PANDA
SECURITY

ضدویروس
مانیتورینگ
HELP DESK

# PANDA CLOUDFUSION

pandacloudsecurity.com

شبکه... در دستان امن و پرتوان شماست!

SECURITY, MANAGEMNENT AND SUPPORT FOR YOUR ENTIRE NETWORK
AT ANYTIME, FROM ANYWHERE YOU ARE!


شرکت ایمن رایانه پندار
مشاور و مجری پروژه های شبکه و امنیت شبکه
نماینده انحصاری ضدویروس پاندا در ایران

۰۲۱ - ۸۸۱۷۰۸۰۱ - ۵
tellus@pandasecurity.ir

## نقاط قوت ما ...

شرکت ایمن رایانه پندار، با بیش از ۱۷ سال سابقه خدمت رسانی در حوزه امنیت فناوری اطلاعات و همکاری رسمی و انحصاری با کمپانی Panda Security اسپانیا بعنوان یکی از برترین شرکتهای بین المللی فعال در این حوزه، مفتخر است تا لایسنس های نرم افزاری PANDA را در حوزه ایران و کشور های جنوب خلیج فارس ارائه نماید. از وجوه تمایز این شرکت نسبت به سایر رقبا، میتوان به موارد ذیل اشاره نمود:

- ثبت لایسنس نرم افزارها بلافاصله و بنام مشترک.
- انحصار نمایندگی در منطقه.
- عدم شمول تحریم های بین المللی و دریافت فایل های بروزرسانی و همچنین خدمات پشتیبانی از طریق وب سایت PANDA SECURITY اسپانیا بصورت مستقیم.
- سبک بودن نرم افزارها و عدم نیاز به صرف هزینه های گزاف جهت ارتقاء سخت افزارهای شبکه.
- ارائه خدمات پاکسازی کلیه سیستم ها از وجود کدهای مخرب.
- نصب و راه اندازی مجدد نرم افزار بر روی کلیه سرورها و ایستگاه های کاری بدون دریافت هزینه مجزا.
- خدمات و پشتیبانی فنی بصورت تلفنی، ریموت و حضوری و بدون دریافت هزینه جداگانه. (خدمات پشتیبانی فنی نرم افزار امنیت شبکه پاندا جزء لاینفک و ضروری نرم افزار مذکور می باشد.)
- آموزش رایگان مدیر / مسئول شبکه در ارتباط با بکارگیری استانداردهای نرم افزار.
- ارسال رایگان آخرین نگارش نرم افزار برای مشترک از طریق پست سفارشی.
- ارائه اخبار امنیت انفورماتیک به زبان فارسی از طریق وب سایت و ایمیل. ( وب سایت این شرکت WWW.PANDASECURITY.IR در سال ۸۹ بعنوان یکی از ۵ وب سایت برتر شرکتهای خصوصی در کشور برگزیده شد.
- سرویس اعلام هشدار از طریق وب سایت و ایمیل.
- امکان ارائه کلیه راهکارهای امنیت اطلاعات بصورت یکپارچه و با تخفیفات ویژه به مشترکین، از قبیل نصب دامین و اکتیو دایرکتوری، پیاده سازی سیاست های دامین، سرورWSUS، ارائه و پشتیبانی فایروال سخت افزاری و دستگاههای UTM و SCM، تست های نفوذ پذیری و طراحی شبکه بر اساس استانداردهای امنیت اطلاعات، آموزش مفاهیم امنیت شبکه و ...

ضدویروس
مانیتورینگ
HELP DESK

Panda Cloud Fusion

## قابلیت ها و امکانات (۱)

### Cloud-based Console :

Panda Cloud Office Protection مجهز به یک کنسول محلی ست که روی یکی از سرورهای شبکه نصب میشود و نیز یک کنسول ابری که در هر زمان و از هر کجای جهان قابل دسترسی و مدیریت می باشد. سادگی کنسول های این نرم افزار از وجوه برتری آن ا ست که در عین حال تمامی امکانات مورد نیاز جهت نصب و مدیریت نرم افزار و تهیه گزارشات مختلف گرافیکی، در این دو کنسول در دسترس است.

### AntiVirus, AntiWorm, AntiTrojan / AntiExploit :

شناسـايي و پاکسـازی بيـش از ۲۵۰ میلیون نوع مختلف از ویروسـها، کرمهاي رایانـه ای و نرم افزارهای تـروژان، با قابلیت ترمیم فایلهـاي صدمه دیده و پاکسـازی اثرات مخرب احتمالی بدافزارها. موتور ضدویروس پاندا موفق به کسـب جوایز بیشماری از معتبرترین مراکز تست و ارزیابی نرم افزارهای امنیتی شده که جدیدترین آن ها گواهی Advanced+ و دریافت عنوان قدرتمندترین موتور ضدویروس در نیمه سال ۲۰۱٤ از طرف مرکز معتبر AV-Comparatives و عنوان قوی ترین ضدویروس سال از طرف نشریه PC Magazine می باشد.
تکنولوژی Anti-Exploit در این نرم افزار، وظیفه کشف حفره های جدید امنیتی در سیستم های عامل و نرم افزارهای کاربردی، هشدار به مدیر شبکه و نیز ارائه راهکار برای برطرف کردن این آسیب پذیریها را بر عهده دارد.

### Integration of Corporate AntiSpyware :

یکپارچگی ماژول AntiSpyware در نرم افزار ضدویروس تحت شبکه پاندا، که موفق شده در جدیدترین (آخرین) تستهای انجام شده توسط AV-Comparatives، با امتیاز ۹۹/۹٪ عنوان قدرتمند ترین ابزار ضد جاسوسی در اینترنت را به خود احتصاص دهد.

### Anti-Hacking Tools and Anti-Keylogger:

سیستم اختصاصی نرم افزار پاندا برای کشف و شناسايي نفوذهای غیرمجاز و همچنین کدهای کلیدخوان که از طریق ثبت کلیدهای فشرده شده، عبارت های تایپ شده توسط کاربر را سرقت می کنند. این عبارت ها می توانند شامل رمزهای عبور، نام های کاربری و یا سایر اطلاعات حساس سازمانی باشند.

### Anti-Spam and Anti-Phishing:

طبق آمارهای پاندا، دست کم ۹۰ درصد از کل نامه های الکترونیک ورودی به مراکز سازمانی، هرزنامه هستند. بنابراین با نصب ماژول ضد هرزنامه که بر روي سـرور Exchange و همچنیـن بر روي سیسـتم هاي نهایی کاربران مسـتقر می شـود، شـبکه سـازمانی شـما در برابـر هجوم نامه هاي ناخواسـته الکترونیکي که بسیاری از آن ها آلوده به ویروس و بدافزار هستند، مصون می ماند. علاوه بر این، کارکنان سازمانی هم در برابر حملات Phishing کاملاً امن خواهند بود. این دسته از حملات، به عنوان یکی از شایع ترین روش های سرقت و فریب کاربران اینترنت محسوب می شوند که البته همگی توسط سد دفاعی نرم افزارهای پاندا شناسایی و متوقف می شوند.

### Anti-Dialer and Anti-Adware:

جلوگیري از ورود و فعالیت کدهاي شماره گیر (نوع خاص و آزارنده ای از نرم افزارهای مخرب) و همچنین جلوگیري از نمایش تبلیغات ناخواسته و پی در پـی اینترنتـی از جمله امکانات مهم نرم افزار آنتي ویروس پاندا مي باشـد. فعالیت Cookie ها نیز توسـط این نرم افزار بطـور کامل کنترل و در صورت لزوم مسدود می شود.

ضدویروس
مانیتورینگ
HELP DESK
Panda Cloud Fusion

## قابلیت ها و امکانات (۲)

### Anti-Rootkit:

روت کیت ها به خودی خود مخرب نیستند اما برای پنهان کردن پردازش های مخرب و عملکرد ویروس ها از دید نرم افزارهای امنیتی، بهترین گزینه هستند. اغلب ویروس های جدید و بسیار مخرب، نظیر استاکس نت از این ابزار برای پنهان شدن در سیستم استفاده می کنند. Panda Anti-Rootkit قدرتمندترین ابزار امنیتی برای کشف و پاکسازی روتکیت های مخرب محسوب می شود که به عنوان بهترین ابزار ضد- روتکیت توسط نشریه معتبر PC-Magazine معرفی شده است.

### Malware quarantine :

این تکنولوژی کمک می کند تا نرم افزار ضدویروس، فایل سالم را اشتباهاً به عنوان فایل مخرب حذف نکند. موتور ضدویروس پاندا به مدد این تکنولوژی و از طرف بسیاری از مؤسسات تست آنتی ویروس، بعنوان بی اشتباه ترین موتور ضدبدافزار شناخته شده است.

### Personal Firewall:

به منظور پیشگیری از حملات هک و آن دسته حملاتی که نرم افزار آنتی ویروس به تنهایی قادر به جلوگیری از آنها نمي باشد، فایروال پاندا یکی از بهترین راهکارهای حفاظتی در لایه های عمیق تر و پایین تر شبکه است.

### IPS (Intrusion Prevention System)

نرم افزارهای پاندا دارای یکی از قوی ترین ماژول های IPS هستند. IPS پاندا، ابزاری بازدارنده است که به منظور جلوگیري از رسیدن بسته های اطلاعاتی آلوده و مخرب، از طریق ترافیک اطلاعاتی شبکه (که حتی فایروال هم قادر به شناسایی آن ها نیست) به مقصد کاربران یا رایانه های حساس سازمان، بکار گرفته می شود.

### HIPS (Host Based Intrusion Prevention System)

سیستم تشخیص و مقابله با نفوذ مهاجم، مبتنی بر میزبان. این سیستم مي تواند از تغییر فایلها بر اثر حملات رایانه ای جلوگیریکند. بنا بر آخرین گزارش های تحلیلی منتشر شده درباره این نوع از سیستم های امنیتی، مؤسسه بزرگ تحقیقات آی تی گارتنر ، HIPS موجود در نرم افزارهای پاندا، به عنوان کامل ترین، مؤثرترین و قوی ترین سیستم HIPS جهان معرفی شده است.

### IDS (Intrusion Detection System)

سیستم کشف ترافیک های غیر مجاز که پس از شناسایی بسته های مخرب یا آلوده، هشدار و اخطار لازم را به مدیر شبکه اعلام می کند.

### Web / Content Filtering

جلوگیري از دسترسي کاربران به صفحات وب (URL)؛ با بهره گیری از این ماژول، کنترل دسترسی کارکنان سازمانی به محتویات اینترنتی غیرمجاز به بهترین نحو ممکن انجام می شود که این مسئله به نوبه خود موجب افزایش بازده کارکنان خواهد بود. و صفحات غیرمجاز افزایش میباید. هم چنین فیلترینگ اطلاعات ورودي به منظور جلوگیري از ورود محتویات اطلاعاتی ناخواسته و کدهاي مخرب ناشناخته در سرورها و ایستگاههای کاری نیز قابل اجراست.

### Mail Sending Control

کنترل میزان نامه های ارسالی و خروجی و نیز جلوگیری از قرار گرفتن دامین شرکت در لیست اسپمها.

ضدویروس
مانیتورینگ
HELP DESK
Panda Cloud Fusion

## قابلیت ها و امکانات (۳)

**Protection Against Buffer OverFlow:**
جلوگیری از سرریز شدن بافر توسط ویروس ها و کدهای مخرب. به عنوان مثال SASSER و BLASTERکه باعث اختلال و گاه توقف کامل در عملکرد های شبکه شرکت میشود.

**Blocking Actions :**
نـرم افزار آنتي ويروس پاندا قادر به جلوگيري از دسترسـي كدهاي مخرب به بخش های بسـيار مهم سيسـتم عامل مثـل ،.User Acc ، System Files Windows Services، Windows Registry و Com Components مي باشد.

**Protections of digitally-signed processes :**
حفاظت از پردازش ها و اطلاعاتی که داراي امضاي ديجيتال و ثبت شده هستند. این قابلیت به ویژه برای محافظت از فرایندهای حیاتی سیستم های سازمان و نیز نگهداشت شرایط عملیاتی و نرمال شبکه در مواقع بحرانی، مؤثر است.

**CPU Load Control :**
کنترل load (بار) منفی بر روی پردازنده های سخت افزاری و ظرفیت عملیاتی شبکه در زمان اسکن سیستم هاو پاکسازی ویروس ها

**Self-Diagnosis :**
کنترل عملکرد نرم افزار های ضد ویروس پاندا توسط فرایندهای حافظتی خاصی که درون این نرم افزارها گنجانده شده است. این یک ویژگی حیاتی برای جلوگیری از صدمه خوردن نرم افزار توسـط نفوذ کدهای مخرب اسـت. ( با توجه به این مسـئله که ویروسهاي چند ماه اخیر قادرند نرم افزارهاي آنتي ويروس را نيز غير فعال سازند).

**Device Control :**
بـرای ایجاد محدودیت در دسترسـی به ابزاری نظیـر 3G, removable storage drives, modem, ,USB, CD/DVD-ROM, Bluetooth image capture device و ... این ویژگی به مدیر شـبکه امکان می دهد تا کلیه ابزارهای جانبی که به سـرورها و کلاینت ها متصل میشـوند را مدیریت و در صورت نیاز، پورت های ارتباطی با این ابزارها را مسدود کنند تا از نشت اطلاعات به خارج از سازمان و نیز از ورود و انتشار آلودگی در شبکه پیشگیری شود.

**Internet Accounting :**
اختصاص اینترنت بصورت زمانی به کارکنان و ایجاد محدودیت در استفاده از پهنای باند اینترنت توسط آن ها

**Panda Collective Intelligence :**
این فن آوری با عنوان "هوش یکپارچه" ، بر مبنای اینترنت و تکنولوژی پیشـرفته ابر ابرعمل می کند و به عنوان یک گزینه مکمل امنیتی برای افزایش قدرت و سرعت موتور ضدویروس پاندا از آن استفاده می شود. با بهره گیری از این فن آوری، تمام کاربران اینترنت به صورت لحظه به لحظه به سرورهای امنیتی پاندا، متصل خواهند بود و در نتیجه همواره و هر لحظه بروز می شـوند. این یعنی بالاترین قدرت دفاعی در برابر ویروس ها و سـایر تهدیدهای اینترنتی. شـرکت پاندا سـکیوریتی با ابداع و بکارگیری این فن آوری موفق شـد تا در سال ۲۰۱۰ میلادی رتبه دوم برترین شرکت امنیتی جهان را از طرف نشریه بسیار معتبر the Wall Street Journal دریافت کند.

ضدویروس
مانیتورینگ
HELP DESK
Panda Cloud Fusion

## قابلیت ها و امکانات (٤)

### Monitoring:
مانیتورینگ جامع و نظارت بر زیر ساخت شبکه و تجهیزات مبتنی بر پروتکل SNMP؛ اعم از کلیه سرورها و کلاینت ها و همچنین مودمها، سوئیچ ها و روترها، پرینترها، اسکنرها و ... اطلاع دائم از وضعیت کاری کلاینت ها و وضعیت RAM Usage, CPU Usage, Hard Disk و... و نیز شرایط عملیاتی سرورها بصورت بهنگام (real-time) از قابلیت های دیگر نرم افزار میباشد.

### Ticket Support:
تمام کاربران سازمانی می توانند مشکلات سیستمی و یا اختلالات عملیاتی در آن ها را از طریق پیام های فوری درون شبکه ای به فارسی یا انگلیسی به مدیران شبکه اعلام کنند. کلیه این پیام ها به صورت تیکت های قابل پیگیری بر روی پنل مدیریتی نرم افزار پاندا قابل مشاهده و دسترسی خواهد بود.

### Patch Management:
تمام فایل های بروزرسانی و اصلاحیه های نرم افزاری سخت افزاری مربوط به سیستم های عامل، پلیرها، مرورگرها و ... با این قابلیت مهم نرم افزار پاندا قابل دریافت و نصب در شبکه می باشد.

### Software Deployment :
اگر بخواهید نرم افزارهای رایج شبکه مانند مرورگر ها، فلش پلیر، اکروبات ریدر و سایر نرم افزارهای کاربردی را در یک، چند یا همه سیستم های شبکه نصب کنید، نسخه به روز این قبیل برنامه ها در ComStore نرم افزار پاندا وجود دارد که می توانند با یک کلیک روی سیستمهای مورد نظرنصب شوند. علاوه بر این، در صورت نیاز به نصب هرگونه برنامه دیگر و یا افزودن Script یا Component سفارشی شده، کافیست آنرا به ComStore اضافه کنید و نصب ساده آن ها را در شبکه خود مشاهده نمایید.
قابل توضیح این که هرگونه نرم افزار در فرمت exe. و اسکریپت های با فرمت msi. از طریق نرم افزار پاندا قابل نصب در شبکه می باشند.

### Asset Directory / Inventory :
شناسایی و ثبت تمام تجهیزات سخت افزاری شبکه با شماره سریال بهمراه نرم افزارهای موجود بر روی هر کدام از ااین سیستم ها. تهیه و بروز نگاه داشتن فهرست سخت افزارها و نرم افزارهای موجود در سازمان. هر نوع تغییری در این فهرست و یا در تنظیمات سخت افزاری و نرم افزاری تجهیزات فوراً به مدیر شبکه گزارش شده و فهرست Inventory به روز می گردد.

### Mobile Device Management :
امکان شناسایی، مانیتورینگ و رهگیری کاربران سیار شبکه که از طریق لپ تاپ و یا تلفن های هوشمند مبتنی بر Android و iOS به شبکه رایانه ای سازمان متصل هستند.

## درباره امنیت خدمات و نرم افزارهای مبتنی بر ابر پاندا

- تعریف پروفایل های امنیتی برای دسترسی به بخش ها و ماژول های مختلف خدمات ابری پاندا {برای سطوح مختلف مدیریتی }
- تعریف رمز های عبور قدرتمند؛ این رمز های عبور خود به صورت رمز گذاری شده در سرور های امن پاندا ذخیره می شوند.
- لزوم تغییر دوره ای رمزهای عبور در دوره های ۳۰و۶۰و۹۰ روزه؛ علاوه بر این قابلیت، تمام مدیران در سطوح مختلف مدیریتی خود میتوانند از روز های عبور مختلف استفاده کنند
- تعریف آدرس های IP اختصاصی برای دسترسی به خدمات ابری پاندا
- محدود کردن دسترسی به کنسول مدیریتی نرم افزار ا از طریق تعریف یک آدرس آی پی منحصر به فرد و یا یک رنج خاص از دامنه آی پی ها
- تعریف یک مدت زمان خاص برای انقضای دسترسی مدیران اصلی و فرعی به کنسول خدمات ابری پاندا
- تصدیق هویت بر اساس تکنولوژی TFA
- تمام خدمات مبتنی بر ابر پاندا برای افزایش ضریب امنیت در هنگام تشخیص و تصدیق هویت کاربران و مدیران و نیز تشخیص سطح دسترسی آنها با سرور های دارای تکنولوزی امنیتی RAIDUIS یکپارچه هستند .
- ارتباط های مبتنی بر SSL / TLS
- ارتباط های کاربر با سرور های پاندا و هر گونه اطلاعات مبادله شده میان آنها با استفاده از پروتکل های قدرتمند رمز گذاری مانند SSL / TSL ۱,۰ ۲۵۶ بیت رمز گذاری می شوند .... این پروتکل ها بهترین استاندارد های امنیتی حال حاضر برای ارتباط های اینترنتی حتی در حوزه مالی و تجاری محسوب می شود.
- عدم ذخیره سازی اطلاعات حساس مانن داده های مربوط به نوع سیستم ها وتجهیزات ای تی سازمان در سرور ها و رایانه های سازمانی علاوه بر سرور های مبتنی بر ابر پاندا
- استفاده سرور های ابری پاندا از یک سیستم عامل اختصاصی مبتنی بر لینوکس(Ubuntu) برای مدیریت فرایند های اصلی و پایه. در این نوع سیستم عامل هیچ نوع داده ی مهمی ذخیره نمی شود. این سیستم عامل اختصاصا با همکاری شرکت کانونیکال یکی از تولید کنندگان اصلی نسخه ی اوبونتوی لینوکس توسعه یافته است .

- فایروال های قدرتمند برای انسداد دستری های نا مشخص و غیر مجاز به سرور های ابری پاندا؛ تنها ارتباط های ورودی بر روی پورت ۴۴۳ که تصدیق هویت و اعتبار شده باشند اجازه دسترسی به این سرور ها را دارند
- ارتباط های بدون اختلال و با سرعت قابل قبول
- به علت استفاده از مسیر های ارتباطی جایگزین و کمکی بر مبنای پروتکل های امن SSL / TSL ۱,۰ و استفاده از سرور های غول پیکر شرکت آمازون (AWS) با قبلیت عملیاتی سطح بالا
- کنترل خودکار و هوشمند ترافیک ارتباطی؛ از طریق اختصاص هوشمند و خودکار منابع مورد نیاز به بخش هایی که از بار ترافیکی بالاتری برخوردارند و یا با کاهش ظرفیت عملیاتی مواجه هستند

## تامین امنیت کنسول خدمات ابری پاندا

| | |
|---|---|
| encryption | AES-256,256bit keys. The connection uses TLS1.0. |
| passwords | Strong passwordsrequired-min8 characters |
| Password expiry | Mandatory password expiration every 30 days |
| Authentication | RADIUS server integration can be enabled together with single sign on and one time passwords, or SecurID tokens. |
| Roles | four user assignable security levels available |
| Accounting | Session activity logged to system level log files |

## تامین امنیت ارتباط با کنسول در ایستگاه های کاری (EndPoint)

| | |
|---|---|
| Encryption{agent to server} | SSL3.0 |
| Encryption {agent to connection broker} | 3DESinCBC mode |
| Protocol | HTTPS/ TCP 443 |

# پرسش های متداول (۱)

## ۱- آیـا برنامـه پیشـنهادی دارای نمایندگـی رسـمی و قانونی در ایران میباشد؟

بلـه؛ شـرکت ایمـن رایانـه پنـدار نماینـده رسـمی و انحصـاری Panda Security در ایـران و امارات متحده عربی می باشد.

## ۲- آیا مدرکی دال بر نمایندگی شرکت فروش اصلی وجود دارد؟

آری، علاوه بر قرارداد رسمی با کمپانی Panda Security ، این شرکت از جانب شورای عالی انفورماتیک نیز بعنوان نماینده انحصاری این شرکت در ایران معرفی گردیده و ضمنا مورد ارزیابی قرار گرفته که به پیوست مدارک آن ایفاد می گردد.

## ۳- در صورت تشخیص اشتباه یک فایل به عنوان ویروس، آیا امکان تصحیح و استثنا وجود دارد؟

میتوان این گونه فایلها را exclude نمود. ضمنا با وجود یک تکنولوژی جدید به نام Malware Freezer تمامی فایل های شناسایی شده در شبکه، به مدت ۷ روز در محیط قرنطینه نگه داشته می شود که در صورت تشخیص اشتباه، می توان آنها را بازیابی کرد.

توضیح: با نگاهی اجمالی به انواع بدافزارهای امروزی می توان نتیجه گرفت که پیچیدگی و توان تخریب آنها بسیار افزایش یافته است و با استفاده از روش های قدیمی شناسایی کدهای مخرب، سازندگان نرم افزارهای آنتی ویروس دیگر توان پاسخ دهی مناسب و به هنگام آنها را ندارند. روزانه بیـش از ۱۷۰،۰۰۰ نمونـه جدید از بدافزارها توسـط لابراتوارهای شـرکت های ضدویروس شناسـایی می شـوند. اسـتفاده از تکنولـوژی Collective Intelligence پاندا و توان عملیاتی آن که به صورت بسـیار گسـترده در سـطح جهان پراکنده شـده است و همچنین بهره گیری از دانش چگونگی رفتار کدهای مخرب به صورت Distributed و موتور هوش مصنوعی فعال در قلب نرم افزارهای پاندا، میتوان با سرعت قابل توجهی به مقابله با این هجوم گسترده برخاست.

پس از ارسال فایل در سرورهای Collective Intelligence پاندا، آنها با در نظر گرفتن موارد زیر آنالیز می شوند:

- آنالیز های بسیار حساس با تکنولوژی اکتشافی (Heuristic Analysis)
- آنالیزهای مبتنی بر Signature File آخرین فایل بروزرسانی
- نماسازی و شبیه سازی (Sandboxing)
- مجازی سازی (Virtualization)
- انطباق با لیست های سفید Process or Code Whitelists

در نتیجـــهٔ بررسی پردازش های Collective Intelligence روی فایل سه حالت حاصل می شود:

۱- فایل آلوده است (The file is Malware) : ارائه اطلاعات نوع کد مخرب و پاکسازی آن بنا به تنظیمات از پیش تعیین شده توسط مدیر سیستم.

۲- فایل آلوده نیست : file is Goodware.

۳- فایل مشکوک به مخرب است : file is Suspicious که در این صورت به بخش قرنطینه فرستاده می شود تا احتمال آلودگی آن بررسی شود.

## ٤- آیا نصب ضد ویروس پاندا، پس از آلوده شدن کامپیوترها به ویروس موثر خواهد بود و آلودگی را از بین خواهد برد؟

در صورتی که آلودگی سیسـتم به گونه ای نباشـد که بر عملکرد آنتی ویروس تاثیر مستقیم داشته باشد، پس از نصب آنتی ویروس بر روی سیستم می توان به راحتی اقدام به پاکسـازی نمود. اما در صورت آلودگی سیسـتم به بدافزارهایی از قبیل Sality که تاثیر مستقیم بر عملکرد آنتی ویروس داشته و آن را غیر فعال می کند، بهتر است از ابزارهای کمکی مانند Panda Bootable CD یا Panda Cloud Cleaner استفاده کرده و پس از پاکسازی سیستم، آنتی ویروس را بر روی آن نصب کنید.

# پرسش های متداول (۲)

### ۵- هنگام نصب برنامه های مورد تایید کارفرما بر روی کلاینت ها رفتار ضد ویروس پیشنهادی به چه ترتیبی است؟ امکان تعریف استثنا وجود دارد یا خیر؟

برخـورد آنتـي ويـروس در برابـر ويروس هـا يا بدافـزار بدين صورت مي باشد :

ابتـدا آن را پاکسـازی(Disinfect) کـرده؛ در غيـر ايـن صـورت کد مخرب مربوطه را پاک (Delete) می نماید.

توضيح: اصولا از لحاظ پاکسازي، کدهاي مخرب فقط شامل دو دسته هستند:

کدهاي مخربي که خود را به يك فايل سـالم متصل مي کنند که براي اين گونه از فايلها مناسـبترين گزينه Disinfection است که به معناي بيرون کشيدن آلودگي از فايل سالم و تحويل آن به شماست (يعني فقط حذف قسمت آلوده فايل)

نوع دوم دسـته اي هسـتند کـه کل فايل يك کد مخرب اسـت و حتما بايد کل آن حذف گردد.

هر چند کاربر نمی تواند برای ضدویروس مشخص کند که فایل ها را چگونـه پاکسـازی، حذف یا قرنطینـه کند، اما مـی تواند فایل مشـکوک یا مخربی را برای اسکن و پاکسازی به موتور ضدویروس معرفـی کـرده و یا فایل هـا، فولدرها و یا پسـوندهای خاصـی را از دسترس ضدویروس برای اسکن ، مستثنی (Exclude) کند.


### ۶- حجم بانک اطلاعاتی برنامه در حال حاضر چقدر میباشد؟

Installation Requirements:
1GB of RAM
Free space on the hard disk
100 MB (Agent + Protection + Update)

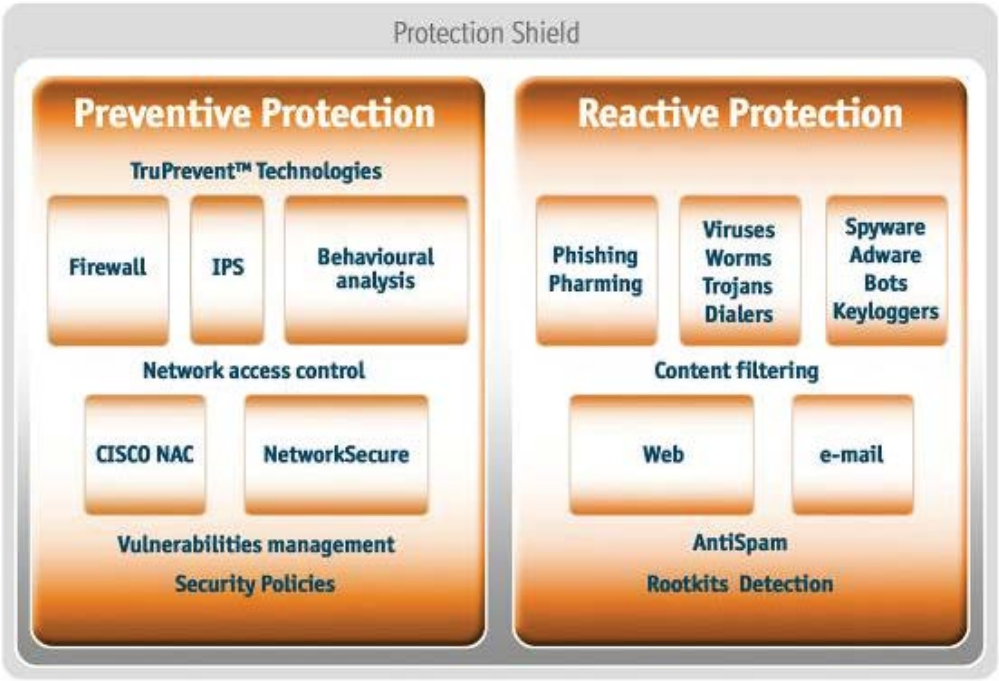
### ۷- آیا نرم افزار Panda Cloud Office Protection سیستم تشخیص وپیشگیری از نفوذ به همراه دیواره آتش شخصی دارد؟

**نرم افزار امنیت شبکه پاندا ۲ مدل امنیتی را ارائه می دهد :**
Preventive Protection یا حفاظت پیشگیرانه شامل: دیوارآتش Firewall، سیستم جلوگیری از نفوذ مبتنی بر میزبان HIPS، آنالیز رفتاری بر اساس ۲۰۰ نوع حرکت ژنتیکی پکت ها در فضای مجازی، کنترل دسترسی ها به منابع حساس شبکه

## پرسش های متداول (۳)

.... لازم به ذکر است با وجود تکنولوژی های فوق، امکان حملات درون شبکه ای، سرریز شدن بافر و دسترسی به منابع حیاتی شبکه ها مثل حساب های کاربری، تنظیمات شبکه ای و سرویس های گوناگون، برای انواع کدهای مخرب مسدود شده است. مدیریت حفره های امنیتی نیز از جمله بخش های اصلی این مدل امنیتی می باشد.

Reactive Protection که حفاظت جامعی از تهدیدات گوناگون شناخته شده و ناشناس همچون: ویروسها، کرمهای اینترنتی، تروژانها، کدهای شماره گیر، ابزارهای جاسوسی، ابزارهای تبلیغاتی، بوت ها، اسپم ها، کلاهبرداری های اینترنتی همانند فیشینگ و فارمینگ و همچنین کنترل محتویات وارده به شبکه را از طریق کنترل نامه های پست الکترونیک و صفحات وب در بر می گیرد.




### ۸- آیا قسمت مدیریت و کنسول Panda Cloud Office Protection بصورت Web based میباشد؟

کنسول این برنامه بصورت Web based بوده و کلیه امکانات Cloud Scanning را دارا میباشد.

ویژگی اصلی آن نیز قابلیت اسکن فایل ها بر مبنای فن آوری ابر ( Cloud ) می باشد. این ویژگی، مزیت های قابل توجهی در پی خواهد داشت :

بهسازی و توسعه پایگاه اطلاعات امنیتی، که توسط نرم افزارهای تحت شبکه پاندا بکار گرفته می شوند افزایش توان دفاعی آن ها، بهسازی زمان واکنش به تهدیدات جدید و پیچیده (افزایش سرعت به کمتر از ٦ دقیقه ) و نیز افزایش دقت لازم در کشف و پاکسازی ویروس های کاملا جدید مزیت های خوبی محسوب می شوند. علاوه بر این، بروزرسانی ماژول heuristic به صورن مستمر (real-time)، در کنار بروزرسانی Signature file (افزایش قابلیت شناسایی و کشف فایل های مخرب) و نیز کاهش احتمال تولید خطا در ردیابی، False Positive، از مزیت های دیگر ضدویروس تحت شبکه پاندا هستند.

# پرسش های متداول (٤)

## ۹- ویژگی های اصلی اسکن رایانه ها و سرورها با استفاده از فن آوری ابر (cloud) چیست؟

- یک فایل موقت حاوی اطلاعات مربوط به ویروس ها و کدهای مخرب اسکن شده ( Malware cache) بر روی سیستم ایجاد خواهد شد که پس از ٢٤ ساعت از بین خواهد رفت.
- اسکن مبتنی برابر (Cloud) قابلیت کشف و تشخیص کدهای مشکوک را نیز خواهد داشت.
- برخی از تنظیمات اعمال شده به علت محلی نبودن تنظیمات اسکن مبتنی بر Cloud ، موقت هستند
- عملیات اسکن در هر کدام از سیستم ها در صورت اتصال به اینترنت در هر ساعت انجام می شود
- اسکن قسمتهای پرخطر سیستم به صورت مداوم :

دایرکتوری ریشه در تمام درایوهای محلی ؛ پروفایل تمام کاربران وارد شده به شبکه؛ پوشه های حاوی فایل ها و اطلاعات موقت؛ پوشه های سیستمی در ویندوز یا سیستم های عامل دیگر؛ پوشه System 32

## ۱۰ - آیا امکان UNINSTALLکردن خودکار سایر آنتی ویروس ها بر روی شبکه در هنگام نصب وجود دارد؟

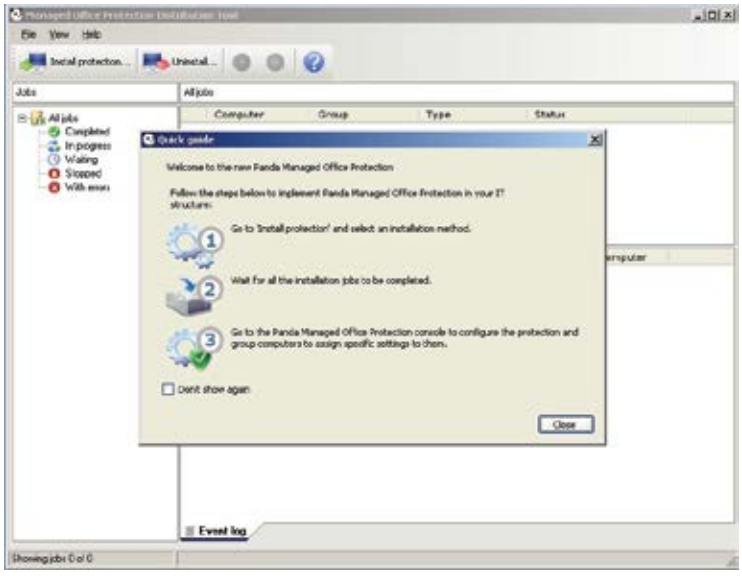
بله، بیشتر نسخه های مربوط به آنتی ویروس های مشهور را می توانید از طریق کنسول مدیریت مرکزی نرم افزار پاندا، غیرفعال کنید.

## ۱۱ - آیا امکان نصب و حذف ضدویروس کلاینت ها از روی سرور بدون متوجه شدن و دخالت کاربر وجود دارد؟

بله ، امکان نصب و حذف آنتی ویروس به صورت متمرکز بر روی بستر شبکه با استفاده از ابزارهای Distribution Tools امکانپذیر می باشد.

## ۱۲- آیا استفاده از امکانات نصب در محیط Active Directory وجود دارد؟

بله، تنها ابزار متمرکز نصب بر روی بستر شبکه استفاده از Distribution tools بوده که امکان شناسایی دامنه های موجود در شبکه را نیز فراهم می آورد. همچنین فایل نصب agent در قالب msi بوده و امکان نصب از طریق Active Directory نیز فراهم می باشد.



## پرسش های متداول (۵)

**۱۳- آیا امکان قرنطینه فایل های مشکوک و بازیابی آنها از قرنطینه از راه دور و توسط ابزار مدیریتی وجود دارد؟ اصلی اسکن رایانه ها و سرورها با استفاده از فن آوری ابر (cloud) چیست؟**

برای هر فایل قرنطینه شده، فرایندهای زیر قابل انجام هستند.

- Restore: برگرداندن فایل به محل اصلی. در این مرحله اگر امکان پاکسازی فایل قرنطینه شده وجود داشته باشد قبل ازبرگرداندن به محل اصلی از کاربر سوال میشود.
- Delete: انتخاب این گزینه فایل را از لیست پاک میکند.

لازم به ذکر است تمامی فایل های قرنطینه شده، به صورت خودکار به آزمایشگاه پاندا ارسال می گردد.

**۱۴ - آیا امکان اعمال تغییرات و تنظیمات برروی گروهی از کامپیوترها وجود دارد؟**

بله؛ این امکان وجود دارد که تنظیمات برروی تک تک و یا گروهی از کامپیوترها اعمال شود.

**۱۵ - آیا این امکان وجود دارد تا از اعمال تغییرات برنامه های ناخواسته برروی مرورگرهای وب گرفته شود؟**

بله، با استفاده گزینه Internet Setting، هر گونه تغییر در تنظیمات مرورگر توسط پاندا بررسی شده و در صورت تایید کاربر اعمال میشود. این عمل به صورت اختیاری می باشد و می توان با استفاده از گزینه های زیر نحوه بر خورد با این تنظیمات را تعیین کرد.

**۱۶- آیا این امکان وجود دارد تا جلوی فعالیت فایل های آلوده هم نام با فایل های اصلی سیستم عامل گرفته شود؟**

بله، ماژول های اختصاصی موتور ضدویروس پاندا این امکان را به صورت خودکار فراهم می کند.

**۱۷- آیا نرم افزار پاندا دارای مکانیزم مدیریت "Licenses" میباشد؟ اصولاً Licenses برچه اساسی است؟ در صورت افزایش رایانه ها و سرورها از تعداد مجاز لایسنس، رفتار ضدویروس پاندا چگونه خواهد بود؟**

بلی، به هر رایانه اعم از سرور و کلاینت یک لیسانس تعلق می گیرد. در صورت افزایش تعداد رایانه ها از تعداد مجاز میتوانید با دپارتمان فروش این شرکت هماهنگ نموده و درخواست افزایش لیسانس بدهید که طبعا این تعداد به اشتراکتان افزوده گردیده و در پایان مدت اشتراک نرم افزار، کلیه لیسانسها با هم به اتمام میرسند که میتوان آنها را تمدید نمود.

**۱۸- آیا نرم افزار پاندا، قادر به حفاظت از خود درمقابل بدافزارهایی که به طور خاص برنامه های ضدویروس را هدف میگیرند می باشد؟**

بله، ضمنا نرم افزار امنیت شبکه پاندا قابلیت شناسایی و پاکسازی بیش از ۲۵۰ میلیون کد مخرب فعال و غیر فعال را دارا می باشد. کدهای مخرب شامل این موارد می باشند: Virus /Worm /Trojans / Hacking tools / Spyware /Adware /Key loggers / Backdoor / downloader /Joker /dialer /phishing tools /shockware / Rootkit /riskware / ...

**۱۹- آیا جهت استفاده از برنامه نیاز به License میباشد؟ نحوه محاسبه قیمت License بر اساس چیست؟**

بلی، نرم افزارهای ضدویروس پاندا، دسته بندی مشخصی بر اساس تعداد لیسانس ها دارد که هر دسته قیمت واحد مشخصی دارند.

## پرسش های متداول (٦)

**۲۰- آیا نرم افزار پاندا قادر به حفاظت یکپارچه در مقابل ویروس ها، بدافزارها، حملات نفوذ گران و هرزنامه ها برای تمام سطوح شبکه از ایستگاه های کاری تا دروازه های اینترنتی میباشد؟**

بله ... ضدویروس تحت شبکه پاندا به صورت جامع و کامل تمامی ماژول های مورد نیاز برای هر مدیر شبکه ای را در اختیار دارد.

**۲۱- آیا محدودیتی در لیسانس نرم افزار با توجه به تعداد کاربران A.D وجود دارد؟**

بله، نرم افزار ضدویروس پاندا، حساس به لایسنس بوده و بیش از تعداد لایسنس خریداری شده نصب نمی گردد. اما شرکت ایمن رایانه پندار آمادگی دارد در هر زمان که نیاز به افزایش لایسنس باشد در کمتر از ۵ دقیقه لایسنس ها به تعداد مورد درخواست به کنسول مرکزی نرم افزار اضافه خواهد شد.

**۲۲- در زمینه پشتیبانی فنی و خدمات در دوره گارانتی محصول چه امکاناتی وجود دارد؟**

- عقد قرار داد خرید و پشتیبانی بصورت شبانه روزی و در تمام روزهای سال
- ارائه خدمات مستمر و بدون وقفه به مشتریان از طریق پاسخگویی تلفنی، وب، پست الکترونیک
- اعزام نیروی متخصص به محل خریدار طی مدت قرار داد
- پشتیبانی از طریق اتصال از راه دور

**۲۳- اگر زمان گارانتی به اتمام برسد به روز رسانی اتوماتیک قطع میگردد یا ادامه می یابد؟**

دوره اشتراک این نرم افزار یک تا ۳ سال می باشد. در طی این مدت تمامی خدمات فوق بانضمام ارسال خبرنامه، ارسال فایلهای بروزرسانی ارسال نگارش جدید نرم افزار، ارائه خدمات پشتیبانی طبق قرارداد، برقراری اتصال راه دور برای کارشناسان Panda Security اسپانیا جهت برطرف نمودن مشکلات و ایرادات خاص، ارائه مشاوره در خصوص سایر مباحث امنیتی در شبکه، انجام خواهد گردید. در صورت پایان یافتن دوره اشتراک و عدم تمدید این دوره، کلیه سرویسهای بروزرسانی و ارتقا نگارش و خدمات فنی این شرکت در خصوص نرم افزار قطع گردیده و بدیهیست نرم افزار از آن به بعد صرفا کدهای مخربی را که تا آن تاریخ توانایی شناسایی آنها را داشته شناسایی و پاکسازی خواهد کرد.

**۲٤-در زمینه به روز رسانی نرم افزار ضدویروس پاندا، چه امکاناتی وجود دارد؟**

- روزآمد شدن پایگاه اطلاعاتی نرم افزار ضد ویروس به صورت مستمر
- روزآمد شدن پایگاه اطلاعاتی ماژول ضد هرزنامه مستمر
- بروزرسانی زمانبندی شده با امکان تعریف رمان دلخواه
- تعریف جایگاههای بروزرسانی(Repository)
- به روز رسانی متمرکز و همزمان کامپیوتر تمام کاربران از یک نقطه مرکزی
- امکان به روز رسانی آنلاین سرورخدمات رساننده و انتشار آن در شبکه
- روزآمد شدن کامپیوتر کاربران از دو منبع سرور خدمات دهنده داخلی و اینترنت(در صورت عدم دسترسی به هرکدام فرآیند به روزرسانی از منبع دوم انجام شود).

# پرسش های متداول (۷)

FAQs

**۲۵- در زمینه شناسایی و پاکسازی ویروس ها چه قابلیت هایی در اختیار مدیر شبکه خواهد بود؟**

- امکان شناسایی IP دستگاه های ارسال کننده ویروس
- تعریف بازه زمانی برای فایل هایی که طی آن مدت ویرایش نشده اند
- انتخاب فایل های مشخص شده برای اسکن
- ویروس یابی فایل های فشرده(zip ،rar ،arj ،cab ،lzh)قبل از باز شدن
- برنامه ریزی و زمان بندی ویروس یابی و اسکن کلاینت ها توسط مدیر شبکه
- پاکسازی فایل های آلوده از ویروس بدون صدمه به فایل کاربر
- ویروس یابی و پاکسازی فایل ها در حال پشتیبان گیری
- هوشمندی در شناخت الگوهای حمله
- پاکسازی بخش راه انداز دیسک(Boot sector)
- دیسکت راه انداز برای ویروس یابی
- CD راه انداز برای ویروس یابی
- شناسایی و پاکسازی فایل های آلوده به ویروس در حین دانلود از اینترنت
- پاکسازی فایل های آلوده به وبروس زمانیکه فایل توسط کاربر دیگری باز است و یا امکان خذف آن توسط سیستم عامل میسر نیست. در این حالت امکان تعیین واکنش ثانویه مثل قرنطینه (move Quarantine)، محدود کردن دسترسی به فایل (Deny Access)و یا حذف(Delete) وجود دارد.

**۲۶- آیا برنامه دارای بخش گزارش گیری مدیریتی می باشد؟**

گزارش های مورد نیاز به شرح ذیل می باشند:

- گزارش از کامپیوتر هایی که طی بازه زمانی خاص Update نشده اند
- گزارش از عملکرد آنتی ویروس بر روی سیستم های نصب شده
- گزارش ویروس یابی هر کلاینت (تاریخ اسکن، نوع ویروس ها، مسیر و غیره)

**۲۷- آیا برنامه دارای امکان سهمیه بندی اینترنت برای کاربران می باشد؟**

بله، این نرم افزار قادر است اینترنت را برای کاربران بصورت زمانی سهمیه بندی کند.

**۲۸- آیا امکان مدیریت پورتهای یو اس بی و ... جهت مدیریت تجهیزاتی که به هرکدام از سیستم های سازمانی متصل خواهند شد در برنامه وجود دارد؟**

بله، در نسخه امنیتی تحت وب پاندا امکان مدیریت پورتهای USB و تجهیزات ذخیره سازی اطلاعات و وسایل جانبی از قبیل موبایل، مودم، اسکنر و .... امکان پذیر می باشد.

# پرسش های متداول (۸)

## ۲۹- در آیا برنامه Panda Cloud Fusion امکان مانیتورینگ کارکنان سازمانی و هم چنین سرورها را در شبکه داراست؟

در قلب مجموعه محصولات تحت ابر پاندا با نام Panda Cloud Fusion، یک نرم افزار مانیتورینگ و HelpDesk تحت شبکه با نام Panda Cloud System Management قرار دارد.

PCSM یک روش فوق العاده ساده و ارزان برای نظارت وپشتیبانی شبکه های سازمانی می باشد.

### اصول کلی PCSM به شرح زیر است:

- کنسول مدیریتی PCSM به صورت web based میباشد
- ماژول agent بر روی هر device نصب میشود
- بعد از نصب، agent با سرور ارتباط برقرار میکند و تمام گزارشات و اطلاعات مربوط به device را ارسال میکند.
- مدیر شبکه از طریق اینترفیس وب ، با ایجاد کردن policy ها ، اجرای script ها به صورت ریموت و توزیع کردن نرم افزار ها مدیریت و کنترل خوبی بر روی device ها اعمال میکند.
- تمام فعالیت های کارکنان سازمانی ثبت و قابل گزارش دادن میباشند.

### ویژگی های PCSM

- یک نرم افزار صد در صد مبتنی بر فناوری ابر
- نصب مبتنی بر ایستگاه های کاری
- نظارت و کنترل وضعیت تمامی تجهیزات سخت افزاری و نرم افزاری شرکت (کنترل services، disk usage، memory، cpu و... با نمودارهای کارایی وهشدارها در لحظه به لحظه)
- مدیریت نصب اصلاحیه های نرم افزاری در تمام شرکت
- نصب و توزیع نرم افزارهای مورد نیاز در تمام شرکت
- دسترسی از دور دست
- کنترل از دور دست
- دریافت گزارش های کاربردی و مفصل
- ایجاد یک محیط اشتراکی برای رفع مشکلات
- ارتباط های کاملا امن

## ۳۰- آیا کاربران قادر به اعلام مشکلات سیستم های خود از طریق تیکت هستند؟ توضیح دهید:

بلی، این امکان در مجموعه محصول Panda Cloud Fusion و نسخه مانیتورینگ Panda Cloud System Management وجود دارد. با دبل کلیک روی آیکن برنامه، کاربر میتواند مشکل خود را بفارسی در نت باز شده نوشته و ارسال کند. این تیکتها روی پنل مدیریتی نرم افزار قابل مشاهده می باشد. کارشناسان واحد IT میتوانند مشکلات اعلام شده را از طریق ابزارهای ریموت معمول، و همچنین ریموت ترنسپرنت نرم افزار برای کاربر حل و فصل نمایند. خاصیت ریموت Transparent ورود نامحسوس به سیستم کاربر و دسترسی به سرویسهای سیستم عامل وی است. بگونه ای که فعالیت کاربر متوقف نمیشود.

## پرسش های متداول (۹)

### ۳۱- آیا برنامه قادر به دریافت و توزیع و نصب اصلاحیه ها و سایر نرم افزارها می باشد؟ فرمت قابل قبول نرم افزارها عنوان گردد ...

در قلب بلی، این امکانات در مجموعه محصول Panda Cloud Fusion و نسخه مانیتورینگ Panda Cloud System Management وجود دارد.

قابلیت Patch Management نرم افزار مدیر شبکه را قادر میسازد تا هر فایلی را در فرمت MSI و EXE دریافت و بر روی سیستم ها نصب نماید. خواه یک نرم افزار خاص باشد و خواه یک اصلاحیه مربوط به مایکروسافت، مرورگرها، ادوبی و ...

همچنین نرم افزار دارای یک Com Store می باشد که در آن غالب نرم افزارهای مورد نیاز و رایگان شبکه از قبیل مرورگرها، پلیرها و ... وجود دارد و با یک کلیک روی آن میتوان از قابلیت Software Deployment نرم افزار استفاده نموده و آن را روی سیستم های مورد نیاز نصب نمود.

### ۳۲- آیا برنامه امکان ره گیری و رصد کاربران سیار شبکه را دارد؟

آری، نرم افزار قابلیتی دارد بنام Mobile Device Management مدیر شبکه را قادر میسازد با نصب یک ایجنت روی هر کدام از سیستمهای ارتباطی کاربران سیار از قبیل اسمارت فون، تبلت، یا نت بوک، بتواند آنها را رصد نموده و از روی نقشه گوگل مکان آنها را مشخص نماید. این امکان با فعال بودن ماژول جی پی اس قابل انجام است. ضمنا سیستم عامل های Android و iOS را نیز ساپورت میکند.

### ۳۳- آیا برنامه قابلیت اضافه کردن و اجرای اسکریپت های مختلف در شبکه را دارد؟

بلی، این امکان در مجموعه محصول Panda Cloud Fusion و نسخه مانیتورینگ Panda Cloud System Management وجود دارد.

# چرا

## راهکارهای امنیتی پاندا را به شما پیشنهاد می‌کنیم؟

- خارج از فهرست شرکت ها و محصولات امنیتی تحریم شده برای ایران
- پشتیبانی فنی مستقیم به صورت شبانه روزی در تمام روزهای سال
- قدرتمندترین موتورهای کشف و پاکسازی تهدیدهای رایانه ای
- سبک ترین و سریع ترین راهکارهای حفاظتی
- مورد توجه و اقبال میلیون ها کاربر در سرتاسر جهان
- پیشرو در تولید و بکارگیری فن آوری های نوین حفاظتی
- توزیع محصولات امنیتی در ۲۰۰ کشور جهان
- حضور مستقیم در بیش از ۶۰ کشور جهان از طریق نمایندگان رسمی
- ۲۲ سال تجربه موفق در حفاظت از اطلاعات رایانه ای


ایمن
رایانه
پندار