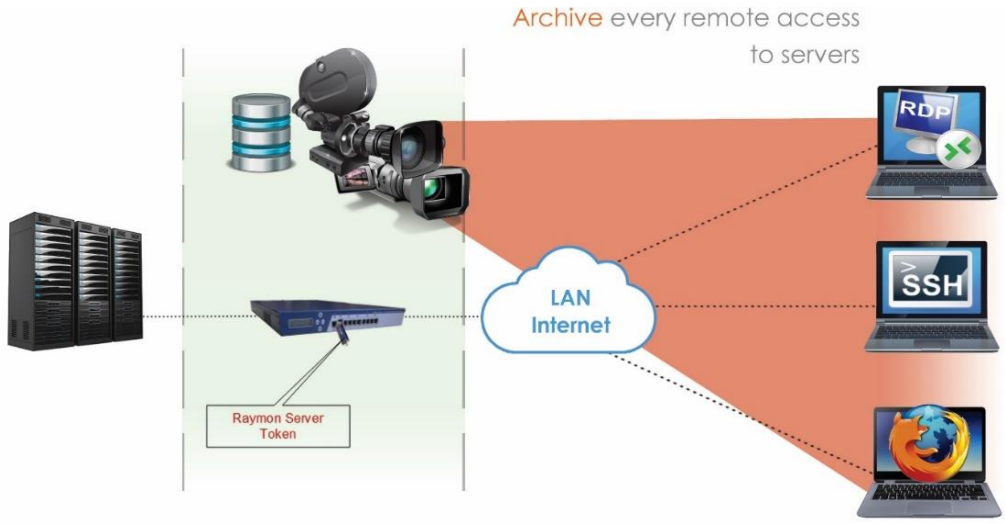
شکل ۱: نحوه فعالیت سامانه رایمون به صورت نمادین

به کمک سامانه رایمون شما قادر خواهید بود تا کاربران مجاز و دسترسی‌های راه دور آنها به منابع مختلف شبکه سازمان را تعریف و مدیریت نمایید. همچنین با بهره گیری از این محصول شما می‌توانید تمامی ارتباطاتی که کاربران مجاز با منابع شبکه سازمان برقرار نموده‌اند در قالب فیلم مشاهده و بررسی نمایید. از طریق کنسول مدیریت این سامانه می‌توانید به جستجوی عبارات خاص، رویدادهای ویژه و ... در فیلم‌ها و مقادیر تایپ شده کاربران نیز بپردازید. همچنین می‌توانید فعالیت‌هایی که کاربر مجاز به انجام آنها می‌باشد را تعریف و کنترل نمایید. برای مثال شما قادر خواهید بود باز شدن هر یک از برنامه‌های mstsc.exe، gpedit.msc و ... در یک ارتباط Remote Desktop و یا اجرای فرمانهای مورد نظر در جلسات ssh را کنترل نمایید. همچنین مدیر قادر است تا باز شدن برنامه‌های دلخواه و یا فرمان‌های خاص خود را در جلسات جستجو نماید و در صورت نیاز ادامه فعالیت‌های کاربر را در قالب فیلم مشاهده و وارسی نمایید.

۲- معماری و نحوه عملکرد سیستم

سامانه رایمون بین کاربران راه دور و سرور یا تجهیزات سازمان قرار میگیرد و بدون نیاز به نصب نرم افزار یا ابزاری بر روی سرورها و کامپیوتر کاربران راه دور توانایی مدیریت و پایش دسترسی آن‌ها را دارد.

پس از قرارگیری سرور رایمون در سر راه ورودی سرویس‌دهنده‌های سازمان، اکنون مدیر سامانه رایمون می‌تواند از طریق کنسول مدیریت این سامانه اقدام به تعریف کاربران ، کنترل مجوزهای دسترسی راه دور آنها و تعیین فعالیت‌های مجاز آنها بنماید. بر مبنای مجوزهای تعیین شده از سمت مدیر، کاربران مجاز از این پس می‌توانند مانند قبل و بدون نیاز به هیچ گونه فعالیت اضافی، اقدام به برقراری ارتباطات راه دور نمایند. البته در این حالت سرور رایمون، تمامی این ارتباطات را دیده‌بانی و پایش می‌نماید و از فعالیت کاربران در قالب فیلم، رویدادنگاری می‌نماید. فیلم‌های مهیا شده از طریق کنسول مدیریت سامانه رایمون قابل مشاهده و نظارت برای مدیر سامانه و یا هر فرد ذی‌صلاح دیگری می‌باشد.



شکل ۲: ساختار کلی استفاده از سامانه رایمون در شبکه سازمان

۳- کاربردهای سامانه رایمون

۳-۱- امن سازی نشست ها ی راه دور

با استفاده از سامانه رایمون امکان کنترل کامل بر زمان و نحوه اتصال کاربران راه دور به سرورها و تجهیزات سازمان و عملیاتی که توسط آنها انجام می شود را خواهید داشت. در طی نشست نیز این سامانه قادرخواهد بود بر اساس سیاست‌های تعریف شده فعالیت‌های کاربران را کنترل نموده و امکان وقوع اتفاقات مخرب را به کمترین میزان ممکن برساند. همچنین استفاده از این سامانه مخاطرات ناشی از ضعف های امنیتی موجود در پروتکل های دسترسی راه دور مانند RDP را به حد اقل می‌رساند.

۳-۲- پایش نشست‌ها ی راه دور

سامانه رایمون امکان آگاهی از تمامی اتفاقاتی که در طی یک نشست راه دور رخ می دهد را فراهم می‌کند. در پایان یک نشست راه دور قادر به دسترسی به محتوای نشست در قالب فیلم نشست، لاگ متنی

نشست و محتوای فایل های منتقل شده در طول نشست خواهید بود. علاوه بر این در طول نشست نیز امکان مشاهده فعالیت های انجام شده به صورت زنده وجود دارد.

۳-۳- کنترل دسترسی پیمانکاران به زیر ساخت فناوری اطلاعات سازمان

سامانه رایمون با ارایه پورتال اختصاصی امکان مدیریت دسترسی پیمانکاران به زیرساخت‌های فناوری اطلاعات سازمان را فراهم می‌کند. با ارایه پورتال رایمون به پیمانکاران دسترسی انها محدود به سرورها و تجهیزات خاص شده و همانطور که قبلا هم اشاره شد تمامی فعالیت‌های آنها قابل بازبینی و پایش هست.

۳-٤- حفاظت از پسوردهای حساس سازمان

با استفاده از سامانه رایمون سازمان می‌تواند بدون آن‌که اختلالی در روال کاری کاربران ایجاد شود، پسورد سرورها و تجهیزات را از دید انها مخفی نماید. این پسوردها به صورت امن در داخل سامانه رایمون ذخیره شده و در موقع نیاز توسط رایمون برای برقراری ارتباط کاربران با سرورها بدون دخالت آنها مورد استفاده قرار خواهد گرفت.

۳-۵- محدودسازی کاربران به کاربرد یا نرم افزار خاص

در بسیاری از مواقع کاربران نیاز به استفاده از یک کاربرد یا نرم افزار خاص دارند. در این مواقع لزومی به دسترسی آنها به شبکه سازمان یا سایر نرم افزارها و سرویس‌ها نمی‌باشد. سامانه رایمون این امکان را می‌دهد که دسترسی کاربر به یک یا چند نرم افزار خاص محدود شده و سایر دسترسی‌ها از او سلب گردد. علاه بر این کلیه فعالیت‌هایی کاربر با نرم افزارهای مورد نظر به صورت زنده در حین نشست یا به صورت فیلم و لاگ های متنوع دیگر در پایان نسشت قابل بازبینی وپایش است.

۳-٦- کنترل ورود و خروج اطلاعات

سامانه رایمون با داشتن امکانات متنوع برای کنترل کانال‌های انتقال اطلاعات از طریق فایل یا کلیپ‌برد. و همچنین ارایه گزارش کامل از اطلاعات منتقل شده ریسک‌های ناشی از نشت اطلاعات یا انتقال اطلاعات مخرب به زیرساخت‌های فناوری اطلاعات سازمان را به حداقل می‌رساند.

٤- امکانات مهم سامانه رایمون

٤-١- روشهای متنوع قرار گیری در شبکه

به منظور تسهیل نصب و استفاده از سامانه رایمون روش‌های متعددی برای استقرار و کاربری این سامانه در نظر گرفته شده است. تنوع این روشها باعث خواهد شد سامانه رایمون با حداقل تغییرات در شبکه و روال کاری کاربران نصب شده و مورد استفاده قرار گیرد. در حال حاضر رایمون از با روشهای زیر قابل استفاده است:

٤-١-١- مد پورتال

در این مد نیازی به انجام تغییرات زیادی در شبکه سازمان وجود ندارد. دسترسی کاربران به سرورها و تجهیزات مورد نظر از طریق پورتال تحت وب رایمون انجام خواهد شد. تمامی عملیات کاربران در مد پورتال از طریق رابط کاربری وب انجام شده و کاربر نیازی به استفاده از نرم افزارهای اتصال راه دور مانند Putty یا MSTSC ندارد.

٤-١-٢- مد شفاف

در این مد سامانه رایمون از دید کاربران شفاف است به این معنی که کاربران متوجه وجود سامانه رایمون در شبکه نخواهند شد. کاربر از همان ابزار و روالی که قبل از نصب سامانه رایمون برای اتصال به سرورها و تجهیزات استفاده می‌کرده بعد از نصب سامانه نیز استفاده خواهد نمود. برای استفاده از این روش باید با اضافه نمودن سیاست مربوطه به فایروال یا سویچ ترافیک پروتکل های مورد نظر به سمت رایمون هدایت گردد(Policy Based Routing).

٤-١-٣- مد Port Forward

در این مد هر سرور یا تجهیز بایک پورت مجزا در سامانه رایمون مشخص خواهد شد. کاربرا برای اتصال به سرور یا تجهیز مورد نظر خود از ابزار یا نرم افزار دلخواه استفاده خواهد نمود.

٤-١-٤- مد Gateway

در این مد رایمون به صورت یک Gateway عمل می‌کند. کاربر با استفاده از نرم افزار مورد نظر خود (مانند Putty یا MSTSC) ابتدا به سامانه رایمون متصل شده و پس از احراز اصالت با همان ابزار به سرور یا تجهیز مورد نظر متصل خواهد گردید.

٤-٢- پشتیبانی از پروتکل های متنوع

سامانه رایمون در حال حاضر از پروتکل های زیر پشتیبانی می‌کند:

- **RDP**
- **RDP-Gateway**
- **Http(s)**
- **VNC**
- **SSH**
- **MS-SQL**
- **SCP**
- **SFTP**
- **TELNET**

کاربران با استفاده از پورتال سامانه یا نرم افزارهای دلخواه خود قادر خواهند بود با استفاده از این پروتکل‌ها با سرورها و تجهیزات سازمان متصل گردند.

٤-٣- امکان تعریف سیاستهای دسترسی متنوع

در سامانه رایمون امکان تعریف سیاست‌های دسترسی بر اساس پارامترهای مختلف مانند زمان، نوع اتصال، آدرس مبدا و نرم افزار قابل استفاده توسط کاربر وجود دارد. ترکیب این سیاست‌ها با یکدیگر انعطاف پذیری زیادی را در مدیریت دسترسی به منابع ایجاد خواهد نمود.

٤-٤- مدیریت پیشرفته سرورها و تجهیزات

در سامانه رایمون به منظور مدیریت بهتر سرورها و تجهیزات امکان تعریف انواع اختصاصی پیش‌بینی شده است که برای هر نوع مشخصاتی مانند پروتکل و پورت‌های مورد استفاده و همچنین ایکون اختصاصی قابل تعریف است. هر سرو یا تجهیز ایجاد شده با این نوع، این مشخصات را به ارث خواهد برد.

روش‌های متنوعی برای افزودن تجهیزات و سرورها به رایمون پیش بینی شده شده است این روش‌ها عبارتند از:

- اسکن شبکه
- خواندن از اکتیو دایرکتوری
- خواندن از فایل CSV

به منظور مدیریت بهتر تجهیزات و سرورهای افزوده شده امکان گروه بندی آنها بر اساس نام دلخواه یا گروه‌های موجود در اکتیو دایرکتوری وجود دارد.

٤-٥- مدیریت پیشرفته کاربران

در سامانه رایمون امکان تعریف کاربران در خود سامانه ویا خواندن کاربران از دامین وجود دارد. همچنین میتوان لیست کاربران را از طریق فایل CVS وارد نمود. به منظور مدیریت بهتر کاربران امکان گروه بندی آنها نیز در نظر گرفته شده. برای منترل دسترسی مدیران سامانه به بخشهای مختلف آن تنظیمات کاملی در سامانه وجود دارد. در کنار این مورد امکان تعریف نقش نیز به سامانه افزوده شده تا کنترل دسترسی‌های مدیران سامانه با سادگی بیشتری صورت پذیرد.

٤-٦- پورتال کاربران راه دور

همانطور که قبلا اشاره شد یکی از روشهایی که برای اتصال به سرورهای مقصد در اختیار کاربران راه دور قرار می‌گیرد استفاده از پورتال سامانه می باشد. کاربران در پورتال سامانه رایمون فهرست سرورها و تجهیزاتی که قادر به دسترسی هستند مشاهده نموده و و از همین طریق امکان اتصال تحت وب به آنها را

خواهند داشت. پورتال رایمون به گونه ای طراحی شده که در یک تب مرورگر امکان مدیریت چند سرور به صورت همزمان وجد خواهد داشت و نیازی به باز نمودن تب‌های متعدد نیست. همچنین فضای یک تب قابل تقسیم بندی به بخشهای مجرا است که در هر بخش می‌توان یک سرور را مدیریت نمود. به منظور سهولت کاربری سامانه امکانات جستجو و گروه بندی سرورها و تجیهزات نیز در پورتال رایمون وجود دارد.

٤-٧- تهیه اطلاعات ممیزی کامل از نشست

سامانه رایمون به منظور فراهم اوردن امکان ممیزی کامل نشست ها اطلاعات متعددی از نشست را در اختیار قرار می دهد این اطلاعات عبارتند از:

- اطلاعات کلی نشست مانند نام کاربری، مشخصات سرور مقصد، زمان و طول نشست
- محتوای تصویری نشست که از طریق پخش کننده تحت وب سامانه قابل بازبینی بوده و قابل تبدیل به فایل تصویری با فرمت قابل پخش در نرم افزارهای پخش کننده استاندارد می باشد.
- فایل های مبادله شده در طول نشست
- فهرست پروسه های اجرا شده در طول نشست
- محتوای منتقل شده از طریق کلیپ برد
- متون تایپ شده به وسیله صفحه کلید(KeyLogger)

٤-٨- جستجو در محتوای نشست ها

به منظور ساده سازی ممیزی نشست‌ها سامانه رایمون امکان جستجو در محتوای نشست‌ها را دارد. برای نشست‌های تصویری (مانند نشست های پروتکل RDP) رایمون با استفاده از تکنولوژی OCR تمام صفحه، کل محتوای متنی نشست را استخراج کرده و به نظور جستجوی سریع اندیس گذاری می‌کند. جستجوی پیشرفته در محتوای نشست ها به صورت فازی یا با استفاده از Wildcard قابل انجام است.

I.

٤-٩- مشاهده زنده نشست ها

در سامانه رایمون این امکان وجود دارد که مدیر سامانه همزمان با نشست راه دور کاربران بتواند محتوای یک یا چند نشست را از طریق رابط وب مدیریت سامانه مشاهده نماید(Live View). همچنین این امکان وجود دارد که مدیر در صورت مشاهده فعالیت غیر مجاز نشست کاربر را قطع نماید.

٤-١٠- کنترل خودکار فعالیت کاربران در طول نشست

به منظور کنترل فعالیت کاربران در طول نشست سامانه رایمون امکان جلوگیری از اجرای پروسه ها یا دستورات غیر مجاز در طول نشست را دارد. به منظور کنترل دقیق دستورات از پروتکل TACACS+ استفاده شده و رایمون می‌تواند مانند یک سرور TACACS عمل کند .در این حالت مجاز بودن یا نبودن دستورات قبل از اجرا از طریق پروتکل TACACS توسط رایمون مشخص می‌گردد.

٤-١١- مدیریت پیشرفته فضای ذخیره سازی و پشتیبان گیری از اطلاعات

در طی زمان و با افزوده شدن اطلاعات نشست ها نیاز به مدیریت فضای ذخیره سازی این اطلاعات وجود دارد. برای این منظور رایمون امکان تعریف زمان بندی برای آرشیو اطلاعات نشست ها و همچنین پاک سازی اطلاعات قدیمی یا انواع خاصی از فایل ها را فراهم آورده است. علاوه بر این برای پشتیبان گیری از اطلاعات و تنظیمات سامانه نیز امکان تعریف زمان بندی وجود دارد.

٤-١٢- ذخیره سازی امن پسورد تجهیزات و سرورها

یکی از چالش‌های مهم در بسیاری از سازمانها مدیریت پسورد تجهیزات و سرورها است. این پسوردها غالبا در اختیار افراد مختلف قرار دارد و همین موضوع مدیریت آنها را با چالش مواجه می‌کند. برای رفع مشکلات مطرح در این زمینه سامانه رایمون مجهز به یک مکانیزم ذخیره سازی امن برای پسوردها است. با وجود این مکانیزم پسوردها داخل سامانه رایمون ذخیره شده کاربران نیازی به دانستن آنها نخواهند داشت. موقع برقرای نشست ، پسورد توسط رایمون برای تشکیل نشست استفاده خواهد شد. پسوردها در سامانه رایمون با الگوریتم های رمزنگاری مناسب و با مدیریت کلید مبتنی بر توکن سخت‌افزاری انجام می پذیرد.

٤-١٣- امکان ممیزی نشست های MSSQL

سامانه رایمون امکان تهیه لاگ از تمام Query های اجرا شده روی پایگاه داده MSSQL را دارد. با استفاده از این ویژگی امکان ممیزی کامل فعالیت‌های مدیران پایگاه داده را خواهید داشت. نکته مهم در مورد این قابلیت عملکرد شفاف آن از دید مدیران پایگاه داده است. به این صورت که هیچ تغییری در نحوه یا ابزاری که مدیر پایگاه داده برای اتصال به پایگاه داده استفاده می‌کند ایجاد نخواهد شد. در نتیجه با وجود سامانه رایمون هیچ محدودیتی برای مدیران پایگاه داده نسبت به حالتی که از رایمون استفاده نمی‌شود ایجاد نخواهد شد.

٤-١٤- نگاشت بین کاربران و حساب های کاربری سرورها و تجهیزات (User Mapping)

در سامانه رایمون این امکان وجود دارد که کاربران برای استفاده از سرورها و تجهیزات محدود به یک حساب کاربری خاص روی ان سرور یا تجهیز شوند. در این صورت کاربر امکان استفاده از اکانت‌های دیگر را نخواهد داشت.

٤-١٥- ارسال لاگ به یک یا چند لاگ سرور بیرونی با استاندارد Syslog

سامانه رایمون امکان ارسال رویدادهای ثبت شده بر روی سامانه شامل نشست های کاربران نهایی و عملکرد کاربران مدیر را در قالب syslog به سامانه های Log server دارد.

٤-١٦- امکان ارتباط با چند Domain با قابلیت همگام سازی اطلاعات در سطح گروه و OU

سامانه رایمون جهت مدیریت کاربران و منابع می تواند به طور همزمان با چند دامین از طریق پروتکل LDAP در ارتباط باشد و هرگونه تغییرات را بر روی سرور رایمون همگام سازی نماید.

٤-١٧- مکانیزم تشخیص و خنثی سازی حملات Brute Force

سامانه رایمون توانایی محافظت از حملات Brute Force در کنسول های مدیریتی و پورتال کاربری دارا می باشد.

۴-۱۸- امکان ارسال آگاه ساز(Notification) از طریق ایمیل

در سامانه رایمون امکان ارسال پیام های اطلاع رسانی به مدیران سامانه مانند اجرای اپلیکیشن های خاص در نشست های راه دور امکان پذیر می باشد.

۴-۱۹- ارایه لاگ جامع از فعالیت مدیران سامانه

در سامانه رایمون هرگونه فعالیت مدیران سامانه رایمون شامل تعریف منابع، قوانین و مشاهده لاگ فعالیت کاربران با جزییات ثبت می گردد.

۴-۲۰- جدول امکانات سامانه رایمون

موضوع	قابلیت	رایمون
نحوه ارائه دسترسی به کاربران ممتاز و پیمانکاران	Invisible Mode	✓
	Portal Mode	✓
	Gateway Mode	✓
	Port Forward Mode	✓
پروتکل های تحت پوشش بدون سرور واسط (Jump Server)	RDP	✓
	RDP Gateway	✓
	SSH	✓
	Telnet	✓
	VNC	✓
	Http(s)	✓
	MS-SQL	✓
	SCP / SFTP	✓
پروتکل های تحت پوشش با سرور واسط (Jump Server)	App Sharing	بدون محدودیت
ممیزی کامل نشست های کاربران ممتاز، ضبط و پخش آن	Convert Users Activity To Video File	✓

	Keystroke	✓
	File Transfer	ارائه نسخه اصلی فایل
	Process & App Monitor	✓
	Command Log	✓
	Video Size for RDP Sessions (1 Min Activity)	۵۰~۶۰ KB
	Replay Activity Player	Web-Based
	Convert Activity Log to General Format	M4V
	Real-Time OCR	✓
نظارت چهارچشمی	On-Line View	✓
	Force Stop Session	✓
	Suspend Session	✗
قابلیت Full-Text Search	OCR	Full Screen Built-in OCR
	Keystroke & Commands	✓
	App & Process	✓
	File Transfer	✓
سیاست‌های کنترلی و اعمال محدودیت	Black listing/Whitelisting of Applications	✓
	Black listing/Whitelisting of commands	✓
	File Transferring	✓
	Time Policy	✓
	Access Control List	✓
	Client IP Restriction	✓
	Local TACACS Server	✓
	امکان Bypass کردن مکانیزم Command Control Policy	غیر ممکن بخاطر وجود Local TACACS Server
مدیریت حساب های کاربری و ماژول احراز هویت	Active Directory/LDAP Integration	✓
	Multi-Domain Support	✓
	Local Identity Provider	✓
	Password Vault	✓

	Password Management	در حال توسعه و بهینه‌سازی
	Remote Password Reset	در حال توسعه و بهینه‌سازی
	تعریف و مدیریت و اختصاص کلید رمز به کاربران جهت اتصالات SSH مبتنی بر کلید با قابلیت Renew هشدار و گزارش منقضی شدن	در حال توسعه و بهینه‌سازی
	تعریف و مدیریت و اختصاص Certificate به کاربران جهت اتصالات مبتنی بر گواهی دیجیتال با قابلیت Renew و هشدار و گزارش منقضی شدن	در حال توسعه و بهینه‌سازی
	رمزنگاری داده های موجود در Password Vault مبتنی بر توکن سخت افزاری	✓
	Single Sign On Client	✓
	MFA	✓
	Credential Mapping	✓
	Authentication Method	Local Active Directory Destination server
	Self-Service Page	در حال توسعه و بهینه‌سازی
مدیریت دارایی ها	Manual	✓
	Import from CSV File	✓
	Active Directory / LDAP	✓
	Auto-Discovery	✓
	Account Discovery	✗
گزارش گیری، هشداردهی و رخدادنماها	امکان ارسال ایمیل هشدار برای مدیر سیستم در صورت اجرای اپلیکیشن غیر مجاز	✓
	امکان تهیه گزارش اپلیکیشن های اجرا شده توسط کاربر و ارسال آن به Syslog Server در شبکه	✓
	قابلیت ارسال امن رویدادهای سیستم به یک Syslog Server در شبکه	✓
	امکان گزارش گیری از عملکرد کاربران در قالب فایل CSV	✓
	پشتیبانی از SNMP Trap	✓

	گزارش سازی دستی و زمان بندی شده با امکان سفارشی سازی قالب، فرمتهای مختلف و ارسال ایمیل	وابسته به ابزار BI
	یکپارچه سازی با سامانه های تیکتینگ رایج	پیاده سازی در صورت نیاز کارفرما
قابلیت های دسترس پذیری، پشتیبان گیری و بازیابی	امکان تهیه نسخه پشتیبان به صورت دستی و خودکار	✓
	امکان تعریف Backup Schedule	✓
	پشتیبانی از High Availability به صورت Active/Passive	✓
	امکان آرشیو نشست های ذخیره شده	✓
مدیریت آبشاری برای سازمان های دارای زیرمجموعه های توزیع شده	• مدیریت سلسله مراتبی سامانه به صورت آبشاری • ماژول گزارش ساز • مدیریت متمرکز لاگ ها • مشاهده وضعیت فعال بودن سامانه ها	✓
سامانه تیکتینگ و درخواست اتصال با تایید مدیر بالادستی	Automation & Approval	در حال توسعه و بهینه‌سازی
نحوه لایسنس گذاری سیستم	دائمی / سالانه	دائمی
	عدم محدودیت در تعریف کاربر	✓
	عدم محدودیت در تعریف کامپیوتر/تجهیز	✓
	محدودیت در نشست های همزمان	✓
سادگی کار با سامانه در محیط وب	پشتیبانی از چند کانکشن در یک تب مرورگر	✓
مکانیزم داخلی محافظت از حملات Brute Force	Brute Force Protection	✓