The background features a light blue, textured surface with a faint, embossed globe. Several large, dark blue gears are positioned around the edges, partially overlapping the globe's texture. The text is centered in a bold, black, sans-serif font.

Sisteme de prevenire a scurgerilor/pierderilor de date

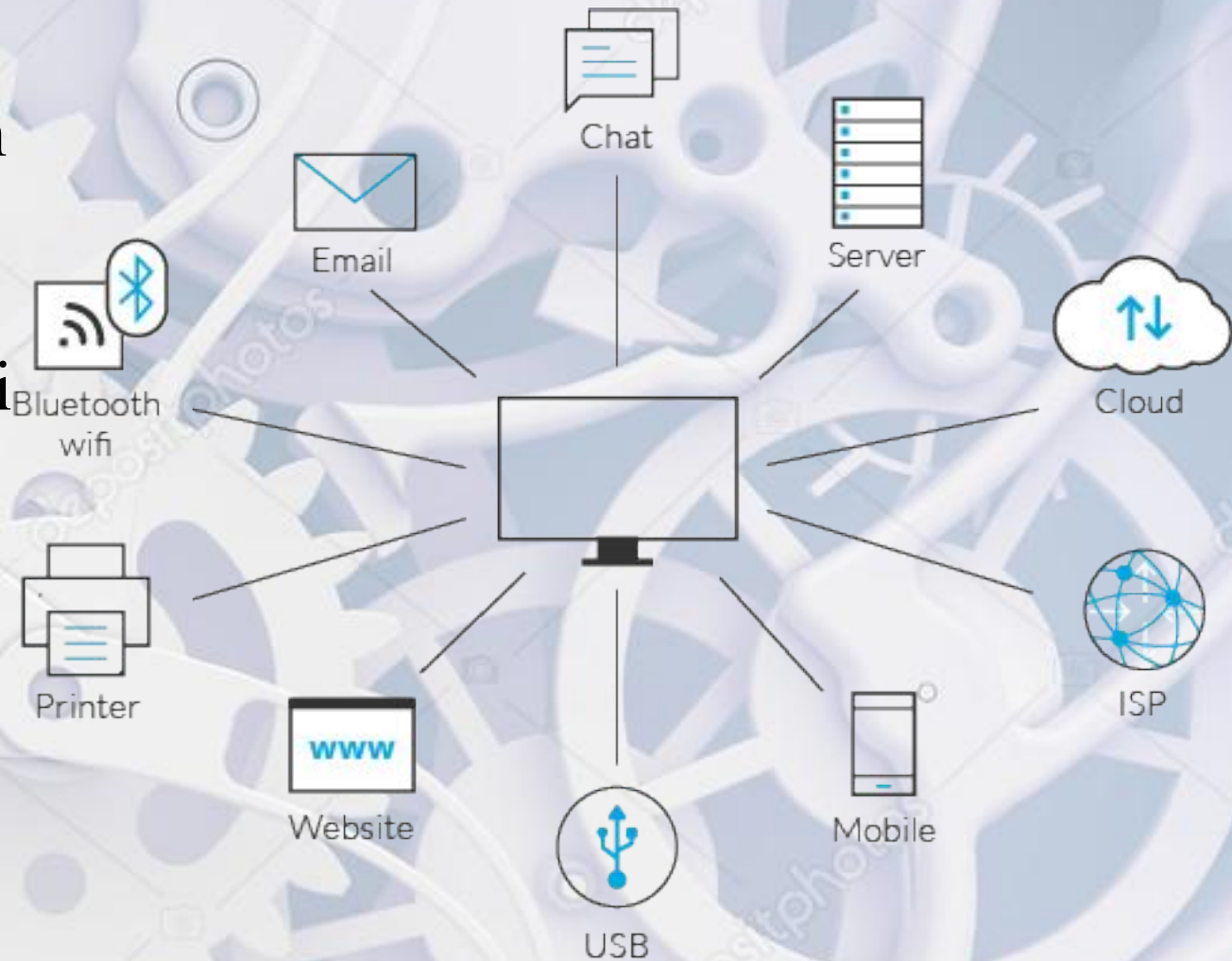
Cea mai bună opțiune tehnică pentru a preveni scurgerile de date este un sistem din clasa DLP(Data Leak Prevention).

Sistemele DLP sunt produse care permit detectarea și blocarea în timp real a transmiterii neautorizate (scurgerii) de informații confidențiale printr-un canal de comunicare care utilizează infrastructura informațională a companiei.



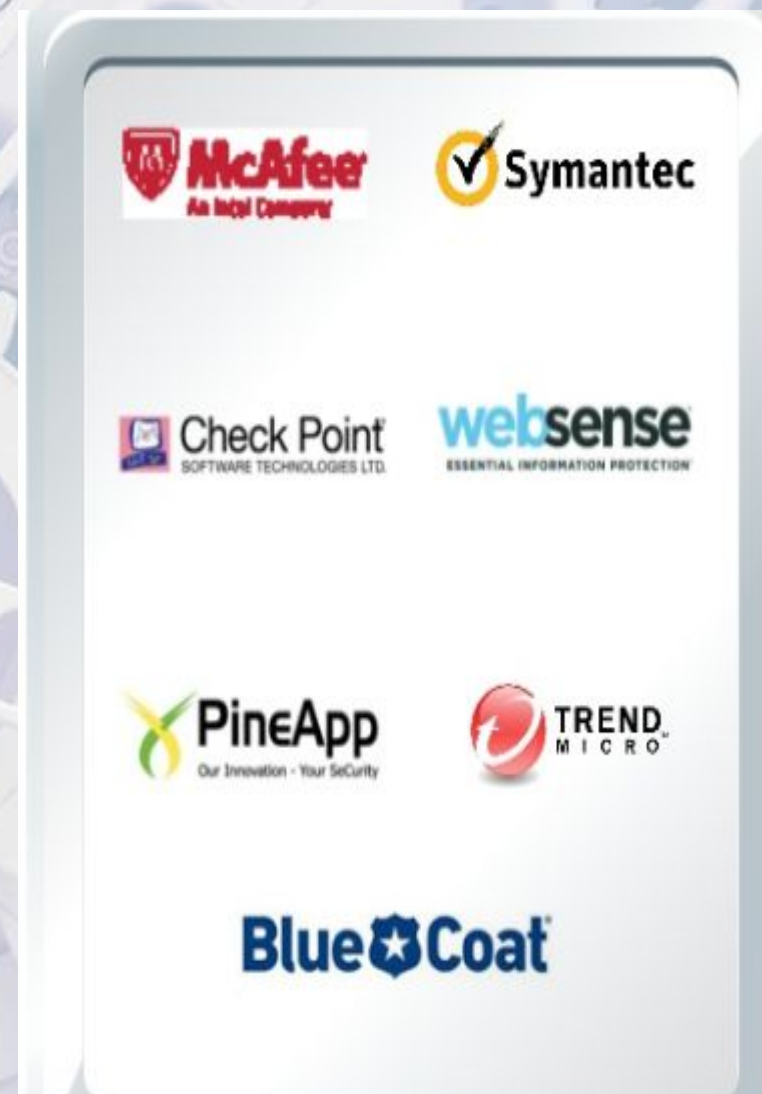
Produsul DLP detectează și / sau blochează transferul neautorizat de informații confidențiale (scurgeri) prin următoarele canale:

- Email (trafic SMTP, POP3, IMAP)
- Resurse web (trafic HTTP, HTTPS și FTP)
- ICQ, Jabber, MSN, Skype,
- Transfer de imprimare pe un dispozitiv extern



În prezent, există destul de multe soluții DLP pe piață care vă permit să identificați și să preveniți scurgerea informațiilor confidențiale.

- InfoWatch Traffic
- Websense
- McAfee
- Symantec
- TrendMicro
- CheckPoint



Принцип работы DLP



Securitatea informațională trebuie să ajute, nu trebuie să creeze obstacole . Toate canalele de comunicare trebuie să fie deschis

Adesea, pentru a preveni scurgerile de informații, companiile interzic angajaților să utilizeze canale convenabile și populare pentru a transmite și comunica cu lumea exterioară.

De exemplu, pentru securitate, este adesea permis să folosești doar e-mailuri corporative, iar mijloace precum ICQ, Skype.

Un sistem modern de securitate a informațiilor ar trebui să permită angajatului să utilizeze toate canalele pentru transmiterea informațiilor, dar să intercepteze și să analizeze fluxurile de informații care parcurg aceste canale.



Vă mulțumesc pentru atenție!