

Collective Intelligence

Fjärde generationens säkerhetsteknik är här

“Cloud-based, collective intelligence services are the next big thing for anti-malware. I expect that every AV vendor will need to embrace an approach like this if they expect to survive”.

Andrew Jaquith, Yankee Group's ledande säkerhetsanalytiker

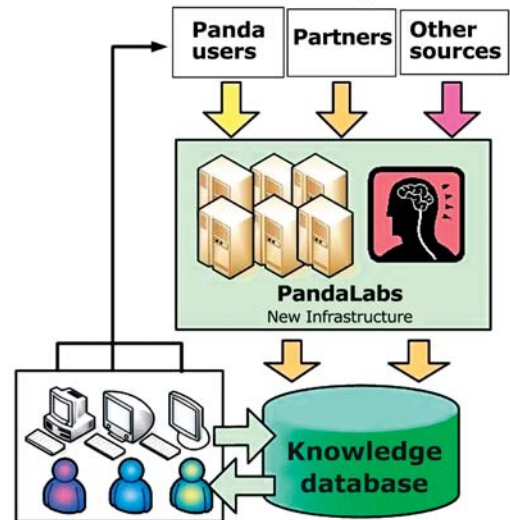
Collective Intelligence säkerhetsmodell bygger på insamlande av information kring skadlig kod från Internet, där informationen sedan analyseras i automatiserade processer i ett datacenter hos Panda. Kunskapen utvinns i Pandas servrar istället för på användarnas datorer.

På så vis kan **Collective Intelligence** maximera detektionskapaciteten i Panda Securitys säkerhetslösningar utan att reducera kundernas bandbredd och resursåtgång.

I dagsläget innehåller **Panda Securitys Collective Intelligence** nätverk cirka 4 miljoner datorer. Den sammanlagda kunskapen i systemet innehåller över 11 miljoner exemplar av skadlig kod och över 100 miljoner analyserade program. Under 2007 blev över 94 procent av de nya hot som nådde PandaLabs upptäckta via **Collective Intelligence**.



Panda Collective Intelligence Model



SÅ HÄR FUNGERAR DET:

1. Insamling av data från nätverket

Systemet samlar och lagrar beteendemönster från program, nya exempel av skadlig kod etc. Informationen kommer från Panda-användare och från andra företag och samarbetspartners.

2. Automatiserade dataprocesser

Systemet analyserar och klassificerar automatiskt de tusentals dagliga insamlingarna. Det sker genom att ett expertsystem korrelerar datainsamlingarna från nätverket med PandaLabs omfattande databas över skadlig kod.

3. Den erhållna kunskapen sprids

Den nya kunskapen levereras till användarna via webbtjänster eller som uppdateringar av signaturfiler. MalwareRadar är kompatibel med alla befintliga antiviruslösningar på datorerna och kompletterar dem för ännu högre nätverkssäkerhet. Tjänsten är transparent för slutanvändaren och administratören kan själv ställa in önskad resursåtgång.