



Adaptive Defense 360

FINN SVARENE, LØS PROBLEMENE

Vi står foran et nytt trusselbilde:

Kriminelle krypterer sensitiv og forretning-kritisk data mot løsepenger

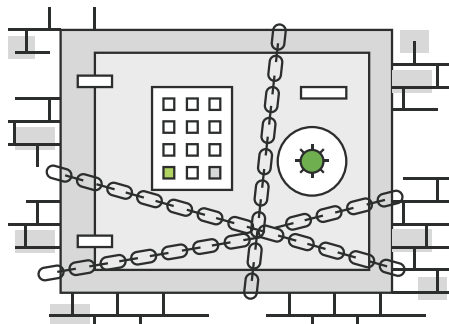
Angrep er blitt mer målrettede og mer intelligente. Det er lett å modifisere angrep og forbigå sikkerhet, selv om man holder seg 100% i tråd med tiden og oppdatert med hva ekspertene sier.

Opplæring og andre tiltak som antivirus, patching, avstengning av tjenester og backup viser seg gang på gang ineffektive mot denne typen angrep.



Dette handler om proaktivt forsvar, ikke førstehjelp og remedier. Adaptive Defense 360 har en lav kostnad både med hensyn til lisensiering, ressurs- og tidsbruk.

På denne måten hindres kriminelle i å angripe bedriften din. Man slipper slisomt og kostnadsfullt oppryddingsarbeid. Eller i verste fall, miste foretningkrittisk data.



Av den grunn har PANDA utviklet et helt nytt sikkerhetskonsept:

Endpoint Protection & Response (EDR)

Denne løsningen overvåker ALT som skjer på Windows-sluttpunktene i IT-miljøet ditt. Den utfører revisjon av ALLE prosesser som ønsker tillatelse til å kjøre.

Dermed stoppes ukjente trusler FØR de får muligheten å kjøre og vorde skade. Teste for svakheter eller utnytte legitime prosesser.

ENDPOINT **E**NDPOINT
DETECTION + **P**ROTECTION
RESPONSE **P**LATFORM

Adaptive Defense 360 kombinerer i tillegg EPP (Endpoint Protection Platform) og EDR i en og samme pakke, i tillegg til å sørge for 100% klassifisering av alle applikasjoner og prosesser som kjører i IT-miljøet.

99.91% revisjonsrutinene er dessuten automatiserte, som drastisk forenkler jobben for administratorer.

Høyt kvalifiserte labteknikere hos PANDA dobbeltsjekker det som ikke lar seg klassifisere gjennom BIG DATA analyse.



Produktspesifikasjoner

Systemkrav

EN GARANTI FOR KOMPLETT OG SIKKER BESKYTTELSE

Panda Adaptive Defense 360 tilbyr to ulike brukersområder:

- **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 ideelle 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

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 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 & 10
- Operativsystemer (servere): Windows Server 2002 - 2016