Teramind DLP

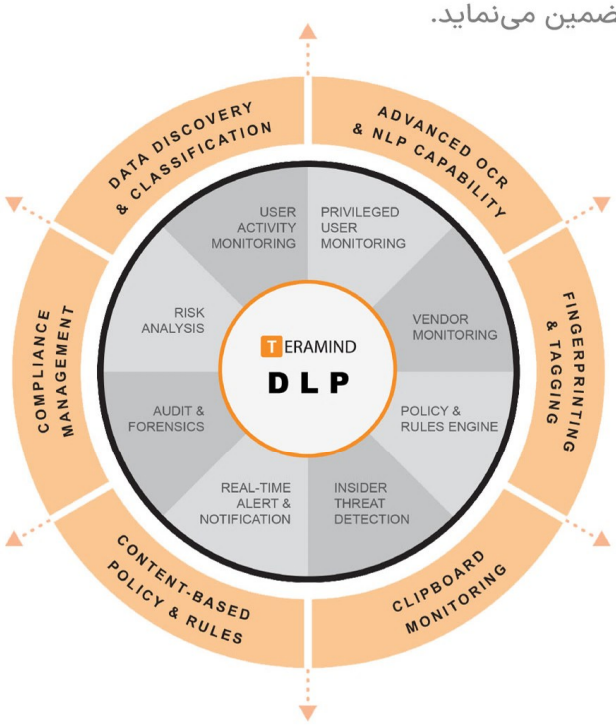
پلتفرم نظارت و جلوگیری از نشت داده

پیشگیری هوشمندانه از نشت داده در نقاط پایانی

TERAMIND

حفاظت هوشمند Teramind در برابر نقض داده، نشت اطلاعات و سرقت مالکیت فکری

راهکار Teramind DLP با ترکیبی از نظارت رفتاری، تحلیل داده و کنترل‌های پیشگیرانه، از خروج ناخواسته یا عمدی اطلاعات حساس جلوگیری می‌کند. این سیستم با کشف خودکار محتوا، بازرسی دیجیتال پیشرفته و تحلیل مبتنی بر زمینه، انواع داده‌های محرمانه و دارایی‌های فکری سازمان را شناسایی و طبقه‌بندی می‌کند.
پس از تعریف قوانین و سیاست‌های امنیتی، Teramind فعالیت کاربران را به‌صورت لحظه‌ای پایش کرده و هر رفتار مخاطره‌آمیز را با سیاست‌های DLP مقایسه می‌کند. در صورت رخداد مغایرت، اقدامات پیشگیرانه به‌صورت خودکار اجرا می‌شود؛ از جمله توقف فعالیت، مسدودسازی کاربر، ارسال هشدار فوری به مدیران یا درخواست تأیید مدیریتی.
این رویکرد یک لایه‌ی حفاظتی قدرتمند ایجاد می‌کند که ریسک نشت داده را به حداقل رسانده و انطباق سازمان با الزامات امنیتی را تضمین می‌نماید.



Teramind DLP: یک پلتفرم یکپارچه برای پیشگیری از نشت داده، نظارت کاربر و شناسایی تهدیدهای داخلی

راهکار Teramind DLP با رویکردی «کاربرمحور» و «نقطه‌پایانی»، فراتر از سیستم‌های سنتی پیشگیری از نشت داده عمل می‌کند. این پلتفرم با اتکا به تحلیل رفتار هوشمند، قادر است عوامل انسانی مانند خطاهای کاربری، اقدامات مخاطره‌آمیز یا سوءنیت را شناسایی کرده و از بروز نقض داده و خروج اطلاعات جلوگیری کند.

Teramind DLP با فراهم‌سازی بالاترین سطح بازگشت سرمایه، نیازهای امنیتی سازمان‌ها در هر اندازه‌ای را پوشش می‌دهد؛ از کسب‌وکارهای کوچک و متوسط (SMB) گرفته تا سازمان‌های بزرگ (Enterprise) و نهادهای دولتی که با چالش‌های نشت داده، امنیت سایبری و تهدیدهای داخلی مواجه هستند.

همچنین قابلیت‌های مدیریت انطباق (Compliance Management) در Teramind، سازمان را در تطبیق با استانداردها و مقررات مهمی همچون PCI DSS، HIPAA، GDPR و ISO 27001 یاری می‌کند.

Teramind DLP: ویژگی‌ها در یک نگاه

نظارت جامع بر فعالیت کاربران (User Activity Monitoring)

Teramind به‌صورت جامع تمامی فعالیت‌های کاربران را، از جمله کاربران داخلی، کاربران دارای دسترسی‌های سطح‌بالا (Privileged Users) و همچنین فروشندگان و پیمانکاران شخص ثالث، در بیش از 12 شاخص و شیء سیستمی پایش می‌کند. این نظارت شامل مواردی مانند وب‌سایت‌ها، برنامه‌های کاربردی، کلیدهای فشرده‌شده (Keystrokes)، پیام‌رسان‌های فوری (IM)، ایمیل، ترافیک شبکه و بسیاری فعالیت‌های دیگر است.این سطح از پایش دقیق به سازمان امکان می‌دهد رفتار کاربران را شفاف‌تر ردیابی کرده و هرگونه فعالیت مشکوک، ناخواسته یا پرخطر را سریعاً شناسایی نماید.

موتور قدرتمند سیاست‌ها و قوانین

Teramind همراه با صدها قانون، الگو و دسته‌بندی داده آماده ارائه می‌شود. همچنین می‌توانید با استفاده از ویرایشگر بصری و کاربرپسند این پلتفرم، سیاست‌ها و قوانین اختصاصی مورد نیاز سازمان خود را به‌سادگی ایجاد و مدیریت کنید.

شناسایی تهدیدهای داخلی

Teramind با تکیه بر تحلیل هوشمند رفتار کاربر و قابلیت‌هایی مانند ضبط و بازپخش جلسات، هشدارهای لحظه‌ای و گزارش‌های غیرقابل‌تغییر، هرگونه رفتار مشکوک یا خطرساز را پیش از تبدیل شدن به یک بحران شناسایی می‌کند. این رویکرد به سازمان کمک می‌کند تا تهدیدهای داخلی را به‌موقع تشخیص داده و از وقوع خسارت‌های جدی جلوگیری کند

اثرانگشت‌گذاری و برچسب‌گذاری

Teramind با بهره‌گیری از قابلیت‌های پیشرفته اثرانگشت‌گذاری و برچسب‌گذاری، اسناد و فایل‌های حساس را به‌طور دقیق شناسایی کرده و رفتار مرتبط با آن‌ها را پایش می‌کند.
این قابلیت امکان ردیابی مداوم داده‌ها را حتی در صورت تغییر، جابجایی یا نام‌گذاری مجدد فایل‌ها فراهم می‌سازد و به سازمان کمک می‌کند کنترل کاملی بر چرخه عمر اطلاعات حیاتی خود داشته باشد.

قابلیت تشخیص متن پیشرفته (Advanced OCR)

Teramind با استفاده از تشخیص متن پیشرفته (OCR)، پردازش زبان طبیعی (NLP) و عبارات منظم (RegEx)، امکان کشف لحظه‌ای محتوا را فراهم می‌کند. این فناوری قادر است داده‌های حساس را در تصاویر، برنامه‌های کاربردی و حتی فایل‌های ویدئویی شناسایی کند و از هرگونه خروج مخفیانه اطلاعات با روش‌های پنهان‌نگاری جلوگیری نماید.

نظارت بر کلیپ‌بورد (Clipboard Monitoring)

Teramind با ارائه قابلیت پایش و رهگیری کامل کلیپ‌بورد، امکان کنترل و محافظت از داده‌های حساس را در زمان انجام عملیات کپی/پیست فراهم می‌کند. این ویژگی از انتقال ناخواسته یا عمدی اطلاعات محرمانه از طریق کلیپ‌بورد جلوگیری کرده و لایه‌ای حیاتی از امنیت داده را در سطح کاربر ایجاد می‌کند.

کشف و طبقه‌بندی محتوا

اطلاعات حساس از منابع ساختاریافته و غیرساختاریافته شناسایی و طبقه‌بندی می‌شوند. قالب‌های داخلی شامل اطلاعات هویتی شخصی (PII)، اطلاعات سلامت (PHI)، اطلاعات مالی (PFI) و سایر موارد است.

مدیریت انطباق

Teramind به‌طور داخلی از انطباق با استانداردها و مقرراتی مانند ISO 27001، PCI DSS، HIPAA، GDPR و سایر الزامات پشتیبانی می‌کند.
با استفاده از موتور قدرتمند قوانین و سیاست‌ها و امکانات گسترده نظارت و گزارش‌دهی، این سیستم به‌راحتی می‌تواند برای پشتیبانی از سایر الزامات نظارتی سازمان نیز تنظیم شود.

مدیریت ریسک

کاربران پرخطر، سیاست‌های پرخطر و اشیاء سیستمی حساس از طریق داشبورد اختصاصی ریسک (Risk Dashboard) شناسایی می‌شوند. امتیازدهی ریسک پیشرفته (Sophisticated Risk Scoring) به شما امکان می‌دهد مناطق پرخطر را اولویت‌بندی کرده و منابع خود را برای کاهش ریسک در آن‌ها متمرکز نمایید.

علل، تأثیرات و فراوانی نشت داده‌ها، اثبات می‌کند که کسب‌وکارها به پیشگیری از، از دست رفتن داده‌ها (Data Loss Prevention) نیاز دارند.

امتیازات بالای کاربران (User Privilege) می‌تواند داده‌های حساس را در معرض خطر قرار دهد.

بر اساس یک نظرسنجی آنلاین از 400,000 عضو توسط Cybersecurity Insiders، که در گزارش «تهدید داخلی 2018» منتشر شد، روشن گردیده است که کاربران دارای دسترسی ویژه نقش مهمی در بروز خطرات داخلی ایفا می‌کنند.

دسترسی بیش از حد	37%
افزایش حجم داده‌های حساس	34%

زیان مالی ناشی از نقض داده‌ها بسیار چشمگیر است.

مطالعه‌ای که در سال 2018 توسط مؤسسه پونمون (Ponemon Institute) انجام شد، نشان می‌دهد که میانگین هزینه هر نقض داده با 6.4٪ افزایش به محدوده‌ای بین 3.86 میلیون تا 350 میلیون دلار رسیده است.

میانگین هزینه هر رخنه داده / نشت اطلاعات	$3.86M
برای نقض‌های امنیتی گسترده‌تر	$350M

زیان‌های مرتبط با سرقت مالکیت فکری (IP) در حملات سایبری، خسارت های قابل توجهی را به شرکت‌ها در سطح جهانی وارد می‌کند.

بر اساس برآوردهای شرکت مک‌آفی (McAfee)، زیان سالانه ایالات متحده بر اثر جرایم سایبری مرتبط با سرقت مالکیت فکری حدود 12 میلیارد دلار است؛ این رقم در سطح جهانی نیز بین 50 تا 60 میلیارد دلار تخمین زده می‌شود.

این مقدار، سقف تخمینی زیان سالانه جهانی مرتبط با مالکیت فکری (IP) محسوب می‌شود.	~60B

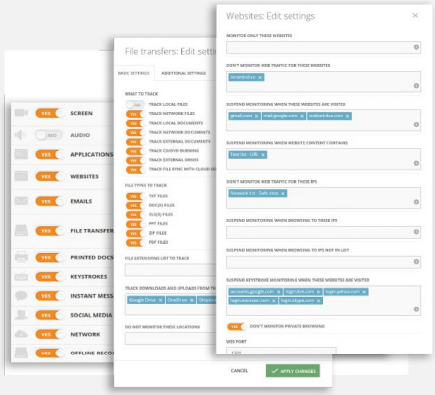
حوادث نشت داده‌ها با سرعتی نگران کننده در حال افزایش است.

بر اساس گزارش پاسخ‌دهندگان یک نظرسنجی فدرال در سال 2018، نرخ نقض داده‌ها به 57 درصد رسیده است؛ رقمی که بیش از سه برابر میزان ثبت‌شده در دو سال قبل است.

افزایش نقض‌های امنیتی در طی دو سال گذشته	300%

Teramind DLP؛ ارزش‌آفرینی فوری برای کسب‌وکار

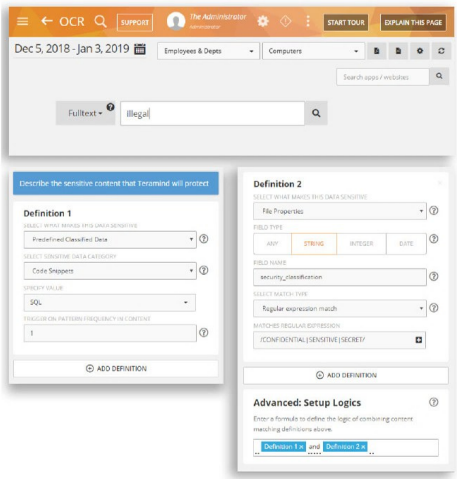
مشاهده‌پذیری جامع و کنترل کامل داده در سراسر سازمان



Teramind تمامی فعالیت‌های کاربران روی بیش از 12 شیء، از جمله برنامه‌ها، وب‌سایت‌ها، فایل‌ها و ایمیل‌ها را نظارت می‌کند.
فعالیت‌ها، هشدارها و شاخص‌های امنیتی را در کنسول مرکزی مشاهده و مدیریت کنید.

کنترل دقیق دسترسی به داده‌ها—چه کسی، چه زمانی و چگونه—از طریق داشبورد DLP قدرتمند و کاربرپسند امکان‌پذیر است.
با ابزارک‌های کشیدن و رها کردن، داشبورد سازمانی خود را بسازید و حتی از طریق تلفن همراه یا تبلت به مشاهده‌پذیری و کنترل کامل داده ها دسترسی داشته باشید.

کشف و طبقه‌بندی خودکار داده‌های حساس

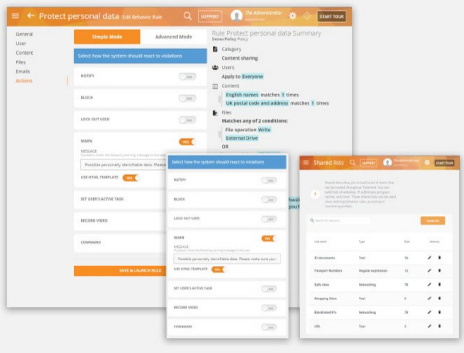


Teramind با قالب‌های داخلی برای انواع داده‌های حساس مانند PII، PHI، PFI، OGD، GSCP و کدهای ویژه ارائه می‌شود.

دسته‌بندی‌های سفارشی را می‌توان با عبارات منظم (RegEx) و پردازش زبان طبیعی (NLP) تعریف کرد.

با ترکیب تشخیص متن پیشرفته (OCR)، اثرانگشت‌گذاری و برچسب گذاری و تحلیل منطق، منشأ و ویژگی‌های فایل‌ها، اطلاعات حساس را در داده‌های ساختاریافته، غیرساختاریافته و حتی تصاویر به‌صورت در لحظه کشف کنید.

ویرایشگر قدرتمند سیاست‌ها و قوانین

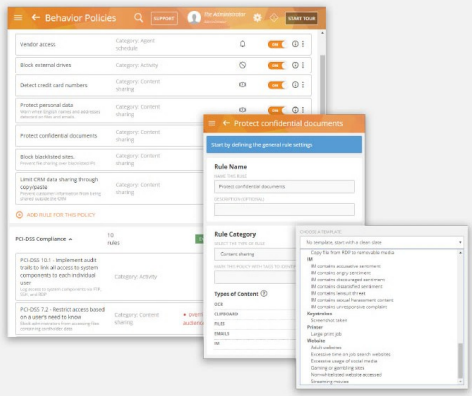


موتور انعطاف‌پذیر قوانین Teramind امکان تعریف سیاست‌های پیشرفته DLP را برای هر سازمان فراهم می‌کند.

ویرایشگر بصری (Visual Policy & Rules Editor) به مدیران اجازه می دهد تا قوانین پیچیده را برای موارد استفاده خاص تعریف کرده و فعالیت‌های کاربران را روی دیسک، ضربات کلید، برنامه‌ها، پیام‌رسانی فوری، شبکه‌های اجتماعی و سایر منابع نظارت کنند.

با استفاده از لیست‌های داخلی، عبارات منظم (RegEx)، الگوهای داده/متن یا پروتکل‌های شبکه‌ای می‌توان لیست‌های سیاه/سفید برای مالکیت فکری، وب‌سایت‌ها و برنامه‌های ایمن یا محدودشده ایجاد کرد و کنترل کاملی بر دسترسی‌ها داشت.

سیاست‌ها و قوانین DLP از پیش تعریف‌شده

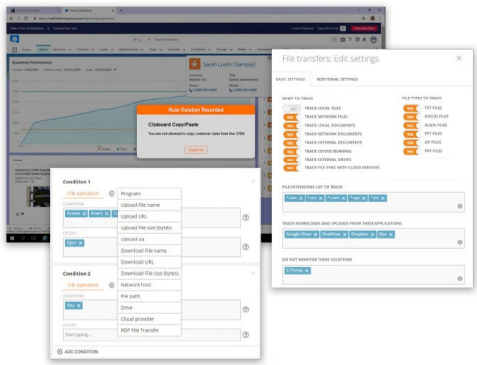


هسته پلتفرم Teramind اتوماسیون قدرتمند آن است و بیش از 200 سیاست و قانون از پیش تعریف‌شده ارائه می‌دهد.

این سیاست‌ها شامل مسدود کردن ایمیل‌های حاوی کلمات حساس، جلوگیری از آپلود اسناد محرمانه، شناسایی ضبط صفحه نمایش، محدودسازی استفاده از درایوهای خارجی و سایر موارد است.

این قالب‌ها تقریباً تمامی موارد استفاده DLP، شناسایی تهدید داخلی و الزامات انطباق (Compliance) را پوشش می‌دهند. کافی است یک سیاست یا قالب را انتخاب کنید تا تمامی تعاریف داده، منبع محتوا و شروط به‌صورت خودکار آماده و قابل ویرایش شوند.

جلوگیری از نشت داده‌ها از طریق درایوهای خارجی، شبکه و خدمات ابری

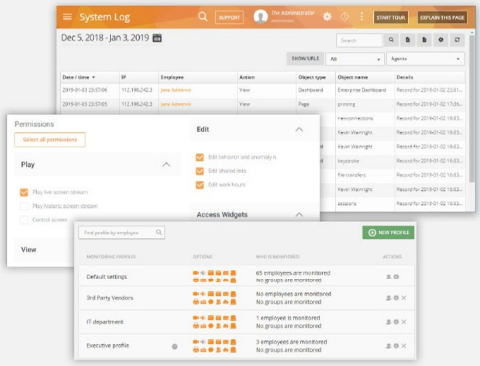


با قوانین انتقال فایل (File Transfer Rules) می‌توانید دسترسی به درایوهای خارجی را محدود کنید، و با قوانین کلیپ‌بورد (Clipboard Rules) از اشتراک‌گذاری اطلاعات محرمانه مانند داده‌های مشتری خارج از سیستم CRM جلوگیری نمایید.

عملیات دانلود و آپلود در فضای ابری نیز برای انواع فایل‌ها یا همه فایل‌ها قابل محدودسازی است. علاوه بر این، Teramind می‌تواند رسانه‌های اجتماعی و پیام‌رسان‌های فوری را نظارت و در صورت تشخیص نشت داده بالقوه، اقدامات لازم را به‌طور خودکار انجام دهد.

با صدها Use Case تعریف‌شده، Teramind به‌صورت فعال از داده‌های شما در برابر نشت یا سوءاستفاده‌های عمدی و تصادفی محافظت می‌کند.

پیشگیری از از دست رفتن داده‌ها در برابر تهدیدهای داخلی

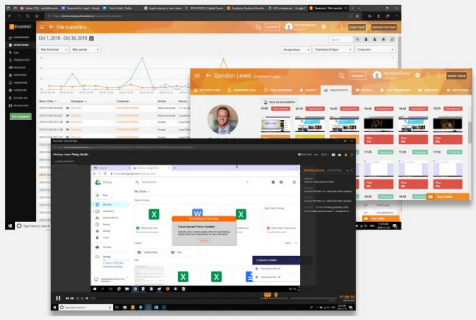


Teramind امکان ایجاد پروفایل‌های کاربری برای کاربران عادی، کاربران دارای امتیاز بالا و کاربران قراردادی یا خارجی را فراهم می‌کند و مشخص می‌سازد که هر پروفایل به کدام داده‌ها و منابع سیستم دسترسی دارد.

با استفاده از سیاست‌های رفتاری (Behavior Policies)، دسترسی به اطلاعات حساس بر اساس سیاست‌های امنیتی سازمان یا اصل نیاز به دانستن (Need-to-Know) کنترل و تفکیک می‌شود.

همچنین می‌توان قوانینی تعریف کرد تا در صورت هرگونه فعالیت مشکوک کاربران دارای امتیاز مانند تغییرات غیرمجاز در پیکربندی سیستم یا ایجاد حساب‌های پشتیبان (Backdoor Accounts) مسئولین به صورت فوری اطلاع‌رسانی شوند.

حسابرسی نقض داده‌ها با شواهد پزشکی قانونی

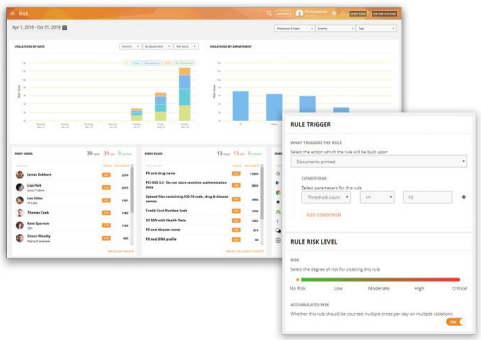


تمامی هشدارها و رویدادهای نقض داده، همراه با اقدامات انجام شده، قابل مشاهده و پیگیری هستند.

پیام‌های هشدار قابل تنظیم به کاربران اطلاع می‌دهد که در حال نقض قوانین مدیریت داده‌های حساس هستند و با ارائه بازخورد و اعلان به موقع، رفتار اصلاحی ترویج می‌شود.

ضبط جلسات (Session Recording) و بازپخش تاریخچه (History Play-back) امکان مشاهده فعالیت دسکتاپ کاربران را برای حسابرسی و جمع آوری شواهد فراهم می‌کند.

شناسایی و مدیریت ریسک داده

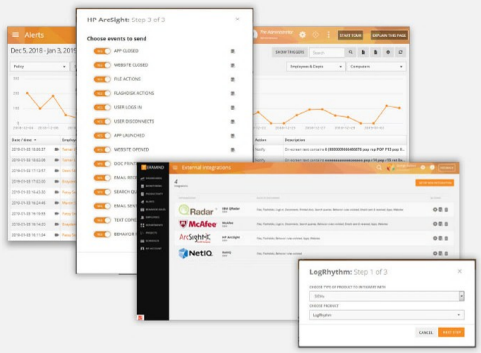


Teramind با داشبورد ریسک اختصاصی (Dedicated Risk Dashboard) امکان ارزیابی ریسک در سطح کل سازمان را فراهم می‌کند.

ریسک‌ها را می‌توان بر اساس کاربران، دپارتمان‌ها یا محتوا دسته‌بندی کرد و گزارش‌ها را بر اساس شدت ریسک‌ها یا تعداد تخلفات امنیتی استخراج نمود.

امتیازهای ریسک منحصر به فرد (Unique Risk Scores) به شناسایی کاربران یا سیاست‌های پرخطر کمک می‌کند تا برنامه‌های موثری برای کاهش و مدیریت ریسک‌ها (Risk Treatment) تدوین شود.

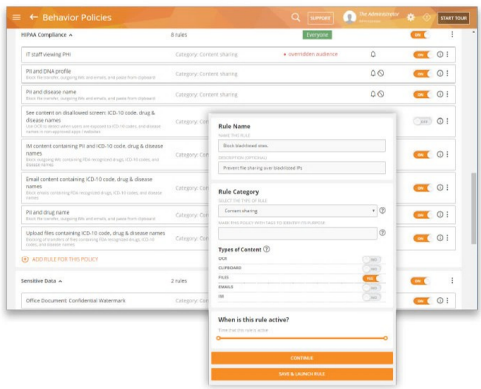
ارکستراسیون امنیتی یکپارچه با سیستم‌های SIEM و تحلیل



رویدادها و گزارش‌های Teramind می‌توانند به سیستم‌های SIEM و ابزارهای تحلیلی مانند HP ArcSight، Splunk، IBM QRadar، McAfee ESM، Log-Rhythm، NetIQ Sentinel و غیره ارسال شوند، تا اطلاعات تهدید (Threat Intelligence) به تیم امنیتی یا سایر دپارتمان‌ها منتقل شود.

Teramind همچنین با ارائه APIهای RESTful مبتنی بر چارچوب ساده Token/Endpoint، امکان اتصال آسان به هر برنامه‌ای که از وب‌سرویس پشتیبانی می‌کند را فراهم می‌نماید.

مدیریت انطباق و حریم خصوصی



Teramind به‌طور داخلی از استانداردهای انطباق مقرراتی مانند GDPR، HIPAA، PCI DSS، ISO 27001، NIST، FISMA و دیگر مقررات پشتیبانی می‌کند.

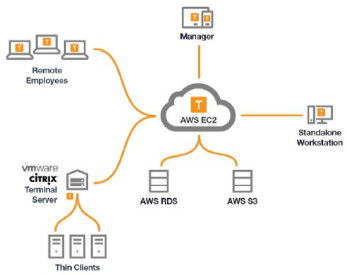
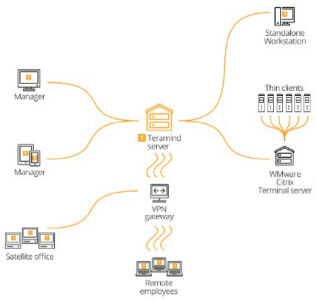
هشدارهای دقیق، گزارش‌های جلسات (Session Logs)، تحلیل ناهنجاری و ریسک، و گزارش‌های رویدادها به شما کمک می‌کنند تا پیروی از بهترین شیوه‌های امنیت داده را اثبات کرده و برای الزامات گزارش‌دهی نقض امنیتی و بار اثبات (Burden of Proof) آماده باشید.

علاوه بر این، می‌توان ویژگی‌های نظارتی Teramind را طوری تنظیم کرد که الزامات حریم خصوصی داده‌های شخصی (Personal Data Privacy) مطابق با GDPR و مقررات مشابه رعایت شوند.

سازگار با همه پلتفرم‌های اصلی

Windows 7 & Up	Citrix XenApp® & XenDesk®	Windows Server 2008 & Up	VMware Horizon	Mac OSX

استقرار انعطاف‌پذیر برای هر نوع محیط

Private Cloud	On-Premise	Cloud
		
از پیاده‌سازی ابری خصوصی، امن و مقیاس‌پذیر Teramind بهره ببرید، شامل AWS، Google Cloud، Azure و سایر پلتفرم‌ها.	کنترل کامل پیاده‌سازی Teramind با اتصال به LDAP، می‌توانید به راحتی مشخص کنید که هر سیاست و قانون برای کدام کاربران یا گروه‌ها اعمال شود و مدیریت دسترسی‌ها را به‌طور کامل در اختیار داشته باشید.	بدون نیاز به نگهداری سرور، فقط کافی است Agents Teramind را روی دستگاه‌های موردنظر نصب کنید، کاربران و سیاست‌ها را تنظیم نمایید، و بقیه امور مدیریت و نگهداری را به Teramind بسپارید.

درباره Teramind

Teramind که از سال 2014 فعالیت خود را آغاز کرده، امروز یکی از پیشگامان جهانی در حوزه نظارت بر فعالیت کاربران، تحلیل رفتار، شناسایی تهدیدهای داخلی و پیشگیری از از دست رفتن داده‌ها (DLP) است. بیش از 2,000 سازمان در صنایع مختلف در سراسر جهان به این پلتفرم اعتماد دارند. دفتر مرکزی Teramind در میامی، فلوریدا واقع شده و خدمات فروش و پشتیبانی آن به‌صورت جهانی ارائه می‌شود.