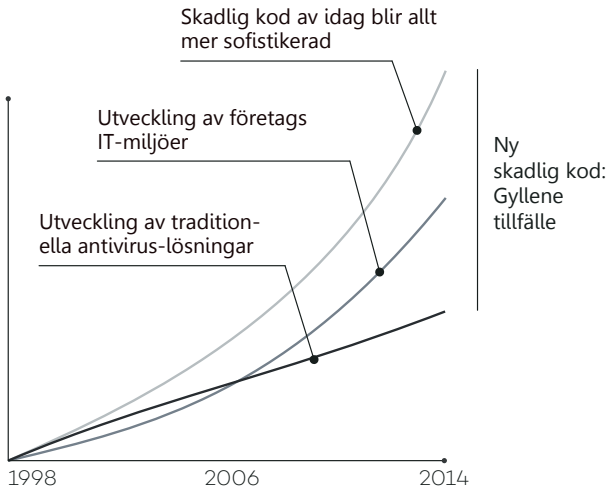
Adaptive Defense 360

Hitta svaren, lös problemet

KOMPLETT FÖRSVAR FÖR ENDPOINT SOM INTEGRERAR SKYDD, DETEKTION, SVAR OCH EFTERBEHANDLING I EN OCH SAMMA LÖSNING

Att försvara endpoints mot angrepp är svårt. Skyddet måste innehålla ett brett spektrum av försvar, inklusive traditionellt antivirus, antimalware, personlig brandvägg, webb- och e-postfilter och enhetskontroll. Varje försvar måste dessutom ge ytterligare täckning mot svårupptäckta zero-day-attacker och riktade attacker. Fram till nu har en IT-avdelning därför behövt införskaffa och drifta flera olika lösningar från olika leverantörer för att skydda endpoints.

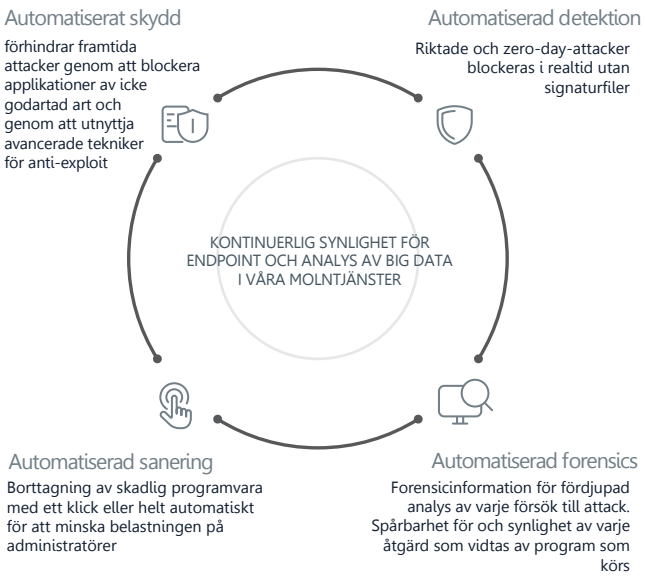
Adaptive Defense 360 är den första lösningen som ger en kombination av Endpoint Protection (EPP) och Endpoint Detection & Response (EDR) i samma lösning. **Adaptive Defense 360** automatiserar också funktioner vilket minskar belastningen på IT-strukturen. **Adaptive Defense 360** börjar med Pandas bäst-i-klassen-lösning för EPP som innehåller enkel och centraliserad säkerhet, korrigerande åtgärder, realtidsövervakning och -rapportering, profilbaserat skydd, centraliserad enhetskontroll samt webbövervakning och -filtrering.



Men det är bara början. Miljön för den skadliga koden och miljön för IT-säkerheten har genomgått stora förändringar när det gäller volym och förfining. Med över 200 000 nya virus som uppkommer varje dag, och den ökat sofistikerade teknik för att penetrera försvar och dölja skadlig kod, blir företagsnätverk mer sårbara än någonsin för zero-day och riktade attacker.
Traditionella Endpoint Protection-lösningar är effektiva på att blockera känd skadlig kod med hjälp av detekterings-teknik baserad på signaturfiler och heuristiska algoritmer. Men de är inget försvar mot zero-day och riktade attacker som drar nytta av det "gyllene tillfället för skadlig kod," det vill säga tiden mellan uppkomsten av nya skadliga program och frisläppandet av ett motgift från säkerhetsföretag.

En ökande klyfta som utnyttjas av hackare för att få in virus, Ransomware, trojaner och andra typer av skadlig kod i företagsnätverk. Sådana allt vanligare hot kan kryptera konfidentiella dokument och kräver en lösensumma, eller helt enkelt samla in känsliga uppgifter för industrispionage.

Adaptiv Defense är Pandas lösning på dessa typer av attacker. Adaptiv Defense ger en EDR-tjänst som exakt kan klassificera varje program som körs i en organisation och endast tillåta legitima program att köra. Den EDR kapacitet Panda Adaptive Defense 360 förlitar sig på som säkerhets-modell som bygger på tre principer: kontinuerlig övervakning av applikationer på företagets datorer och servrar, automatisk klassificering enligt maskininlärning på vår stora plattform data i molnet, och slutligen, våra tekniska experter analyserar de ansökningar som inte har klassificerats automatiskt att vara säker på beteendet hos allt som körs på företagets system.



Dessa funktioner kombineras nu i denna bäst-i-klassen-EPP-lösning från Panda, vilket sluter cirkeln av den adaptiva skydd mot skadlig kod, som nu omfattar **automatiserat förebyggande, upptäckt, forensics och sanering.**

DEN ENDA LÖSNINGEN FÖR ATT GARANTERA SÄKERHETEN FÖR ALLA PROGRAM SOM KÖRS

KOMPLETT OCH ROBUST SKYDD GARANTERAS

Panda Adaptive Defense 360 erbjuder två sätt att arbeta på:

- Standardläget gör att alla applikationer som katalogiserats som goodware ska köras, och de program som ännu inte är katalogiserade av Panda Security i det automatiserade system körs i väntan på katalogisering.
- Avancerat läge tillåter endast driften av goodware. Detta är den ideala formen av skydd för företag med en inställning av "nollrisk" till säkerhet.

FORENSIC INFORMATION

- Visar händelsediagram och logg för att få en klar uppfattning om alla händelser som orsakats av skadlig kod.
- Ger visuell information genom värmekartor på det geografiska ursprunget av anslutningar för skadlig kod, filer som skapats och mycket mer.
- Lokaliserar program med kända sårbarheter som installerats på ert nätverk.

SKYDD FÖR UTSATTA OPERATIVSYSTEM OCH APPLIKATIONER

System såsom Windows XP, som inte längre stöds av utvecklare och är därför blir ouppdaterade och sårbara, blir ett lätt byte för zero-day och den nya generationen attacker.

Dessutom utnyttjas sårbarheter i program som Java, Adobe, Microsoft Office och webbläsare till 90 procent av skadlig kod.

Modulen för att skydda sårbarheter i Adaptive Defense 360 använder kontextuella och beteenderegler för att säkerställa att företag kan arbeta i en säker miljö, även om de har system som inte uppdaterats.

TOTAL EPP-KAPACITET

Adaptive Defense 360 integrerar Panda Endpoint Protection Plus, den mest sofistikerade EPP lösningen från Panda, vilket ger fulla EPP funktioner, inklusive:

- Korrigerande åtgärder
- Centraliserad enhetskontroll: Förhindrar skadlig kod att komma in och förlust av data genom att blockera enhetstyper
- Webbövervakning och -filtrering
- Exchange-server antivirus och anti-spam
- Brandvägg för endpoint, och mycket annat...

KONTINUERLIG STATUSINFORMATION FÖR ALLA ENDPOINTS I NÄTVERKET

Få omedelbara varningar i det ögonblick som skadlig kod identifieras på nätverket, med en omfattande rapport om läget, smittade datorer, och vad skadlig kod orsakat.

Få rapporter via e-post på den dagliga verksamheten av tjänsten.

SIEM TILLGÄNGLIG

Adaptive Defense 360 integreras med SIEM lösningar för att ge detaljerade uppgifter om aktiviteten hos alla program körs på ditt system.

För kunder utan SIEM-lösning, kan Adaptive Defense 360 inkludera sitt eget system för lagring och hantering av säkerhetshändelser för att analysera all information som samlas in i realtid.

100% HANTERAD SERVICE

Sluta behöv investera i teknisk personal för att ta itu med karantäner eller misstänkta filer eller desinfektion och återställning av infekterade datorer.

Adaptiv Defense 360 klassificerar alla program automatiskt tack vare maskininlärning i våra Big Data-miljöer under kontinuerlig övervakning av PandaLabs experter.

TEKNISKA KRAV

Webbkonsol (för övervakning)

- Internetuppkoppling
- Internet Explorer 7.0 eller senare
- Firefox 3.0 eller senare
- Google Chrome 2.0 eller senare

Agent

- Operativsystem (arbetsstationer): Windows XP SP2 och senare, Vista, Windows 7, 8 & 8.1
- Operativsystem (servrar): Windows 2003 Server, Windows 2008, Windows Server 2012
- Internetuppkoppling (direkt eller via proxy)

Supporteras delvis (endast EPP): -

Linux, MAC OS X och Android