CORE SISTEMI

## REALIZZAZIONE DI UN INFRASTRUTTURA ANTI-MALWARE

Una delle principali multiutility italiane attiva nella gestione e nello sviluppo di reti e servizi nei business idrico ed energetico, ha espresso l'esigenza di sostituire il sistema di Antivirus precedentemente in uso con un sistema anti-malware in grado di fornire una protezione a 360° sulle postazioni lavoro e sull'infrastruttura server, permettendo agli utenti di lavorare in totale sicurezza, mantenendo i livelli di performance efficaci sui servizi utilizzati.

Il progetto di implementazione della nuova piattaforma anti-malware ha previsto l'installazione nel data center, di 2 server in alta affidabilità dove risiede la Managemet per la gestione del sistema di distribuzione del client, policy di sicurezza, struttura dei gruppi ed aggiornamento delle postazioni (client/server ad essa collegati) e 2 server sempre in alta affidabilità dedicati al repository dei dati.

In particolare, le esigenze manifestate sono state le seguenti:

- Protezione sugli endpoint multilivello;
- Mantenimento dei livelli di performance sugli endpoint interessati;
- Gestione centralizzata intelligente ed efficiente;
- Blocco proattivo delle minacce (combinazione AV, IPS e Firewall locale).

Mediante le competenze sviluppate in tale ambito, Core Sistemi ha individuato in Symantec Endpoint Protection la soluzione in grado di soddisfare pienamente le esigenze manifestate. Attraverso la gestione da un'unica consolle di management efficiente è possibile impostare delle policy granulari sugli endpoint che abilitano il blocco del sistema, il controllo di applicazioni e dei dispositivi.

Di seguito vengono evidenziati alcuni dei principali passaggi eseguiti:

- Assessment dei requisiti del cliente al fine di comprendere i requisiti di sicurezza e di capacity dell'infrastruttura;
- Rimozione della precedente infrastruttura antivirus distribuita sulle postazioni di lavoro;
- Distribuzione del nuovo pacchetto antimalware sugli endpoint facenti parte del parco macchine;
- Distribuzione di Site server replicati per l'aggiornamento delle sedi remote in locale, con minor utilizzo di banda;
- Fine tuning dei gruppi suddivisi per centro di costo e sede, configurazione e distribuzione delle policy granulari da applicare sui sistemi facenti parte del datacenter (AD, Exchange ecc.).

I benefici più significativi riscontrati dall'adozione della nuova soluzione Anti-Malware sono:

- ✓ Alta affidabilità del servizio (Management e Database sempre on line);
- ✓ Elevato livello di sicurezza di ogni postazione di lavoro;
- ✓ Gestione granulare degli aggiornamenti (Gruppo o singolo endpoint);
- ✓ Analisi della Reputation e delle caratteristiche dei file sospetti per determinare se costituiscono un pericolo per i sistemi;
- ✓ Policy di interfaccia utente granulari per proteggere l'endpoint da qualsiasi modifica da parte dell'utente stesso;
- ✓ Possibilità di effettuare specifiche analisi di file sospetti attraverso il Security Response del vendor mediante rilascio delle funzionalità di ATP integration della nuova versione.