ivanti

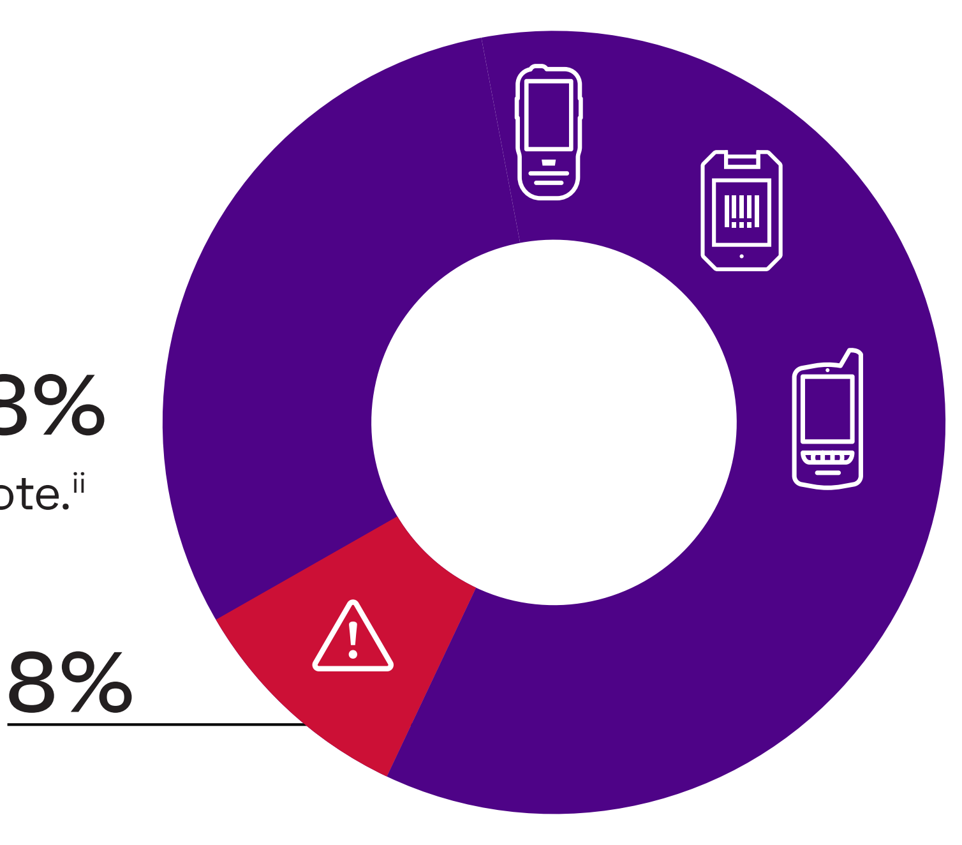
# Cinque cose da migliorare nella gestione delle vulnerabilità

## 1 Punti ciechi della vulnerabilità

Non è possibile proteggere e riparare ciò che non si vede o che non si sa cercare.

**1 dipendente su 3** delle aziende Fortune 1000 utilizza applicazioni SaaS basate su cloud non approvate.[i]

Tre degli scanner più famosi – Nessus, Qualys e Nexpose – **non hanno ancora individuato quasi l'8%** delle vulnerabilità ransomware note.[ii]



## 2 Mancanza di larghezza di banda del team

Supponiamo di dover cercare di applicare una patch a ogni vulnerabilità o rischio esistente, o semplicemente di dover esaminare manualmente le vulnerabilità più rilevanti per l'organizzazione e l'ambiente.

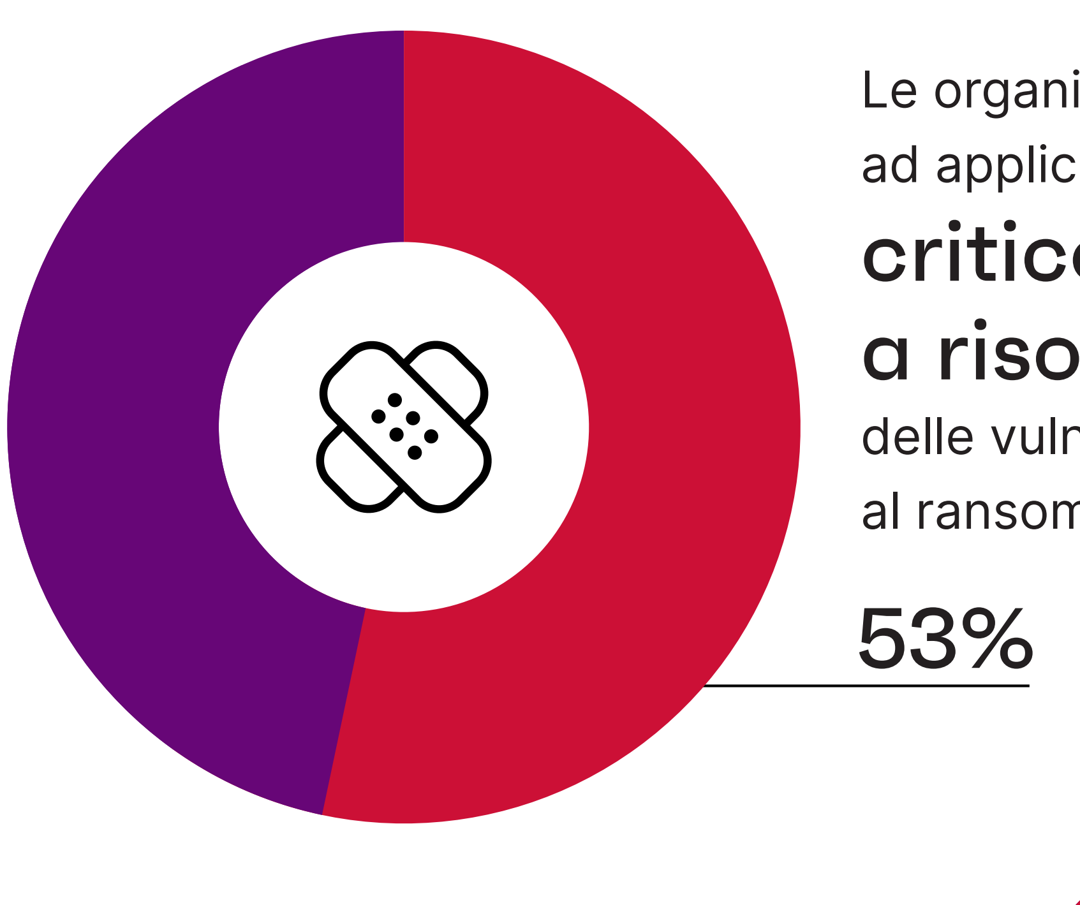
⚠
**236,000+**
Oltre 236.000 vulnerabilità ed esposizioni critiche (CVE)

⚠ ⚠
**29,000+**
Armamento di oltre 29.000 CVE

⚠ ⚠ ⚠
**+ di 9.600**
CVE con capacità di Remote Code Execution (RCE) e/o Privilege Escalation

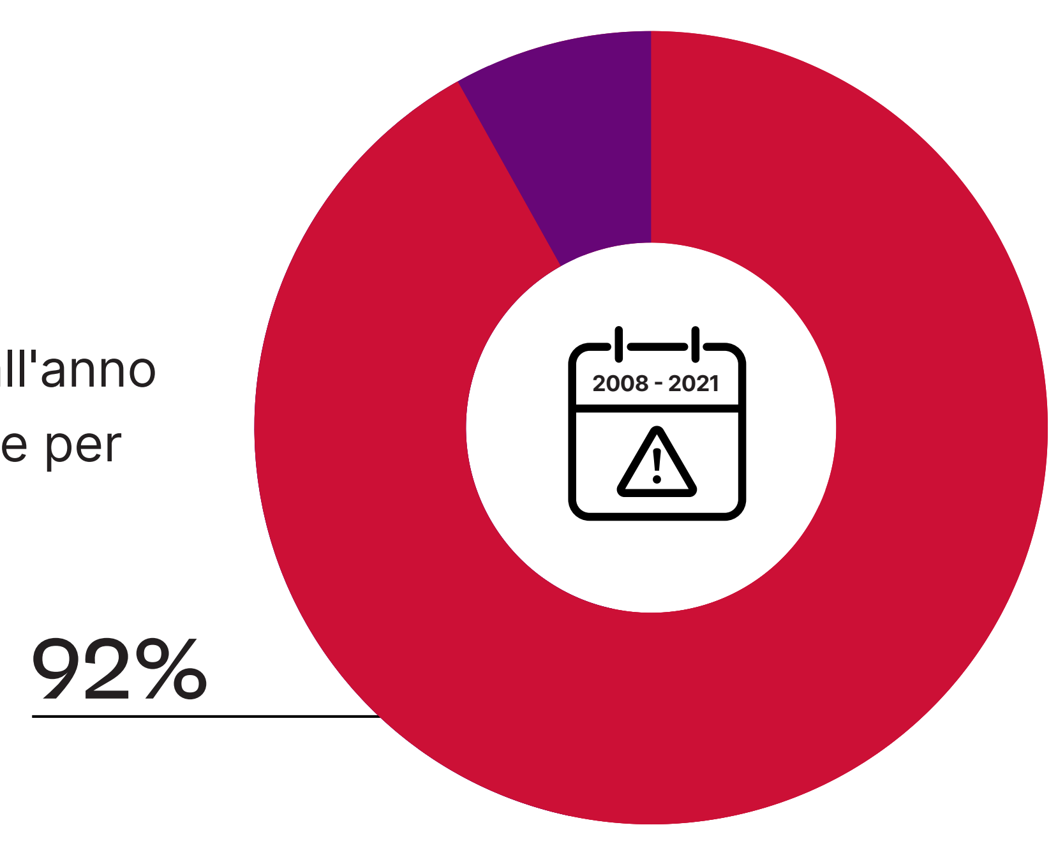
## 3 Esposizione a CVE meno "critiche" e più vecchie

Non tutte le vulnerabilità comportano lo stesso rischio e non è possibile stabilire quali siano rilevanti per l'organizzazione solo in base all'età o alla criticità.



Le organizzazioni che si limitano ad applicare patch alle CVE di livello **critico non riescono a risolvere il 53%** delle vulnerabilità legate al ransomware.[iii]

Il 92% delle vulnerabilità più importanti sono precedenti all'anno scorso, con alcune pubblicate per la prima volta nel 2008![iv]



## 4 Poche risorse del programma e buy-in interno

### RBVM di base

Assegnazione di priorità tramite punteggi CVSS e punteggi dello scanner

**Punti deboli**
Dipendono dalla qualità dei dati e dalla frequenza degli aggiornamenti dello scanner

Tralascia le vulnerabilità con basso punteggio in relazione ai rischi specifici dell'organizzazione

**Punti di forza**
Esiste una gestione delle vulnerabilità

### RBVM intermedio

Definizione delle priorità in base alla probabilità di utilizzo delle CVE dell'anno precedente

**Punti deboli**
Necessita di sintonizzazioni manuali e verifiche costanti

Tralascia le vulnerabilità più vecchie ancora rilevanti (+1 anno)

**Punti di forza**
Dà priorità alla risoluzione oltre che al punteggio CVSS

Enfatizza le nuove patch di vulnerabilità

### RBVM avanzato

Assegnazione delle priorità tramite informazioni sulle minacce provenienti da più fonti e rischi organizzativi contestualizzati

**Punti deboli**
Richiede una suite di strumenti completa per coprire più dati

**Punti di forza**
Contiene tutte le possibili fonti di dati sulla vulnerabilità

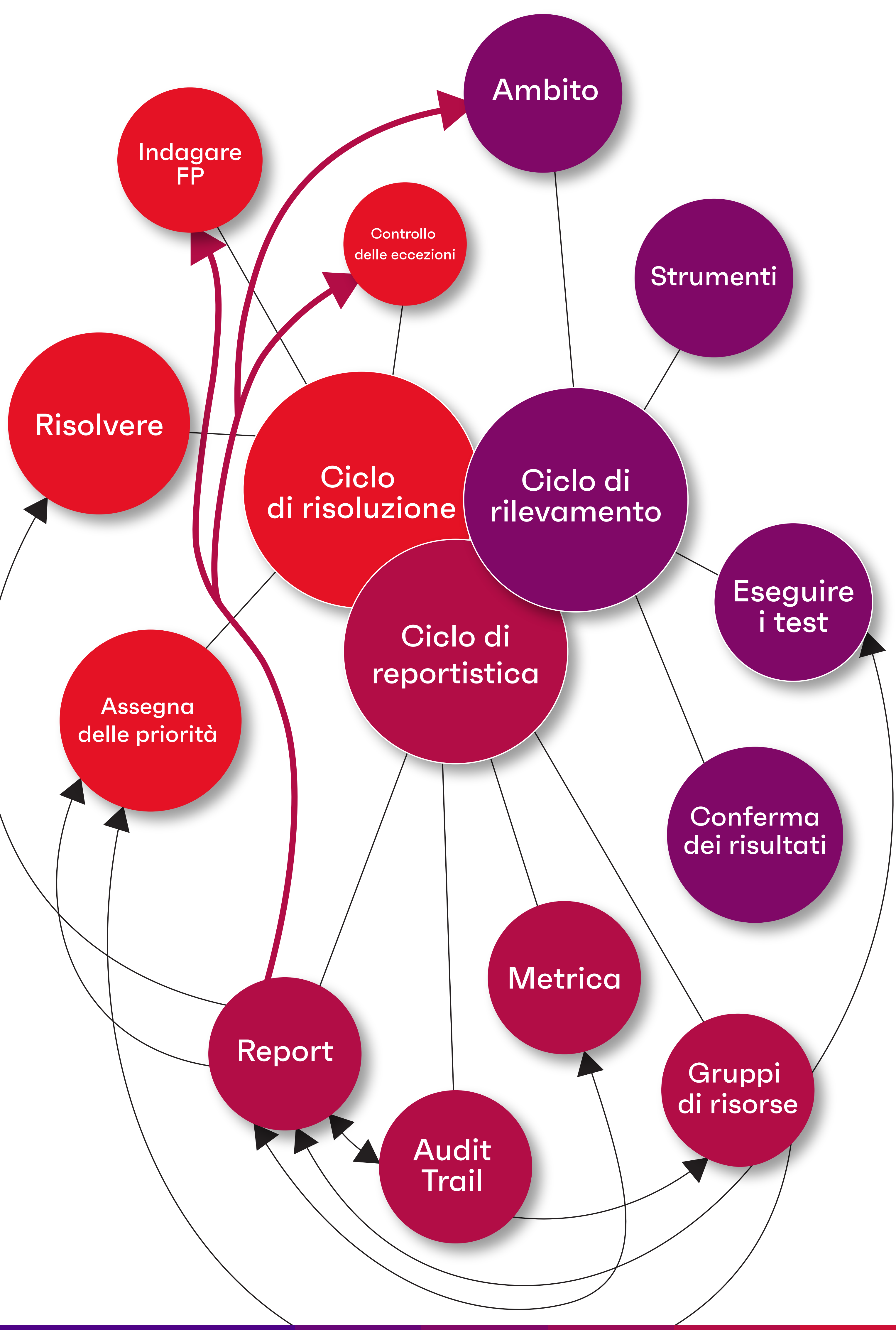
Assegna priorità in base a rischi specifici e univoci

Si adatta rapidamente per incorporare nuovi contesti e perfezionare la definizione delle priorità

## 5 Reportistica

Un programma di gestione delle vulnerabilità efficace può creare rapidamente una rete intricata di rilevamento, risoluzione e reportistica interdipartimentale necessaria per una corretta esecuzione.

Senza una sorta di strumento di automazione per aggregare, dare priorità e visualizzare le informazioni e le attività sulle vulnerabilità, il programma di cybersecurity potrebbe essere vanificato dai requisiti di reportistica prima ancora di iniziare.[v]



Non deve essere così. Leggere il Spotlight Ransomware Report 2022 per le ultime vulnerabilità di tendenza.

Scarica il report

---

[i] "Why shadow IT is the next looming cybersecurity threat" (The Next Web)
[ii] Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
[iii] Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
[iv] Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
[v] OWASP Vulnerability Management Guide (OVMG) - June 1, 2020