

PANDA CLOUD OFFICE PROTECTION

ضدویروس و مدیریت امنیت شبکه؛ در هر زمان و از هر کجای جهان ...
با استفاده از یک کنسول مدیریت تحت وب



ENJOY THE FIRST WEB-BASED IT SECURITY SOLUTION WITH CENTRALIZED DEVICE MANAGEMENT AND ...
PROACTIVE ANTIVIRUS - INTELLIGENT FIREWALL - MAIL PROTECTION - MALWARE FREEZER
WEB-BASED CONSOLE + REAL-TIME UPDATES AND AUTOMATIC UPGRADES



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 کشورهای 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، سرور WSUS، ارائه و پشتیبانی فایروال سخت افزاری و دستگاههای UTM و SCM، تست های نفوذ پذیری و طراحی شبکه براساس استانداردهای امنیت اطلاعات، آموزش مفاهیم امنیت شبکه و ...



Panda Cloud Office Protection

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 است 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

شناسایی و پاکسازی بیش از ۲۵۰ میلیون نوع مختلف از ویروسها، کرمهای رایانه ای و نرم افزارهای تروژان، با قابلیت ترمیم فایلهاي صدمه دیده و پاکسازی اثرات مخرب احتمالی بدافزارها. موتور ضدویروس پاندا موفق به کسب 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 ۲۰۱۴ 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 برعهده 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 قدرتمندترین ابزار ضد جاسوسی در اینترنت را به خود اختصاص دهد.

:Anti-Hacking Tools and Anti-Keylogger

سیستم اختصاصی نرم افزار پاندا برای کشف و شناسایی 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 روی سرور Exchange و همچنین بر روی سیستم های نهایی کاربران مستقر می شود، شبکه سازمانی شما در برابر هجوم نامه های ناخواسته الکترونیکی 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

جلوگیری از ورود و فعالیت کدهای شماره گیر (نوع خاص و آزارنده ای از نرم افزارهای مخرب) و همچنین جلوگیری از نمایش تبلیغات ناخواسته و پی در پی اینترنتی از جمله امکانات مهم نرم افزار آنتی ویروس پاندا می باشد. فعالیت Cookie ها نیز توسط این نرم افزار بطور کامل کنترل و در صورت لزوم مسدود می شود.

Panda Cloud Office Protection

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 ضد ویروس، فایل سالم را اشتباهاً به عنوان فایل مخرب حذف نکند. موتور ضد ویروس پاندا به مدد این تکنولوژی و از طرف بسیاری از مؤسسات تست آنتی ویروس، بعنوان بی اشتباه ترین موتور ضد بد افزار 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 نمی 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 جلوگیری 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 می تواند از تغییر فایلها بر اثر حملات رایانه ای جلوگیری کند. 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

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

:Mail Sending Control

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

Panda Cloud Office Protection

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 BLASTER که باعث اختلال و گاه توقف کامل در عملکرد های شبکه شرکت میشود.

: Blocking Actions

نرم افزار آنتی ویروس پاندا قادر به جلوگیری از دسترسی کدهای مخرب به بخش های بسیار مهم سیستم عامل مثل Windows Registry، Windows Services، User Accounts، System Files و Com Components می باشد.

: Protections of digitally-signed processes

حفاظت از پردازش ها و اطلاعاتی که دارای امضای دیجیتال 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 ها 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 توسط نفوذ کدهای مخرب است. (با توجه به این مسئله که ویروسهای چند ماه اخیر قادرند نرم افزارهای آنتی ویروس را نیز غیر فعال سازند).

: Device Control

برای ایجاد محدودیت در دسترسی به ابزاری نظیر 3G, removable USB, CD/DVD-ROM, Bluetooth storage drives, modem, image capture device و ... این ویژگی به مدیر شبکه امکان می دهد تا کلیه ابزارهای جانبی که به سرورها و کلاینت ها متصل میشوند 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 فن آوری قدرتمند ابر عمل می کند و به عنوان یک گزینه مکمل امنیتی برای افزایش قدرت و سرعت موتور ضد ویروس پاندا می توان از آن استفاده کرد. با بهره گیری از این فن آوری تمام کاربران اینترنت به صورت مستمر و لحظه به لحظه به سرورهای امنیتی پاندا، متصل خواهند بود و در نتیجه همواره و هر لحظه بروز می شوند و از بالاترین قدرت دفاعی در برابر حملات ویروس های بسیار جدید و نفوذ های غیرمجاز برخوردار خواهند بود.

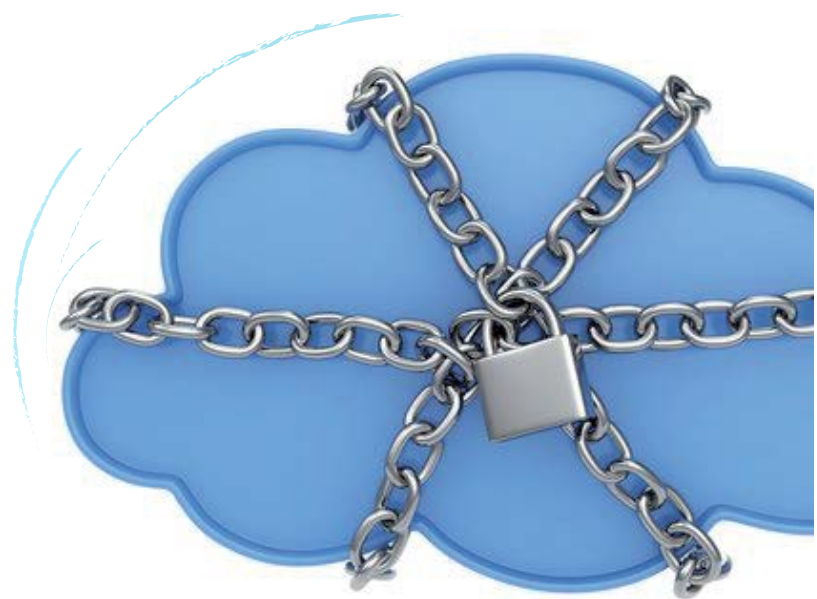
هوش یکپارچه بر مبنای فن آوری ابر (Cloud Technology) عمل می کند و یکی از بهترین راهکارها برای افزایش امنیت شبکه های شرکت محسوب می شود. شرکت پاندا با ابداع و بکارگیری این فن آوری موفق شد تا در سال ۲۰۱۰ میلادی رتبه دوم برترین شرکت امنیتی جهان را از طرف نشریه بسیار معتبر the Wall Street Journal دریافت کند.



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 رمزهای عبور قدرتمند؛ این رمزهای عبور خود به صورت رمز گذاری شده در سرورهای امن پاندا ذخیره می شوند.
- لزوم تغییر دوره ای رمزهای عبور در دوره های ۳۰ و ۶۰ و ۹۰ 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 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 سرورهای دارای تکنولوژی امنیتی RAIDUIS یکپارچه هستند .
- ارتباط های مبتنی بر SSL / TLS
- ارتباط های کاربر با سرورهای پاندا و هرگونه اطلاعات مبادله شده میان آنها با استفاده از پروتکل های قدرتمند رمز گذاری مانند SSL / TLS، ۱۰۲۵ 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 و تجهیزات ای تی سازمان در سرورها و رایانه های سازمانی علاوه بر سرور های مبتنی بر ابر پاندا
- استفاده سرورهای ابری پاندا از یک سیستم عامل اختصاصی مبتنی بر لینوکس (Ubuntu) برای مدیریت فرایندهای 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 دسترسی های نامشخص و غیرمجاز به سرورهای ابری پاندا؛ تنها ارتباط های ورودی بر روی پورت ۴۴۳ که تصدیق هویت و اعتبار شده باشند اجازه دسترسی به این سرورها را دارند
- ارتباط های بدون اختلال و با سرعت قابل قبول
- به علت استفاده از مسیرهای ارتباطی جایگزین و کمکی بر مبنای پروتکل های امن SSL / TLS، ۱۰ و استفاده از سرورهای غول پیکر شرکت آمازون (AWS) با قابلیت 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- آیا برنامه پیشنهادی دارای نمایندگی رسمی و قانونی در ایران میباشد؟

بله؛ شرکت ایمن رایانه پندار نماینده رسمی و انحصاری Panda Security در ایران 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 ضمناً 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. ضمناً 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 بیچیدگی 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 بیش از ۱۷۰,۰۰۰ نمونه جدید از بدافزارها توسط لابراتوارهای شرکت های ضدویروس شناسایی می شوند. استفاده از تکنولوژی Collective Intelligence پاندا و توان عملیاتی آن که به صورت بسیار گسترده در سطح جهان پراکنده شده 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:

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

در نتیجه 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.

۴- 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 سیستم به گونه ای نباشد که بر عملکرد آنتی ویروس تاثیر مستقیم داشته باشد، پس از نصب آنتی ویروس بر روی سیستم می توان به راحتی اقدام به پاکسازی نمود. اما در صورت آلودگی سیستم به بدافزارهایی از قبیل Salty 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.

FAQS

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؟

برخورد آنتی ویروس در برابر ویروس ها یا بدافزار بدین صورت می باشد:

ابتدا آن را پاکسازی (Disinfect) کرده؛ در غیر این صورت کد مخرب مربوطه را پاک (Delete) می نماید.

توضیح: اصولا از لحاظ پاکسازی، کدهای مخرب فقط شامل دو دسته هستند:

کدهای مخربی که خود را به یک فایل سالم متصل می کنند که برای این گونه از فایلها مناسبترین گزینه Disinfection است که به معنای بیرون کشیدن آلودگی از فایل سالم و تحویل آن به شماست (یعنی فقط حذف قسمت آلوده فایل)

نوع دوم دسته ای هستند که کل فایل یک کد مخرب است و حتما باید کل آن حذف گردد.

هر چند کاربر نمی تواند برای ضدویروس مشخص کند که فایل ها را چگونه پاکسازی، حذف یا قرنطینه کند، اما می تواند فایل مشکوک یا مخربی را برای اسکن و پاکسازی به موتور ضدویروس معرفی کرده و یا فایل ها، فولدرها و یا پسوندهای خاصی را از دسترس ضدویروس برای اسکن، مستثنی (Exclude) کند.

The screenshot shows three sections for exclusion settings:

- Extensions to exclude:** A text input field, an 'Add' button, and a list box containing 'Delete' and 'Clear' buttons.
- Folders to exclude:** A text input field, an 'Add' button, and a list box containing 'Delete' and 'Clear' buttons.
- Files to exclude:** A text input field, an 'Add' button, and a list box containing 'Delete' and 'Clear' buttons.

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 و پیشگیری از نفوذ به همراه دیوار آتش شخصی دارد؟

نرم افزار امنیت شبکه پاندا ۲ مدل امنیتی را ارائه می دهد:

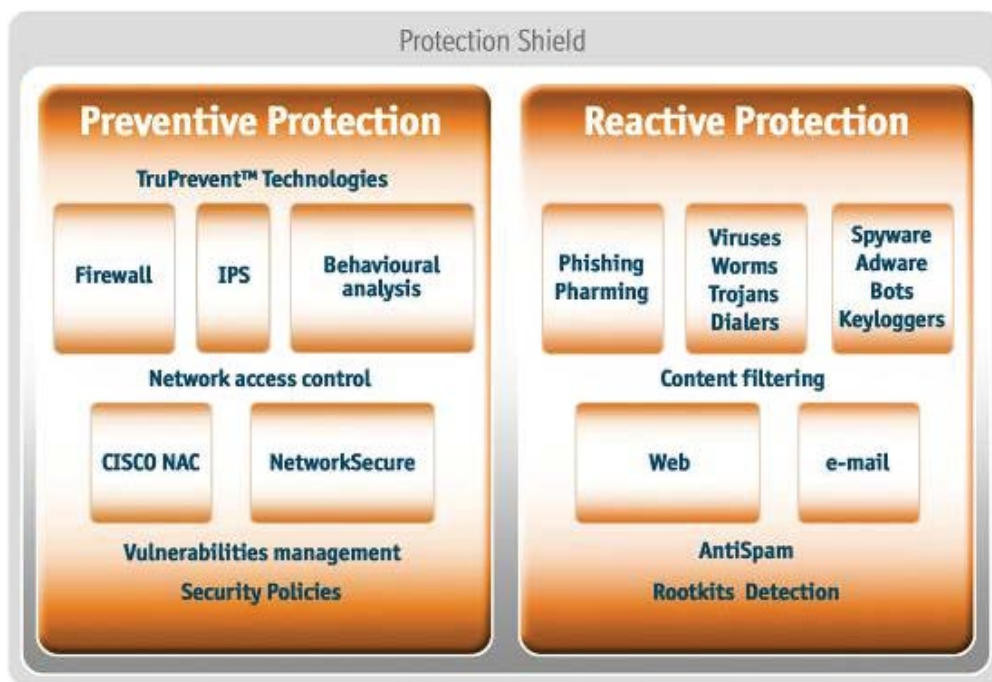
Preventive Protection یا حفاظت پیشگیرانه شامل: دیوار آتش Firewall، سیستم جلوگیری از نفوذ مبتنی بر میزبان HIPS، آنالیز رفتاری بر اساس ۲۰۰ نوع حرکت ژنتیکی پکت ها در فضای مجازی، کنترل دسترسی ها به منابع حساس شبکه

پرسش های متداول (۳)

FAQS

.... 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، اسپیم 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 ۶ دقیقه) و نیز افزایش دقت لازم در کشف و پاکسازی ویروس های کاملاً جدید مزیت های خوبی محسوب می شوند. علاوه بر این، بروزرسانی ماژول heuristic به صورت 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 ضد ویروس تحت شبکه پاندا هستند.

پرسش های متداول (۴)

FAQS

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 ۲۴ ساعت از بین خواهد رفت.
 - اسکن مبتنی بر ابر (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 UNINSTALL کردن خودکار سایر آنتی ویروس ها بر روی شبکه در هنگام نصب وجود دارد؟

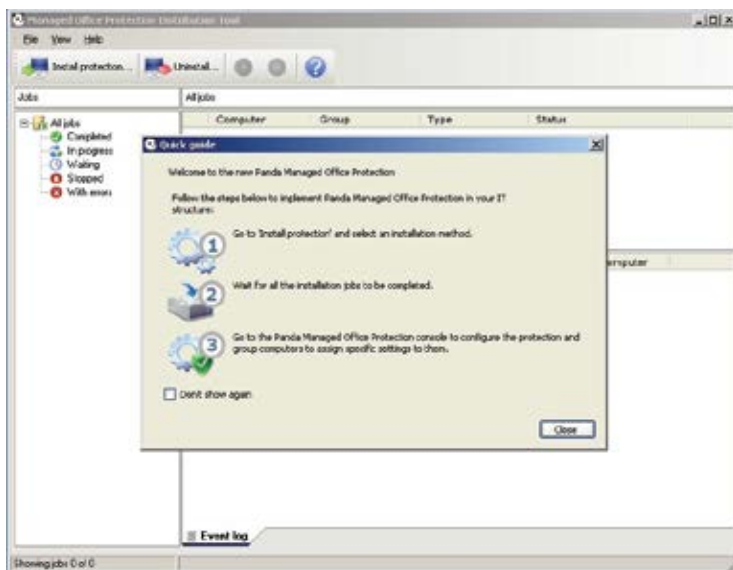
بله، بیشتر نسخه های مربوط به آنتی ویروس های مشهور را می توانید از طریق کنسول مدیریت مرکزی نرم افزار پاندا، غیرفعال کنید.

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)

FAQS

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 از برگرداندن 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 بروی گروهی از کامپیوترها وجود دارد؟

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

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

بله، با استفاده از 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 برخورد 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 بر چه 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 لایسنس تعلق می گیرد. در صورت افزایش تعداد رایانه ها از تعداد مجاز میتوانید با دپارتمان فروش این شرکت هماهنگ نموده و درخواست افزایش لایسنس بدهید که طبعاً این تعداد به اشتراکتان افزوده گردیده و در پایان مدت اشتراک نرم افزار، کلیه لایسنسها با هم به اتمام میرسند که میتوان آنها را تمدید نمود.

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

بله، ضمناً 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/ .../riskware/ Rootkit /shockware/ phishing tools/dialer/Joker

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 لایسنس ها دارد که هر دسته قیمت واحد مشخصی دارند.

پرسش های متداول (۶)

FAQS

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 هرمدیر 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 قرارداد 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 قرارداد
- 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 فایل های 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.

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

- روز آمد شدن پایگاه اطلاعاتی نرم افزار ضد ویروس به صورت مستمر
- روز آمد شدن پایگاه اطلاعاتی ماژول ضد هرزنامه مستمر
- بروزرسانی زمانبندی شده با امکان تعریف زمان دلخواه
- تعریف جایگاههای بروزرسانی (Repository)
- به روز رسانی متمرکز و همزمان کامپیوتر تمام کاربران از یک نقطه مرکزی
- امکان به روز رسانی آنلاین سرور خدمات رساننده و انتشار آن در شبکه
- روز آمد شدن کامپیوتر کاربران از دو منبع سرور خدمات دهنده داخلی و اینترنت (در صورت عدم دسترسی به هر کدام فرآیند به روز رسانی 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 ویروس زمانیکه فایل توسط کاربر دیگری باز است و یا امکان حذف 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 کامپیوترهایی 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.

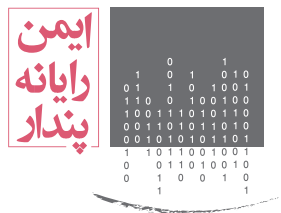
۲۸- آیا امکان مدیریت پورتهای یواس بی و ... جهت مدیریت تجهیزاتی که به هر کدام از سیستم های سازمانی متصل خواهند شد در

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، اسکرو امکان پذیر می باشد.



- ↓ ۲۲ سال تجربه موفق در حفاظت از اطلاعات رایانه‌ای
- ↓ حضور مستقیم در بیش از ۶۰ کشور جهان از طریق نمایندگان رسمی
- ↓ توزیع محصولات امنیتی در ۲۰۰ کشور جهان
- ↓ پیشرو در تولید و بکارگیری فن آوری‌های نوین حفاظتی
- ↓ مورد توجه و اقبال میلیون‌ها کاربر در سرتاسر جهان
- ↓ سبک‌ترین و سریع‌ترین راهکارهای حفاظتی
- ↓ قدرتمندترین موتورهای کشف و پاکسازی تهدیدهای رایانه‌ای
- ↓ پشتیبانی فنی مستقیم به صورت شبانه‌روزی در تمام روزهای سال
- ↓ خارج از فهرست شرکت‌ها و محصولات امنیتی تحریم شده برای ایران



WWW.PANDASECURITY.IR