

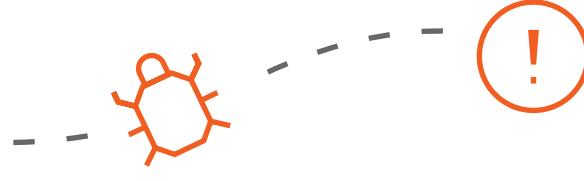
Aumento degli attacchi agli endpoint

Il passaggio allo smart working e al lavoro ibrido è stato accolto con piacere dagli hacker, che in questo modo possono sfruttare le vulnerabilità e le lacune di un ambiente senza perimetro:



105%

aumento del ransomware nel 2021¹



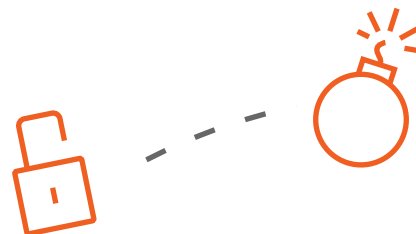
93%

delle reti aziendali sono state violate²

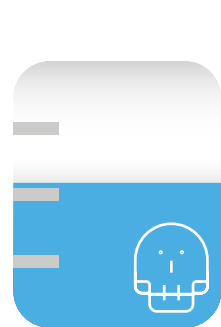


14%

delle aziende sono pronte a difendersi²

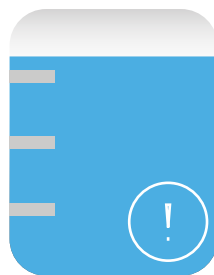


OGNI ENDPOINT È UN POTENZIALE PUNTO DI ACCESSO AI DATI DELLA VOSTRA AZIENDA. E i cybercriminali lo sanno bene.



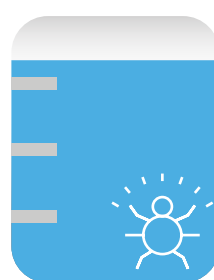
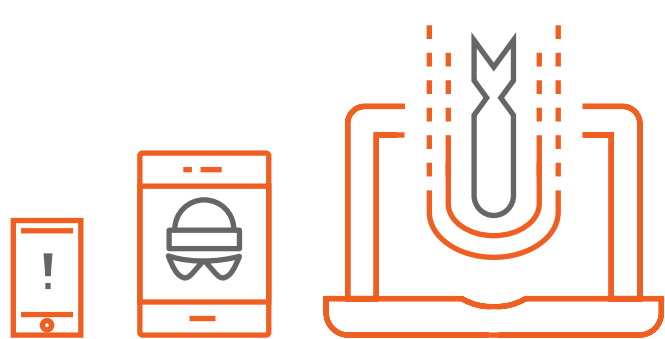
68%

delle aziende ha subito attacchi agli endpoint³



80%

delle violazioni rilevate sono attacchi zero-day³



81%

degli attacchi alle aziende includeva una qualche forma di malware³



83%

delle minacce malware viene salvato nelle posizioni seguenti:³

%temp%



%appdata%



%cache%



%desktop%



Per consentire alle aziende di essere più proattive e resilienti contro gli attacchi informatici è consigliabile un approccio moderno alla sicurezza degli endpoint.



Migliore protezione dei dipendenti da remoto con sistemi EDR e strumenti di visibilità automatizzati:
Capture Client

Informazioni più accurate grazie a funzioni di intelligence e reporting immediatamente fruibili:
Real-Time Deep Memory Inspection™

Ricerca proattiva delle minacce nascoste nel vostro ambiente:
Threat Hunting

BLOCCO DELLE MINACCE A UNA VELOCITÀ SENZA PRECEDENTI

Siete pronti per i prossimi passi?

SCARICA IL FOGLIO DATI

GUARDA IL VIDEO

PROVA GRATIS

SONICWALL®



¹ Rapporto SonicWall 2022 sul Cybercrime: <https://www.sonicwall.com/2022-cyber-threat-report/>

² Forbes: <https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/>

³ Expert Insights: <https://expertinsights.com/insights/50-endpoint-security-stats-you-should-know/>