Adaptive Defense 360

Finn svarene, løs problemene

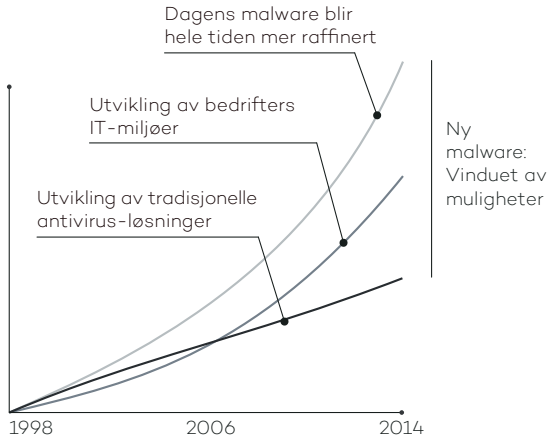
FULLFØR BESKYTTELSESSYKLUSEN MOT MALWARE GJENNOM Å INTEGRERE TOTAL GJENKJENNING, RESPONS OG UTBEDRING I ÉN ENKELT LØSNING

Å skulle forsvare Endpoints mot angrep er vanskelig. Beskyttelsen må inkludere et vidt spekter av mekanismer: tradisjonelle antivirus/antimalware, personlig brannmur, web- og epostfiltere samt kontroll av enheter. I tillegg må enhver beskyttelse også inneholde sikringstiltak mot zero-day og målrettede angrep. Fram til nå har det vært nødvendig å skaffe og opprette en rekke ulike produkter fra forskjellige tilbydere for å forsvare endepunktene innen IT.

Adaptive Defense 360 er den første og eneste tjenesten som kombinerer egenskapene Endpoint Protection (EPP) og Endpoint Detection & Respons (EDR) i én enkelt løsning.

Adaptive Defense 360 effektiviserer dessuten mulighetene, noe som reduserer byrdene hos IT.

Adaptive Defense 360 starter med Pandas beste EPP-løsning, noe som inkluderer enkel og sentralisert sikkerhet, avhjelpingshandlinger, real-time overvåking og rapporter, profilbasert beskyttelse, sentralisert enhetskontroll og web-overvåking og filtrering.

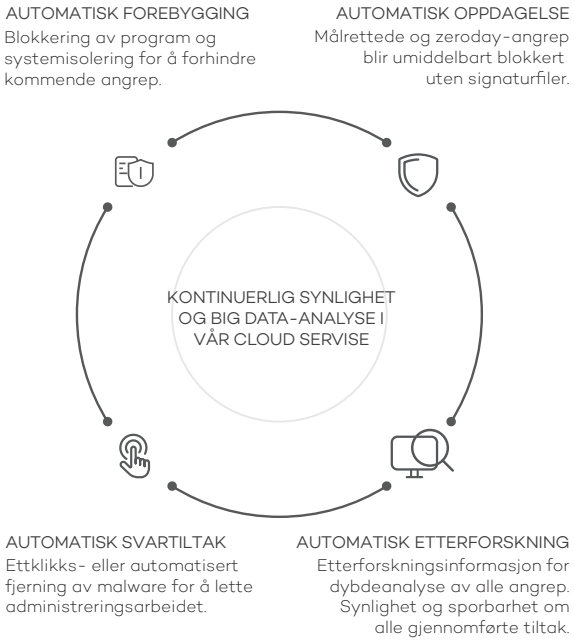


Dette er dessuten bare begynnelsen. Innen IT har malware- og sikkerhetsbildet gjennomgått store forandringer når det gjelder både volum og raffinement. Tatt i betraktning at over 200.000 nye virus dukker opp hver dag samt at stadig mer sofistikerte metoder benyttes for å penetrere eksisterende forsvar og med mål om å gjemme malware, så er bedriftsnettverk blitt mer sårbare enn noen gang ovenfor zero-day og målrettede angrep.

Tradisjonelle Endpoint Protection-løsninger er effektive til å blokkere kjent malware ved benyttelse av gjenkjennelsesteknikker bygget på signaturfiler og heuristiske algorytmer, men mot zero-day og målrettede angrep som benytter seg av «vinduet av muligheter» (tidsrommet mellom den første forekomsten av et nytt virus og sikkerhetskompanienes tilsvar) kommer de tradisjonelle forsvarene til kort. Dette «vinduet av muligheter» blir utnyttet av hackere for å plassere virus, ransomware, trojanere og andre typer malware i bedriftsnettverk. Slike stadig økende type trusler er i stand til å kryptere konfidensielle dokumenter med intensjoner om å forlange løsepenger, eller ganske enkelt bare stjele sensitive data for industrispionasje.

Adaptive Defense er Pandas løsning mot slike typer angrep. Adaptive Defense betyr en EDR-service som på en nøyaktig måte klassifiserer hvert eneste program i nettverket og bare tillater bruk av godkjente programmer.

Mulighetene til EDR (Endpoint Detection & Respons) i **Panda Adaptive Defense 360** bygger på en sikkerhetsmodell med tre prinsipper: kontinuerlig oversikt av programmer i selskapets computere og servere; automatisk klassifisering gjennom maskinlæring på Big Data-plattformen (i skyen/cloud) og helt til slutt; våre tekniske eksperters analyser av de programmene som ikke har blitt automatisk klassifisert, slik at all aktivitet i selskapets systemer er sikker.



Disse mulighetene og evnene er nå kombinert med den beste sorten EPP-løsning fra Panda, noe som fullfører sirkelen av tilpasningsdyktig beskyttelse mot malware og som nå også inkluderer automatisert forebygging, deteksjon, etterforskning og utbedring.

DEN ENESTE LØSNINGEN FOR Å GARANTERE SIKKERHETEN I ALLE PROGRAMMER SOM BENYTTES

EN GARANTI FOR KOMPLETT OG SIKKER BESKYTTELSE

Panda Adaptive Defense 360 tilbyr to ulike bruksområder:

- **Standard mode** godkjenner bruk av alle programmer katalogisert som goodware, samt programmer som gjenstår å bli katalogisert av Panda Security og de automatiserte systemene.
- **Extended mode** godkjenner kun bruk av goodware. Dette er den idéelle formen for beskyttelse for bedrifter med tilnærming til sikkerhet som ønsker nullrisiko.

DETALJERT ETTERFORSKNINGSINFORMASJON

- **Grafer med hendelsesforløp** gir klar og god oversikt over alle tilfeller som skyldes malware.
- Få visuell informasjon via **heat maps** om geografiske kilder av malware-kontakter, filer som er laget og mye mer.
- Lokaliser software som inneholder kjente svakheter innen nettverket ditt.

BESKYTTELSE FOR SÅRBARE OPERATIVSYSTEMER OG PROGRAMMER

Systemer som Windows XP, som ikke lenger er støttet av utvikleren og som derfor er sårbare og upatchet, blir et lett bytte for zero-day og andre nye generasjoner angrep.

Dessuten blir sårbarheter i programmer som Java, Adobe, Microsoft Office og ulike nettlesere utnyttet av 90% av malware.

Enheten med sårbarhetsbeskyttelse i **Adaptive Defense 360** bruker kontekstuelle- og relevante atferdsregler for å sikre bedriftens mulighet til å arbeide i et sikkert miljø selv om det skulle være systemer som ennå ikke er blitt oppdatert.

EN KOMPLETT EPP-LØSNING

Adaptive Defense 360 integrerer Panda Endpoint Protection Plus, den mest sofistikerte EPP-løsningen fra Panda, noe som medfører en komplett EPP-løsning, blant annet med:

- Utbedringskommandoer.
- Sentralisert enhetskontroll: forhindre malware og datatap gjennom blokkering av enheter.
- Web-overvåkning og filtrering.
- Mail-overvåkning og filtrering.
- Endepunktsbrannmur, mm.

KONTINUERLIG INFORMASJON OM NETTVERKSSTATUS

Få øyeblikkelige varsler når malware blir identifisert i nettverket, sammen med en full rapport som spesifiserer plasseringen, hvilke datamaskiner som er infisert og hvilke angrep malwaren har satt i gang.

Motta rapporter på e-post om den daglige aktiviteten servicen omfatter og utfører.

SIEM TILGJENGELIG

Adaptive Defense 360 er integrert med SIEM-løsninger som gir detaljerte data om aktiviteten til alle programmene som brukes i systemene dine.

For brukere uten SIEM, så inkluderer **Adaptive Defense 360** et eget system for å kunne lagre og styre sikkerhetstiltak som umiddelbart analyserer all informasjon som samles inn.

100% STYRT SERVICE

Du behøver ikke å måtte investere i teknisk personell som tar seg av karantener og mistenkelige filer, eller som må gjenopprette infiserte datamaskiner. **Adaptive Defense 360** klassifiserer alle programmer automatisk, takket være maskinlæring i vårt Big Data-miljø som igjen kontinuerlig overvåkes av PandaLabs egne eksperter.

KOMPATIBILITET MED TRADISJONELLE ANTIVIRUS-LØSNINGER

Adaptive Defense 360 kan operere sammen med tradisjonelle antivirus-løsninger, samt ta rollen som **et bedriftsverktøy i stand til å blokkere alle typer malware, inkludert målrettede og zeroday-angrep** som de tradisjonelle løsningene ikke klarer å finne.

TEKNISKE KRAV

Web Console (kun monitoring)

- Internettforbindelse
- Internet Explorer 7.0 eller nyere
- Firefox 3.0 eller nyere
- Google Chrome 2.0 eller nyere

Agenter

- Operativsystemer (arbeidsstasjoner): Windows XP SP2 og nyere, Vista, Windows 7, 8 & 8.1
- Operativsystemer (servere): Windows 2003 Server, Windows 2008, Windows Server 2012
- Internettforbindelse (direkte eller via en proxy)