

# ANTIVIRUS

## Sicurezza informatica

Elena Maria Dal Santo

[elen.dalsanto@its-ictpiemonte.it](mailto:elen.dalsanto@its-ictpiemonte.it)

Intervento realizzato da

**ITS**  
TECNOLOGIE  
DELL'INFORMAZIONE E  
DELLA COMUNICAZIONE

# Storytime

**1967** nasce ARPANET

**1969** ARPANET collega i primi computer di 4 università americane

**1971** ARPANET connette 23 computer

*“Possiamo  
passare un  
programma da un  
computer a un  
altro?”*

# The Creeper

1971 nasce Creeper

Primo esempio di worm per computer

Non era malevolo, si limitava a mostrare un messaggio a video e a passare da un computer all'altro attraverso ARPANET.



I'M THE CREEPER,  
CATCH ME IF YOU CAN!

# The Creeper

La prima versione passava da un computer all'altro ripetendo le stesse operazioni (messaggi a video, passaggio su un altro pc).

**Ray Tomlinson:** crea una seconda versione.

Ora Creeper è un vero e proprio worm, che si replica e spedisce agli altri computer una copia di sé stesso.

*“Come  
controlliamo  
un worm?”*

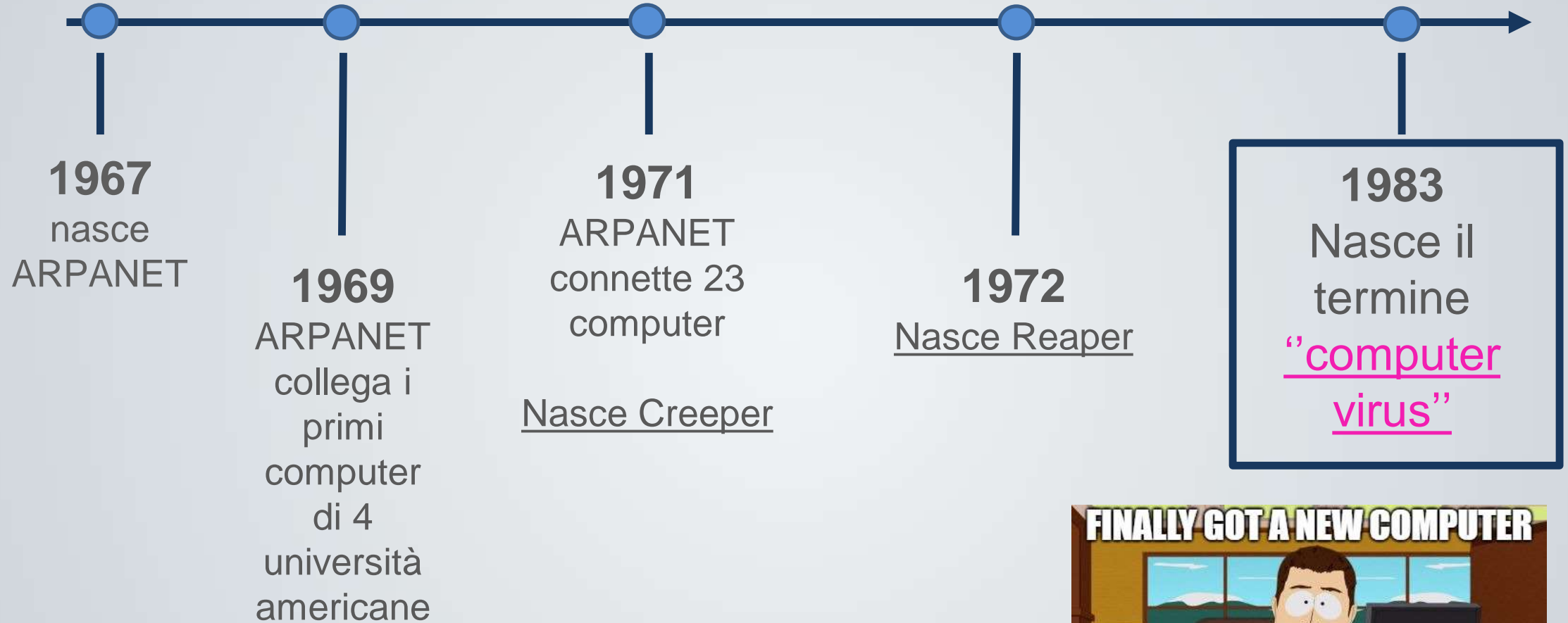
# The Reaper

Ray Tomlinson, creatore della seconda versione di Creeper, è anche il creatore del **primo antivirus della storia**



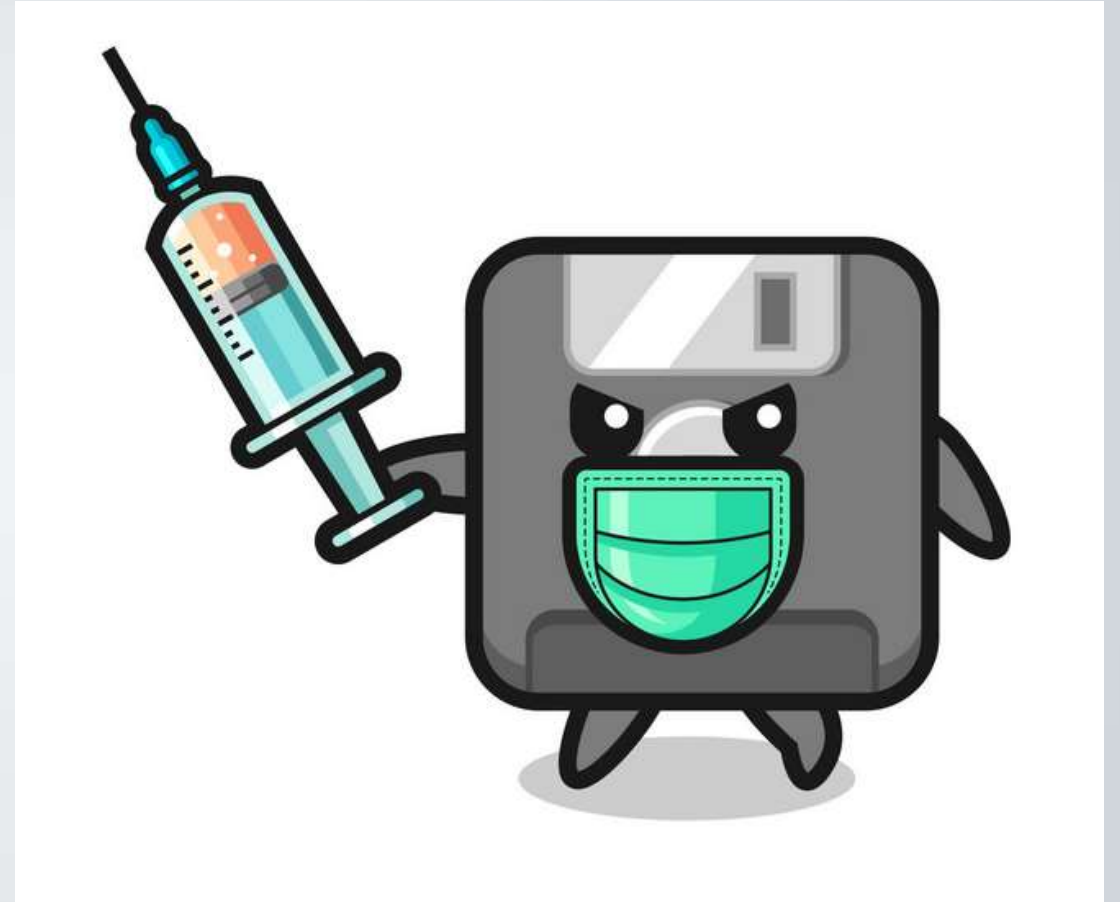
**1972** nasce Reaper

È un programma scritto per replicarsi e viaggiare su ARPANET, con il solo scopo di scovare Creeper.



All'inizio i virus venivano diffusi tramite floppy disk infettati, poi si è passati alle chiavette usb, e infine a internet

Verso la metà degli anni '80 nascono i primi antivirus



1987

Frederik Cohen dimostra che non è possibile costruire un algoritmo in grado di rilevare tutti i virus possibili e immaginabili



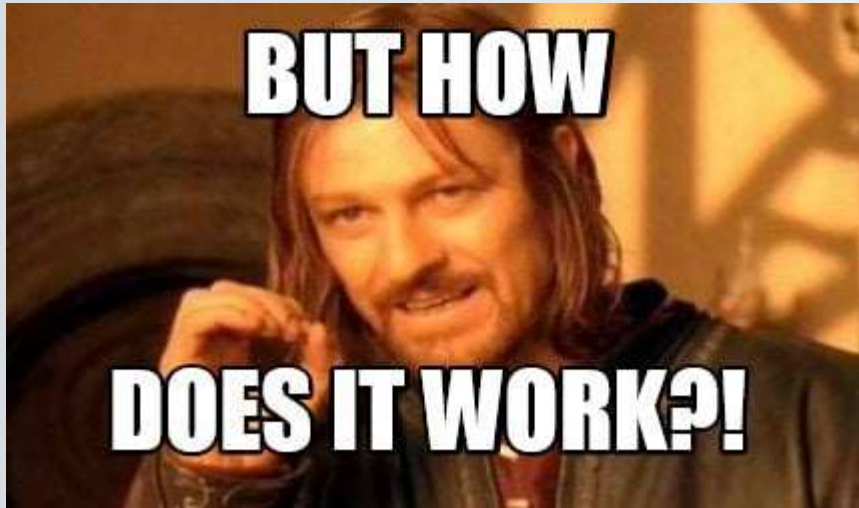


I moderni antivirus hanno un'efficacia che va dal 91% al 99,9%

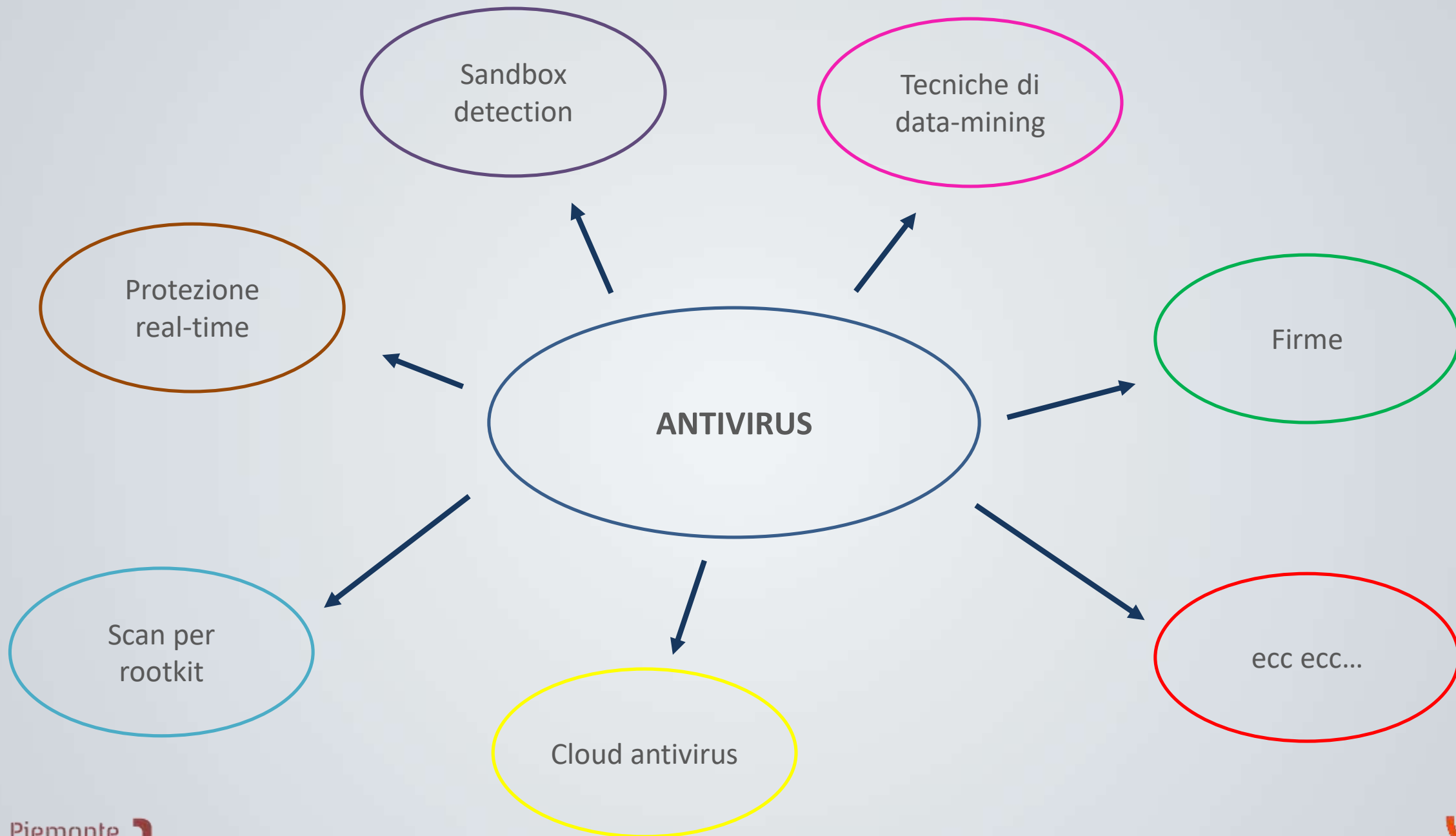
Le difficoltà maggiori sono nel rilevare vulnerabilità di tipo 0-days.

**PIUTOST, CHE  
NIENT L'È MEI  
PIUTOST**

# Come funziona un antivirus?



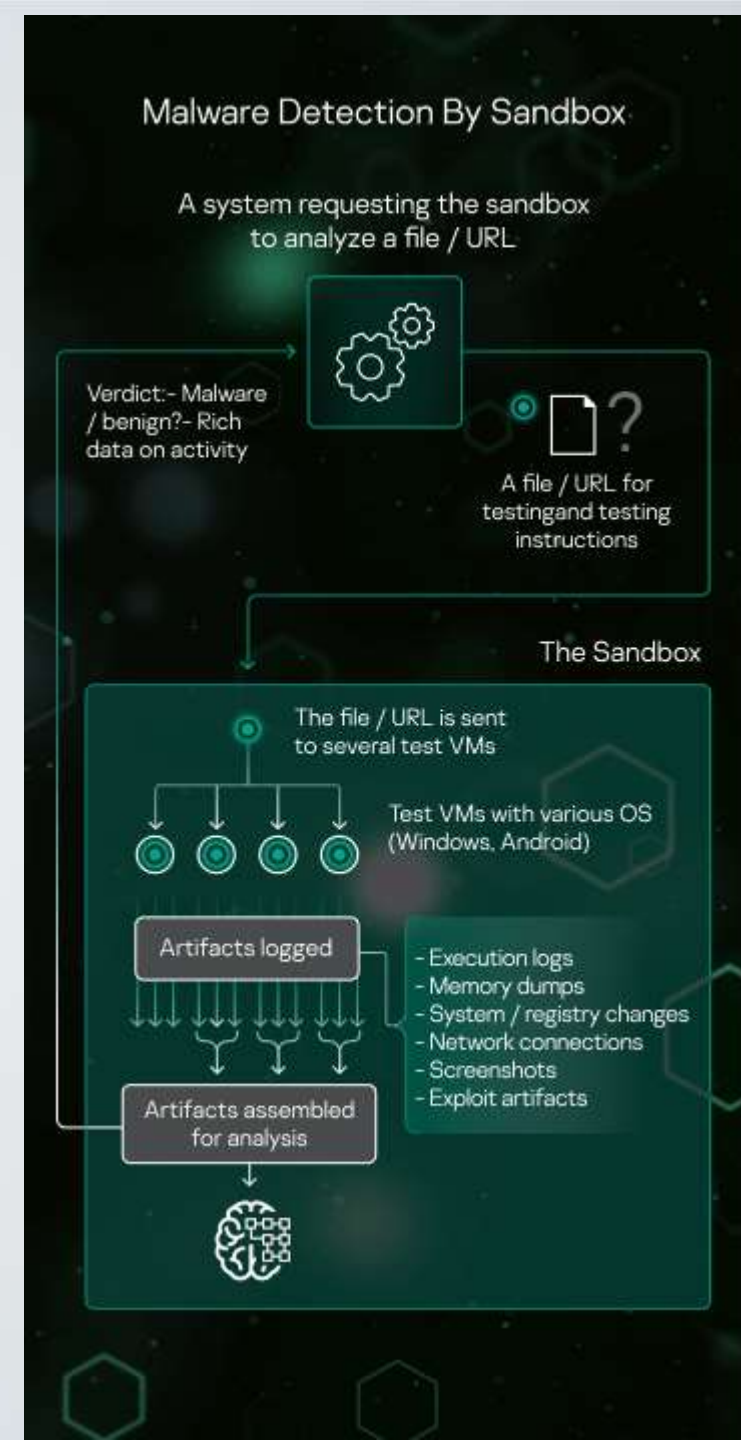
Esistono vari metodi per identificare un virus, e i moderni antivirus solitamente ne combinano più di una per raggiungere un livello di efficacia più elevato



# Sandbox detection

Il programma viene eseguito in un ambiente virtuale, dove l'antivirus ne analizza il comportamento e, analizzandone i log, determina se si tratta di un file infetto.

Come tecnica non viene utilizzata da sola, in quanto eseguire ogni singolo file in una VM richiede tempo e effort da parte della macchina.



# Tecniche di data-mining



## AntiVirus with Advanced Machine Learning

Scans and helps remove malware files that enter a device, using emulation to test and see what files do, and machine learning.

PC, Mac, Android



## Behavioral Protection

Uses artificial intelligence to classify applications based on behavior, and automatically helps block applications that display suspicious behavior.

PC

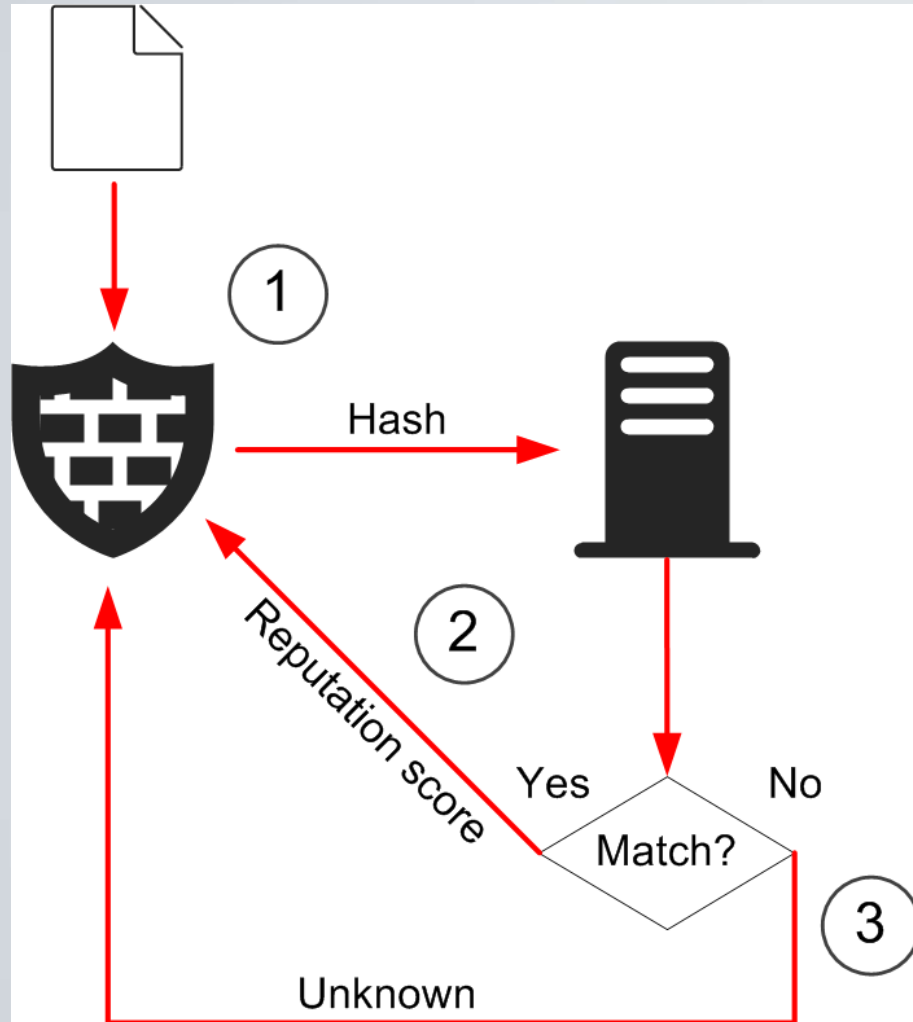


Algoritmi di machine learning vengono utilizzati per analizzare il file, il suo contenuto e il suo comportamento.

# Firme

Tramite ricerca euristica, per ogni antivirus viene costruito un database di firme note.

I file sospetti vengono analizzati in base alle loro caratteristiche peculiari e viene confrontato l'hash estratto con tutti quelli già noti.





# Firme

Norton protection also uses “emulation” (running each file in a lightweight virtual machine) to cause online threats to reveal themselves – this happens in milliseconds as you double-click on files on your desktop. File signature data is now stored in the cloud, and Norton protection has undergone hundreds of optimizations on the antivirus engine to minimize impacting the user experience.



Per sfuggire a questo tipo di analisi, gli hacker solitamente criptano parti dell’algoritmo del virus per non ricadere nelle firme salvate.

# Rootkit detection

L'antivirus continua a scansionare il sistema in cui si trova nel tentativo di trovare eventuali rootkit prima che vengano eseguiti.

Molti rootkit, oltre a tentare di ottenere privilegi amministrativi sul sistema, contengono righe di codice che si assicurano che un eventuale antivirus venga disabilitato.





# Protezione real-time

L'antivirus resta sempre attivo in background e si occupa di scansionare qualsiasi file o programma correlato alle azioni che compiamo.

Si occupa inoltre di monitorare in modo costante il contenuto della macchina, in modo da individuare in modo tempestivo eventuali comportamenti sospetti.



E quindi perché continuiamo ad avere problemi di malware?



**C'È CHI HA  
UNA SOLUZIONE  
PER OGNI PROBLEMA**

**E C'È CHI HA  
UN PROBLEMA  
PER OGNI SOLUZIONE**

Ci sono vari motivi per cui non riusciamo a trovare una soluzione definitiva al problema dei virus (e per cui dobbiamo partire dal presupposto che mai nessun programma potrà rilevare il 100% dei virus possibili e immaginabili)

Alcuni problemi dipendono dall'antivirus stesso, altri dalla macchina su cui gira, molti dipendono da come i malware stessi sono stati progettati e pensati...

# Rogueware

Categoria di malware che finge di essere un programma noto.

Basandosi su tecniche di social engineering, convincono l'utente ad effettuare download e installazione.

RogueAV è un tipo di rogueware che finge di essere un antivirus. Una volta installato, finge di effettuare una scansione e di rilevare dei virus, per poi proporre un pacchetto a pagamento per risolvere il problema.



# Falsi positivi

Si verifica quando un antivirus identifica come malware un software non dannoso.

Se l'antivirus è configurato per mandare immediatamente in quarantena o eliminare i file infetti, un falso positivo può risultare nell'impossibilità di usare un programma.

Nei casi più gravi, un falso positivo può rendere inutilizzabile parti di un sistema operativo (SO) o l'intero sistema.

# Falsi positivi



2010 McAfee VirusScan identifica svchost.exe (un file binario del SO Windows) come virus, causando alle macchine su cui girava dei continui reboot e impossibilità di connettersi a internet.

2010 un update di AVG danneggia la versione 64-bit di Windows, rendendo impossibile l'avvio del SO a causa di continui reboot.

2022 Microsoft Defender segnala tutte le app basate sul framework Electron come gravi minacce. App come Whatsapp, Spotify e Discord sono state impattate.



# Nuovi virus

Un buon virus è costruito sulle debolezze dell'antivirus

Per questo motivo, virus nuovi  
possono essere difficili da individuare  
anche se appartengono a una  
famiglia di virus già noti

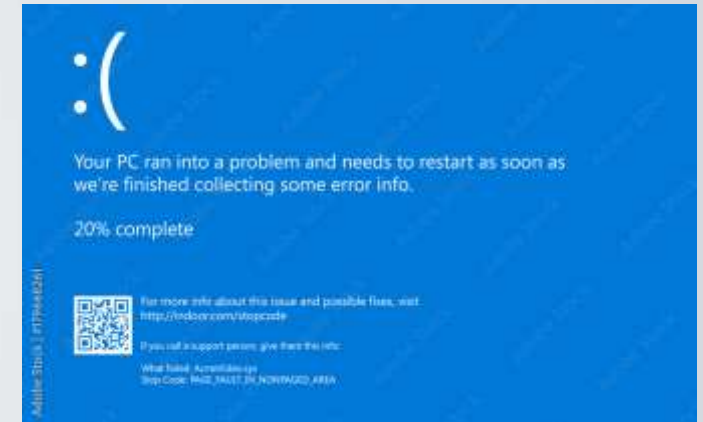


# Danni irreparabili

Quando trova un file danneggiato, l'antivirus cerca di rimuovere il codice compromesso.

Questa operazione non sempre lascia il file intatto e ancora utilizzabile.

Dal momento che ogni parte del computer può essere attaccata da un virus (quindi anche il BIOS), un antivirus potrebbe rendere inutilizzabili parti fondamentali della macchina.





Visti i problemi che potrebbero esserci, viene spontaneo chiedersi se gli antivirus sono l'unica soluzione possibile al problema dei malware...



La risposta è no! Esistono soluzioni alternative, che possono essere utilizzate anche in combinazione con un antivirus...



# Firewall

Un **firewall** è un componente, inizialmente passivo, di difesa perimetrale di una rete.

Il suo compito è quello di regolare l'accesso a un dato servizio di rete o a un sistema, secondo delle regole precedentemente definite.

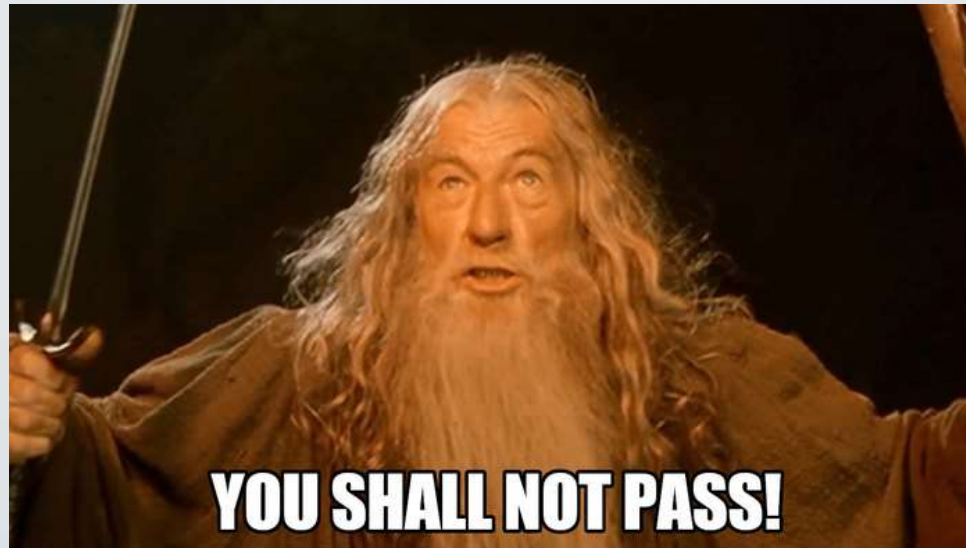
Analizzando una piccola porzione dei dati in transito (presenti nell'header dei pacchetti), decide se lasciar passare o eliminare il pacchetto.



# Firewall

Il compito del firewall ci fa capire anche il suo posizionamento all'interno della rete:


*Un firewall è il primo punto di accesso e l'ultimo punto di uscita della rete*



# Firewall

Che criteri usa un firewall per verificare le sue regole?

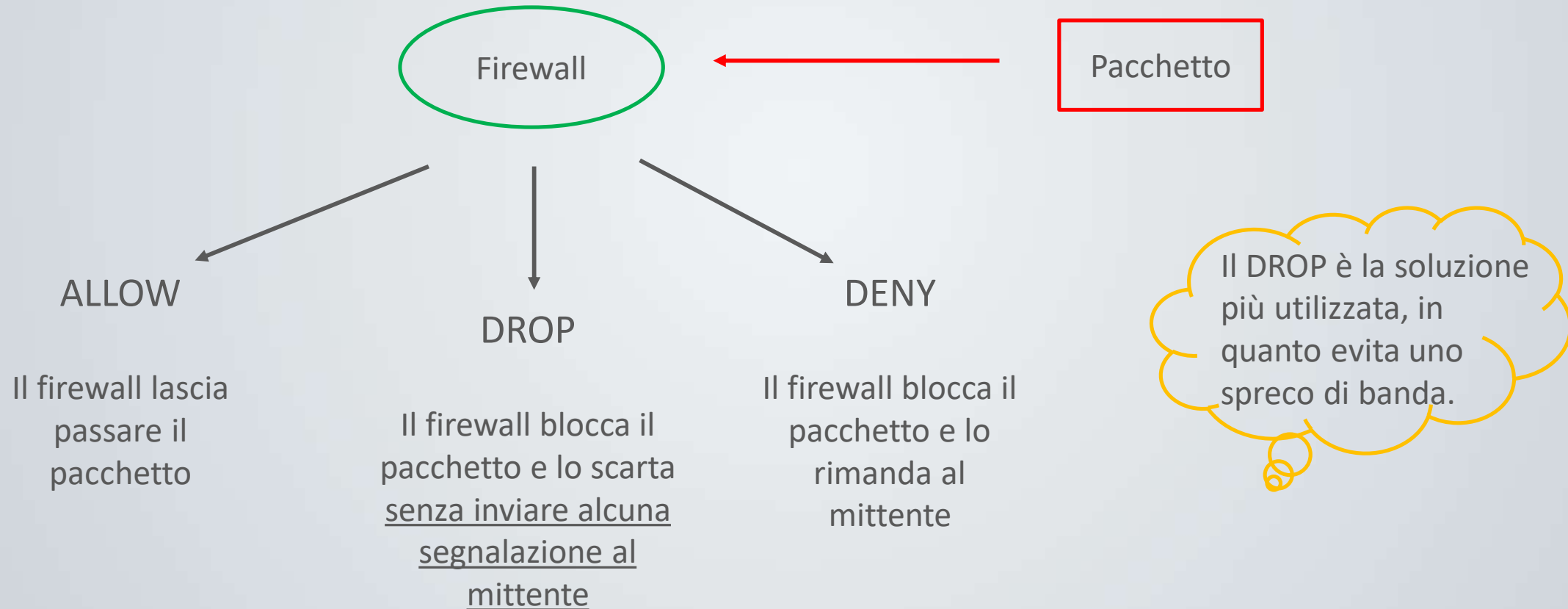
- *Default-allow* → tutto è concesso, tranne ciò che è esplicitamente vietato
- *Default-deny* → tutto è vietato, tranne ciò che è esplicitamente concesso



È quello solitamente utilizzato, in quanto garantisce più sicurezza e maggiore precisione nella definizione delle regole

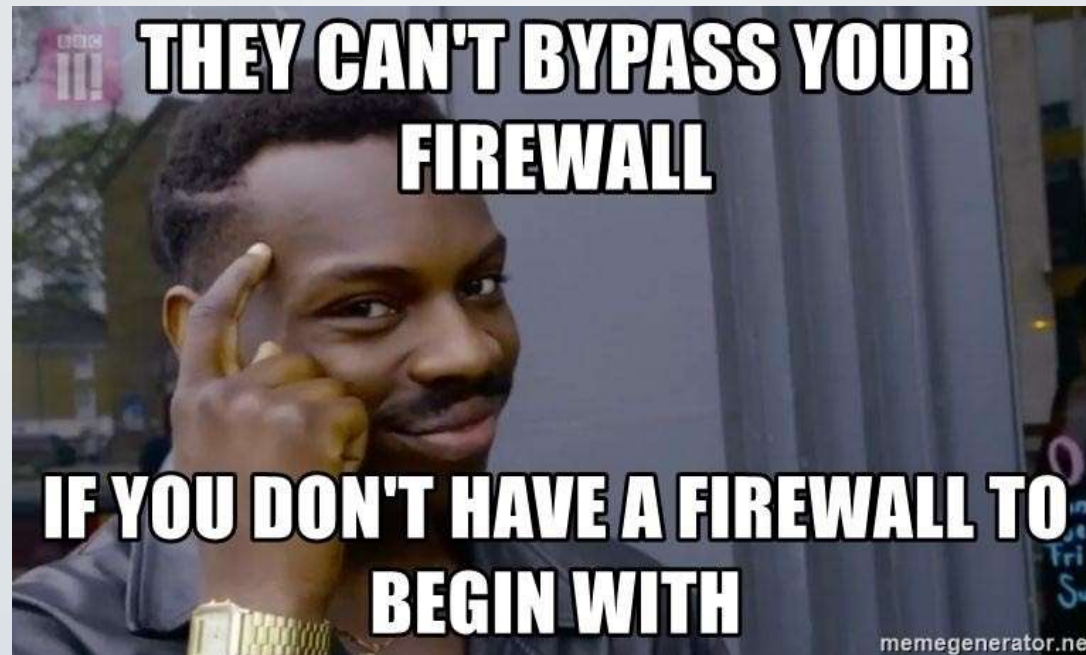
# Firewall

*Come funziona un firewall?*



# Firewall

Esistono varie tipologie di firewall, ne vediamo alcune e le loro caratteristiche principali...





# Firewall

- Network-based firewall (o firewall perimetrale)

Componente hardware stand-alone che viene posto sul confine di rete per filtrare tutto il traffico che questa scambia con l'esterno. Le regole vengono impostate in base all'indirizzo IP sorgente, a quello di destinazione e alla porta usata per la connessione.

- Personal firewall (o firewall software)

Applicazione software che controlla tutti i programmi che tentano di accedere a Internet presenti sul computer su cui è installato. Le regole vengono impostate dall'utente, tramite consensi negati o concessi all'applicazione.



# Firewall

- Stateless firewall

Analizza ogni pacchetto che lo attraversa singolarmente, senza tenere conto di quelli che l'hanno preceduto. Le regole si basano su indirizzo IP sorgente e destinazione, porta della sorgente e protocollo utilizzato.

- Stateful firewall

Ha le stesse regole del firewall stateless, ma in più tiene traccia delle connessioni e del loro stato (individuando così eventuali connessioni non più attive).

# Firewall

- Next generation firewall

Riunisce in un unico pacchetto firewall le tecnologie viste finora, più altre funzionalità aggiuntive (es. un supporto per le VPN). L'obiettivo è di semplificare la configurazione e la gestione di un sistema di tecnologie e al tempo stesso di migliorarne le performance.

- Web Application Firewall (WAF)

Specifica forma di software firewall che filtra, monitora ed eventualmente blocca il traffico HTTP in entrata e uscita da un servizio web. Utile per prevenire minacce veicolate attraverso il web.

# Firewall

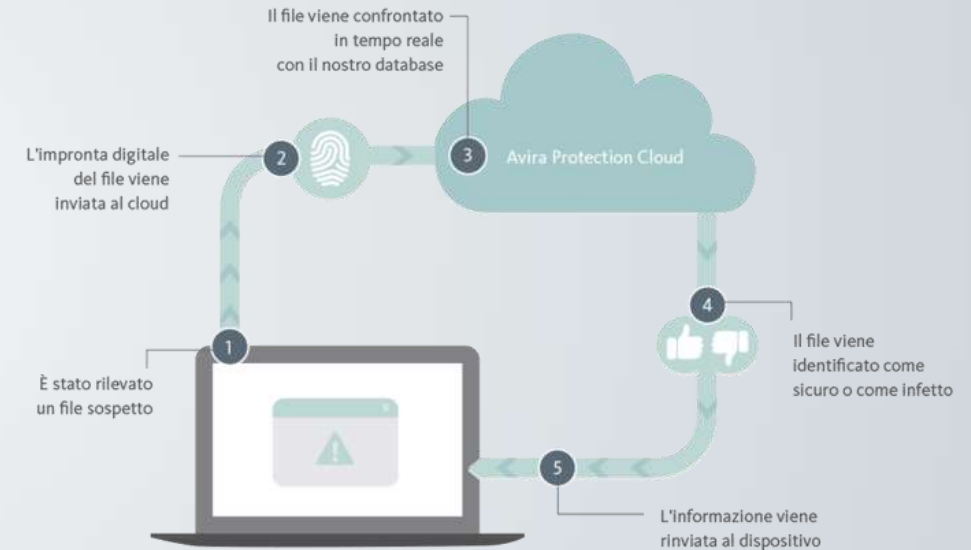
Per quanto utili, i firewall presentano 3 limiti principali per cui è sconsigliato usarli al posto di un antivirus:

1. Efficacia di un firewall  $\longleftrightarrow$  efficacia delle regole con cui è stato configurato
2. La configurazione di un firewall è il risultato di un compromesso tra usabilità della rete, sicurezza e risorse a disposizione
3. Una grande quantità di minacce proviene dalla rete interna (portatili, virus, reti non adeguatamente protette, ecc)

# Cloud antivirus

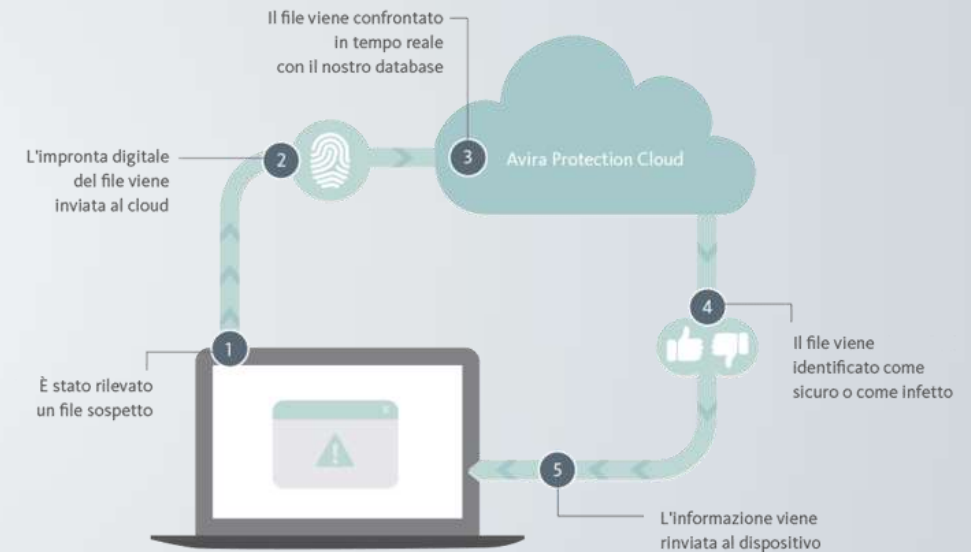
Tecnologia che usa un software installato sulla macchina in uso per interfacciarsi con un'infrastruttura provider, che si occupa di fornire tutti i normali servizi di un antivirus.

Le operazioni di scansione e rilevamento dei virus sono quindi gestite da un provider esterno, evitando così sovraccarichi di lavoro.



# Cloud antivirus

Inoltre, un antivirus cloud può sfruttare diversi software antivirus per compiere l'analisi del file sospetto, evitando così all'utente di dover installare più software sulla propria macchina locale.



# Online scanning

Si tratta di antivirus gratuiti, che vengono messi a disposizione su siti solitamente mantenuti da aziende proprietarie di software antivirus.

Utili in quanto potrebbero essere più aggiornati del nostro software, pur offrendo meno funzionalità.

Inoltre, la prima cosa che cerca di fare un virus è disabilitare qualunque software antivirus: un servizio completamente online potrebbe essere l'unico modo di sapere se il nostro pc è stato infettato.



# Tools specializzati

Utili per rimuovere i malware più aggressivi o appartenenti a tipologie rare/particolari/non coperte dagli antivirus.

Data la loro specializzazione, sono meno soggetti a falsi positivi rispetto a un antivirus tradizionale.

Appartengono a questa categoria anche software avviabili tramite chiavette usb o cd, che possono essere utilizzati nei casi in cui il sistema operativo stesso non è più avviabile in quanto compromesso da un malware.

# Proviamo?

Proviamo a costruire un semplice antivirus





# Link utili

- An undetectable computer virus-  
<https://web.archive.org/web/20110604155118/http://www.research.ibm.com/antivirus/SciPapers/VB2000DC.htm>
- Computer viruses – Theory and experiments -  
<https://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html>
- Un database di hash di virus noti (per costruire il vostro antivirus) - <https://virusshare.com/hashes>

