

Bitdefender

GravityZone

Risk Management - Patch Management

Roberto Novasconi - Avangate Italia

Senior Support and Training Specialist

AVANGATE
Distributore a valore aggiunto

Bitdefender
AUTHORIZED DISTRIBUTOR

Agenda

Bitdefender

- Normativa e rischi reali
- L'antimalware non basta
- Workflow tipico per la gestione di rischi e patch
- Funzionalità e punti di forza di GravityZone Patch Management
- DemoPatch Management:
Deploy, OnDemand Patching, Automated Patching, Report, Notification

GDPR

Normativa e rischi reali

2016 GDPR indirizza in modo esplicito il fattore configurazione ed aggiornamento software

I sondaggi indicano che un incidente di sicurezza su 3, con conseguente furto di dati, è stato reso possibile dalla mancanza di patch.

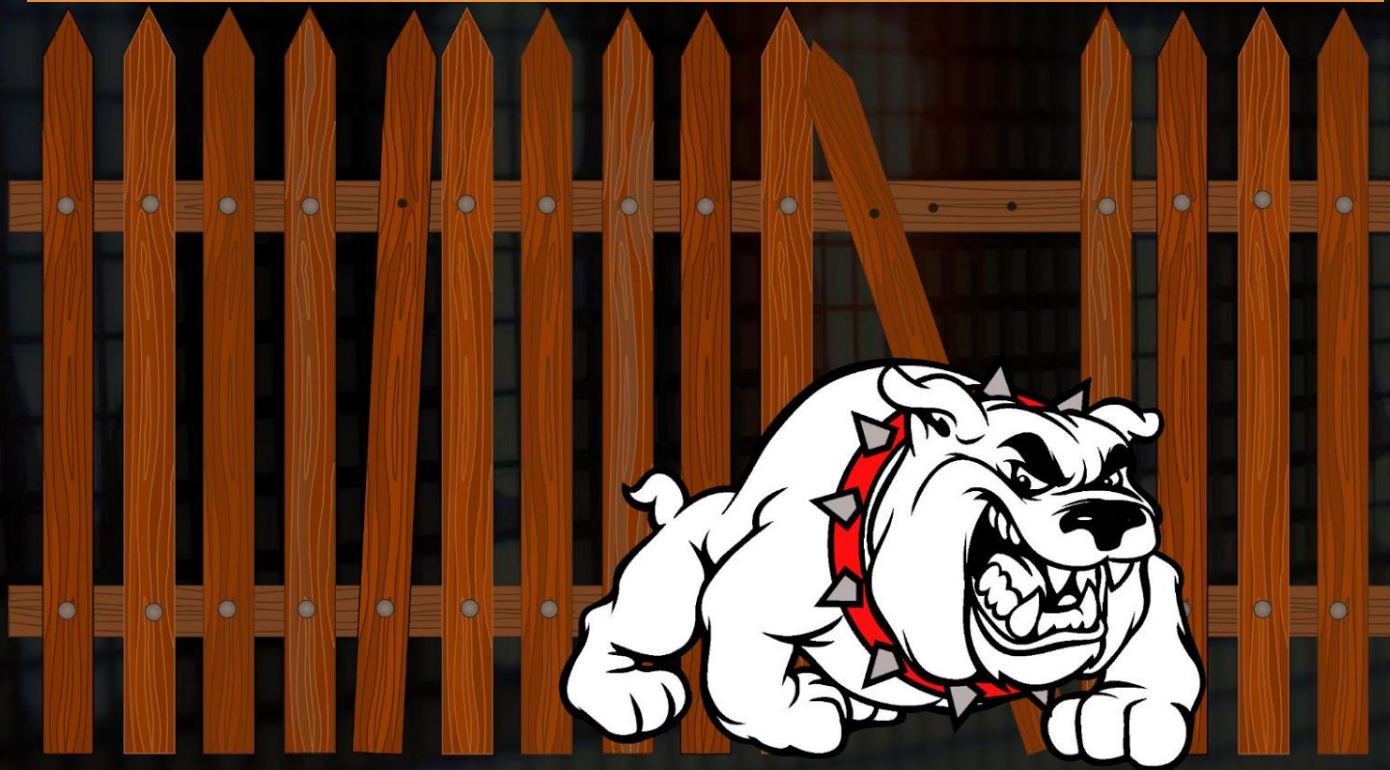
La telemetria Bitdefender conferma che, nel 27% degli attacchi, i cybercriminali ottengono l'accesso grazie configurazioni fragili degli endpoint.

Top 5 Misconfiguration risks

<https://businessinsights.bitdefender.com/top-5-endpoint-misconfigurations-that-open-security-gaps-whitepaper>

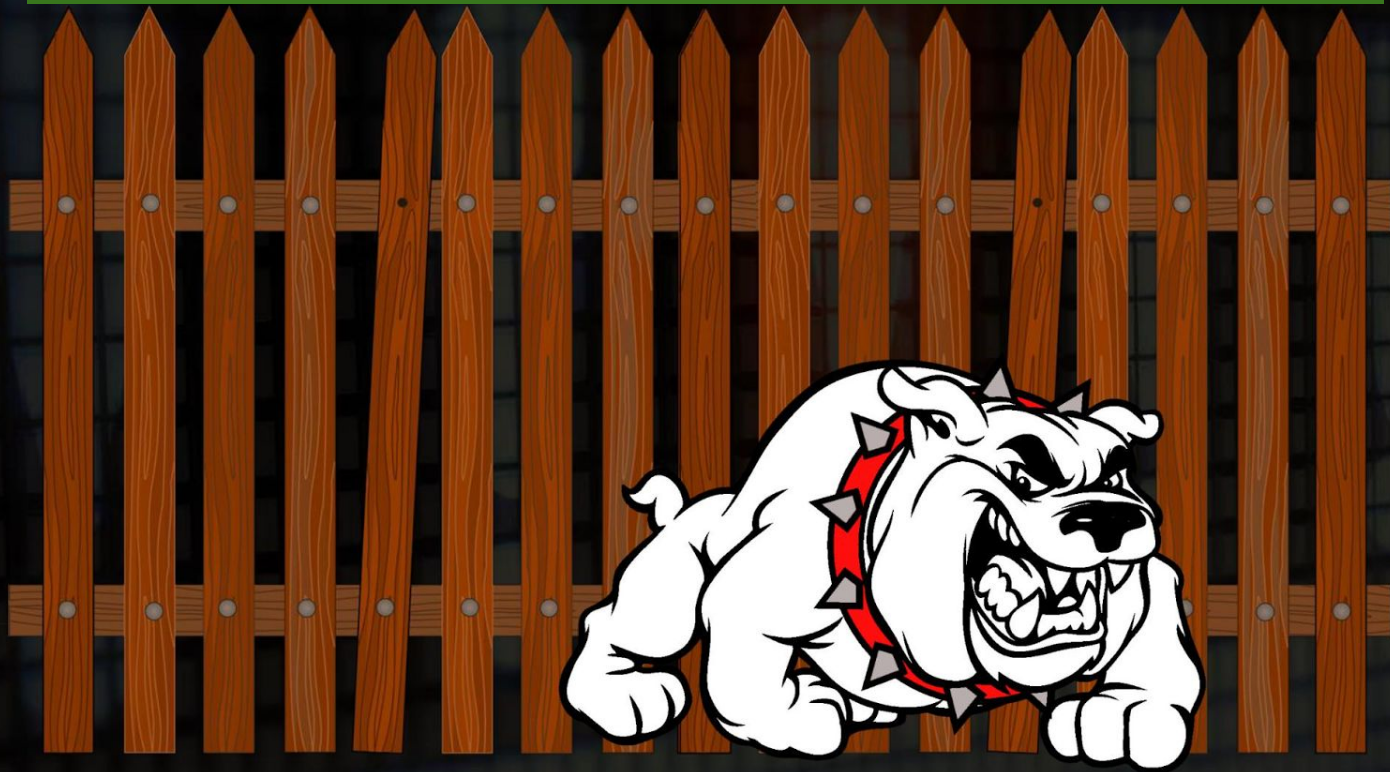
L'ANTIMALWARE NON BASTA ?

Antimalware only



L'ANTIMALWARE NON BASTA ?

Best config + Patch + Antimalware



GravityZone

Workflow del security admin

- Attività **una tantum** su **Risk Management**
- Attività **una tantum** su **Patch Management**
- Attività **periodiche** su **Risk Management**
- Attività **periodiche** su **Patch Management**

sempre incluso
richiede licenza add-on

Workflow del security admin

attività una tantum

Bitdefender

1. **Policy -> Risk Management**
pianifico la rilevazione di Misconfiguration e App Vulnerabilities
2. **Risk Management -> Dashboard**
valuto in sintesi il tasso di esposizione dell'azienda
3. **policy -> Path Management**
pianifico rilevazione ed installazione delle patch
4. **Risk Management->Dashboard**
rivaluto il tasso di esposizione dell'azienda, alla luce del patching pianificato

Workflow del security admin

Bitdefender

attività periodiche Risk Management

5. Risk Management -> Security Risks -> App Vulnerabilities

Prioritizzo le vulnerabilità software residue per gravità, le analizzo singolarmente e decido per ignorarle oppure pianificare un intervento.

6. Risk Management -> Security Risks -> Misconfigurations

Prioritizzo le misconfigurations per gravità, le analizzo singolarmente e decido se ignorarle, oppure intraprendere una azione. Dove possibile GravityZone ci assiste intervenendo, on demand, su tutti gli endpoint interessati dalla misconfiguration. In tutti i casi, ho suggerita la misura da intraprendere.

7. RiskManagement -> Dashboard

Rivaluto il tasso di esposizione dell'azienda sulla timeline. Condivido i risultati con il cliente/management.

Workflow del security admin

Bitdefender

attività periodiche Patch Management

8. **Report -> Network Patch Status**

Rilevo patch ancora da installare.

Rilevo patch con errori di installazione

9. **Patch Inventory**

Applico on demand le patch più urgenti che non possono attendere la prossima pianificazione.

10. **Troubleshooting endpoint con errori di aggiornamento**

Attività da svolgere presso gli endpoint che vedono errori, durante l'installazione di patch.

Workflow del security admin

Bitdefender

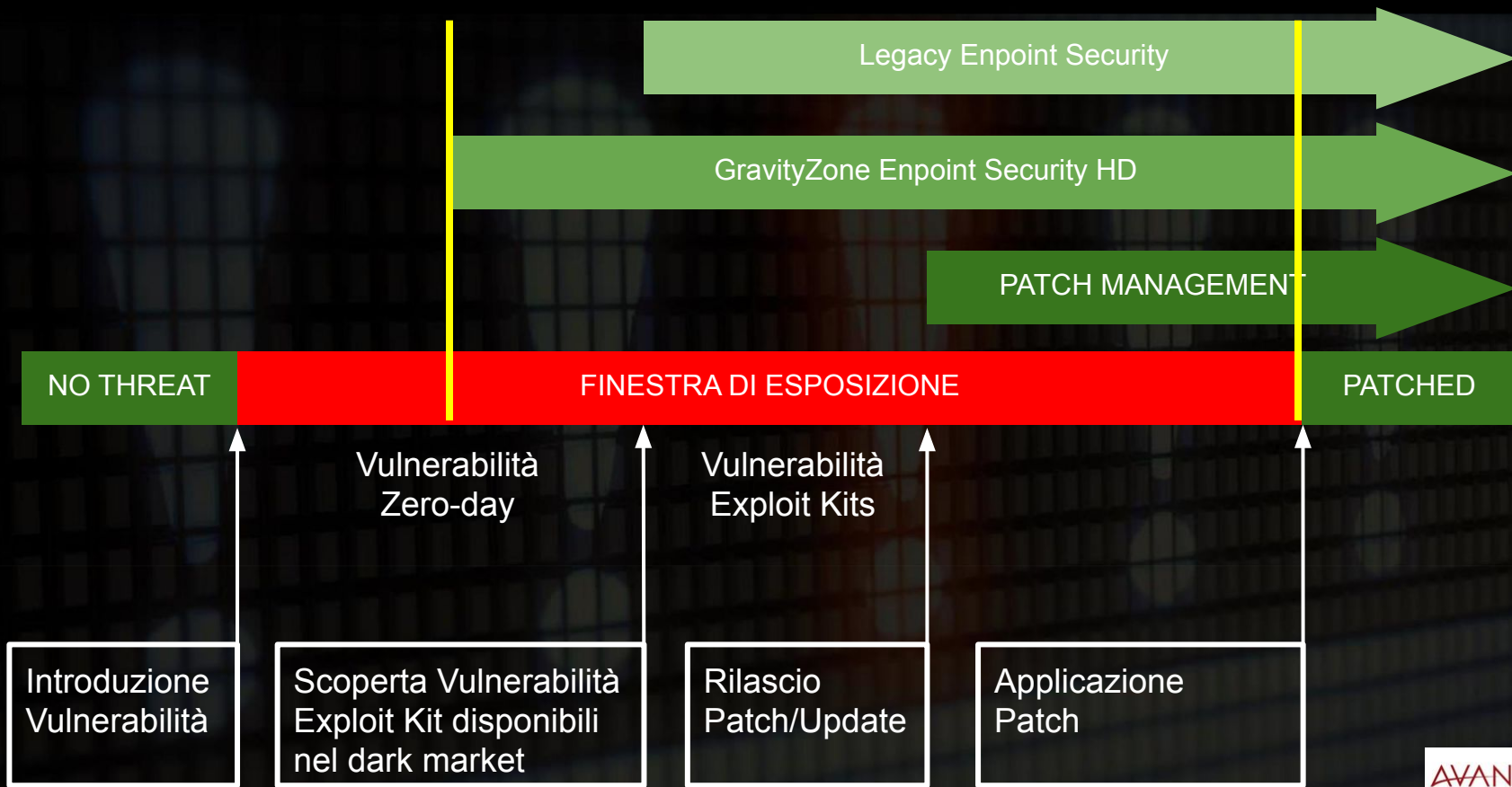
quando non posso rimuovere la vulnerabilità di una App

A fronte di un software non patchabile,
per indisponibilità della patch, o per incompatibilità con altro sw/applicazione,
si può provare ad irrobustire l'endpoint con misure di altra natura.

Es:

- proteggere l'applicazione vulnerabile,
con una configurazione mirata del **Advanced Anti-Exploit**
- ridurre l'esposizione con misure di hardening:
 - limitare l'accesso al web (Web Access Control)
 - limitare l'accesso ai dispositivi (Device Control)
 - limitare l'accesso a e dalla rete (Firewall)

VULNERABILITA' - CICLO DI VITA



PERCHE' PATCHING CON GravityZone



Interamente integrato in GravityZone, il modulo Patch Management permette alle aziende di mantenere i sistemi aggiornati su tutti i dispositivi basati su MS Windows.

GravityZone Patch Management gestisce gli aggiornamenti software per i **sistemi operativi Windows*** ed una **vastissima gamma di applicazioni***, sull'intero parco di **workstation e server, fisici e virtuali.**

*lista O.S., Vendor e applicazioni supportati:

<https://www.bitdefender.com/business/support/en/77209-79404-bitdefender-patch-management-supported-vendors-and-products.html>



Unico Agent
Unica Console

GravityZone Layered Next-Gen Endpoint Security

CARATTERISTICHE

Patching Automatico

- Scansione pianificata per patch mancanti
- Gestione differenziata per patch di sicurezza e non
- Patching automatico per una selezione di prodotti
- Rimanda il riavvio per le patch che lo richiedono

Patching OnDemand

- Task di rilevamento ed installazione patch distinti
- Report di successo/fallimento nella installazione patch

Inventario Patch

- Informazioni sulle patch: CVE, BulletinID
https://cve.mitre.org/cve/search_cve_list.html
<https://technet.microsoft.com/en-us/security/bulletins.aspx>
- Installazione on demand delle patch inventariate
- Blacklist di patch che compromettono il workflow

Report

- Stato del patching per endpoint

Notifiche

- Notifiche per mancanza di patch di sicurezza e non

Caching delle Patch

- Deduplica del traffico internet
- Accelerazione della installazione patch

Patch Management

MODELLO DI LICENZA PREPAGATO

La licenza prepagata di GravityZone Patch Management
può essere acquistata come ADD-ON
per tutte le licenze GravityZone Suite e A-La-Carte,
per il numero di dispositivi su cui intendiamo attivare il modulo Patch Management.

Patch Management

MODELLO DI LICENZA PER MSP

Il licensing mensile di GravityZone per MSP (monthly subscription),
contempla anche il servizio Patch Management

Il suo utilizzo prevede un costo specifico, per il numero di dispositivi su cui si attiva il modulo
Patch Management.

Patch Management

Requisiti software degli endpoint

- Windows 7 e successivi
- Windows Server 2008 R2 e successivi

- Linux CentOS 7
- Red Hat Enterprise Linux (RHEL) 6,7,8
- SUSE Linux Enterprise (Server 12 SP4 e Server 15)
- SUSE Linux Enterprise (Desktop 15)

Dettagli

<https://www.bitdefender.com/business/support/en/77209-146153-patch-management-for-linux.html>

TRIAL

GravityZone Cloud Console

La TRIAL che equipaggia le nuove company include Patch Management

GravityZone OnPremise Console

Chiedi una TRIAL Patch Management ad Avangate Italia

Licenza GravityZone già attiva

Chiedi una TRIAL Patch Management ad Avangate Italia

AVANGATE

ALTRE RISORSE

CONDIVISE

Sezione Documenti

Queste Slide

GravityZone Business Premium - Scheda tecnica

GravityZone Patch Management - Scheda tecnica

Sito istituzionale Avangate Italia

<https://www.avangate.it/calendario-eventi/>

[<ARCHIVIO WEBINAR>](#)

Domande

Sezione Domande: facci sapere la tua

CONTATTI

Contatti per i Partner Avangate

Login AREA PARTER

<https://nova.avangate.it>

Chat *in alto a destra* LiveSupport

Telefono *in alto a sinistra* Linea Diretta Partner

Ticket *menu Supporto* Inserisci una richiesta

Contatti pubblici

Primo contatto

<https://www.avangate.it/contattaci>

Supporto <https://supporto.s8group.it>

AVANGATE

Distributore a valore aggiunto



Roberto Novasconi

GRAZIE