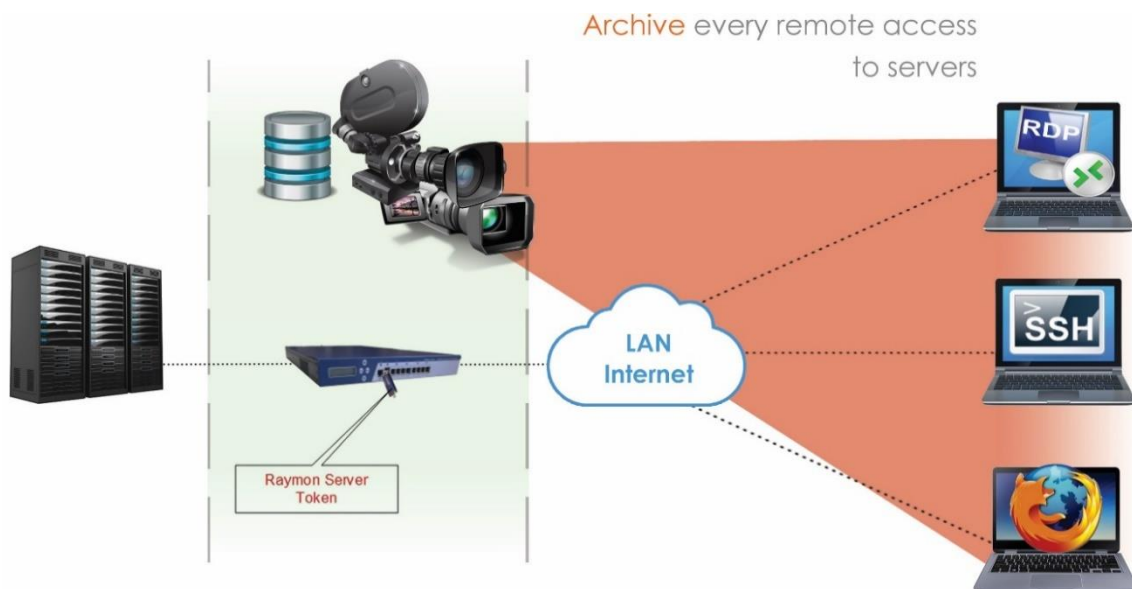


## رایمون

### سامانه دیده‌بانی و پایش دسترسی‌های راه دور

نظارت و کنترل بر دسترسی‌های راه دور کاربران مجاز و پیمانکاران به تجهیزات مستقر در مراکز داده و منابع حساس شبکه سازمان اعم از سرورها، تجهیزات شبکه ای و امنیتی از نگرانی‌های جدی مدیران سازمانی محسوب می‌گردد. این کاربران با استفاده از پروتکل‌های مختلف دسترسی راه دور نظیر *RDP, Telnet, SSH* و *VNC* به تجهیزات حساس سازمانی متصل میشوند. این در حالیست که معمولاً این پروتکلها فاقد امکانات کیفی ثبت رخداد و رویدادنگاری بوده و لذا مدیر امنیت سازمان، نظارت لازم را بر اینگونه دسترسیها نخواهد داشت.

سامانه رایمون، راهکاری است که بمنظور مدیریت دسترسی‌های ویژه (*Privileged Access Management*) ارایه شده تا به سهولت و بدون نیاز به تغییر در فرآیندهای سازمانی، سطح نظارت بالایی را بر اینگونه دسترسی‌های راه دور فراهم آورد. این سامانه امکان نظارت و پایش بر دسترسی‌های راه دور را از طریق ضبط و نمایش فیلم، ثبت رخداد و امکان جستجو بر جلسات فراهم مینماید. همچنین مدیر قادرست سیاستهای فیلترینگ لازم را نیز بر مبنای امکان اجرای برنامه ها و فرامین در جلسات دسترسی اعمال نماید.



(۱)

## ویژگیهای رایمون

### احراز اصالت و کنترل دسترسی کاربران

- احراز اصالت کاربران بصورت محلی
- احراز اصالت از طریق اکتیو دایرکتوری
- تعریف گروه نظارت و بازرسی بر جلسات نشست کاربران

### پشتیبانی از پروتکل‌های دسترسی راه دور رایج

- RDP
- Telnet
- SSH

### نظارت بر جلسات نشست کاربران با ذخیره سازی بصورت فیلم

- ذخیره سازی هر نشست کاربر بصورت فیلم مجزا
- رمزنگاری فیلم های ضبط شده

### امکان جستجو در فیلمهای جلسات نشست

- قابلیت جستجو در عناوین پنجره‌های باز شده
- قابلیت جستجو بر متون مشاهده شده کاربران
- قابلیت جستجو در واژگان تایپ شده کاربران
- اندیس گذاری تصاویر به منظور افزایش سرعت جستجو

### نظارت زنده بر جلسات نشست کاربران

- امکان مانیتورینگ زنده فعالیت کاربر
- امکان قطع نشست کاربر

### پشتیبانی از عملکرد کاملا شفاف

- عدم نیاز به نصب نرم افزار در سمت سرور و یا رایانه کاربران
- عدم آگاهی کاربران راه دور از وجود رایمون
- جلوگیری از تشخیص حضور رایمون در شبکه
- عدم تاثیر بر کارایی سرورها
- عدم نیاز به آموزش کاربران

### پشتیبانی از عملکرد غیر شفاف

- امکان مشاهده و انتخاب سرورهای قابل دسترس کاربر
- هشدار به کاربران جهت وجود فرآیندهای نظارتی
- عدم نیاز به نرم افزارهای سمت کاربر مانند *putty* و *tightVNC*

### امکان فیلترینگ

- فیلترینگ فرامین
- فیلترینگ برنامه های اجرایی

### امکان نسخه برداری از اطلاعات مبادله شده

- نسخه برداری از فایل ها و اطلاعات مبادله شده کاربران با سرورها

### ثبت رخدادها

- ثبت رخدادهای مهم سیستمی و شبکه ای
- ثبت رخدادهای عملکردی کاربران

### دسترسی پذیری بالا

- قابلیت دسترسی بالا و مقاومت در برابر خرابی
- امکان همگام سازی خودکار ما بین سرورهای افزونه

### تعامل با سامانه های مدیریت رخداد و حوادث امنیتی

- امکان ارسال رخدادها برای سامانه های *SIEM* (نظیر راوین)
- ارائه گزارشات متنوع تحلیل رویدادهای امنیتی

### کنسول مدیریتی

- کنسول مدیریتی مبتنی بر وب

## کاربردهای رایمون

- نظارت تصویری بر دسترسی راه دور کاربران به سرورها و تجهیزات حساس شبکه
- رهگیری دسترسی و فعالیت کاربران راه دور به منابع شبکه
- امکان جستجو در فیلمهای جلسات نشست
- کنترل و فیلترینگ دسترسیهای راه دور به منابع شبکه سازمان
- نظارت بر فعالیت‌های پیمانکاران

## اجزای رایمون

### سامانه سرور رایمون

سرور رایمون بصورت سخت افزاری و همچنین ماشین مجازی (VM) قابل ارایه میباشد. کلیه سیاستهای کنترلی و نظارتی کاربران مجاز راه دور در سرور رایمون تعریف شده و تنظیمات این سامانه از طریق کنسول مدیریتی مبتنی بر وب انجام میشود



### نرم افزار پخش کننده رایمون

از طریق این نرم افزار، مدیر امنیت سازمان فیلمهای ضبط شده مربوط به جلسات دسترسی کاربران به تجهیزات حساس سازمانی را مشاهده مینمایند



### کنسول مدیریتی رایمون

از طریق این نرم افزار مدیر قادرست علاوه بر تنظیمات سیستمی و شبکه ای اقدام به تعریف سیاستهای فیلترینگ و جستجو در جلسات مختلف دسترسی نماید

