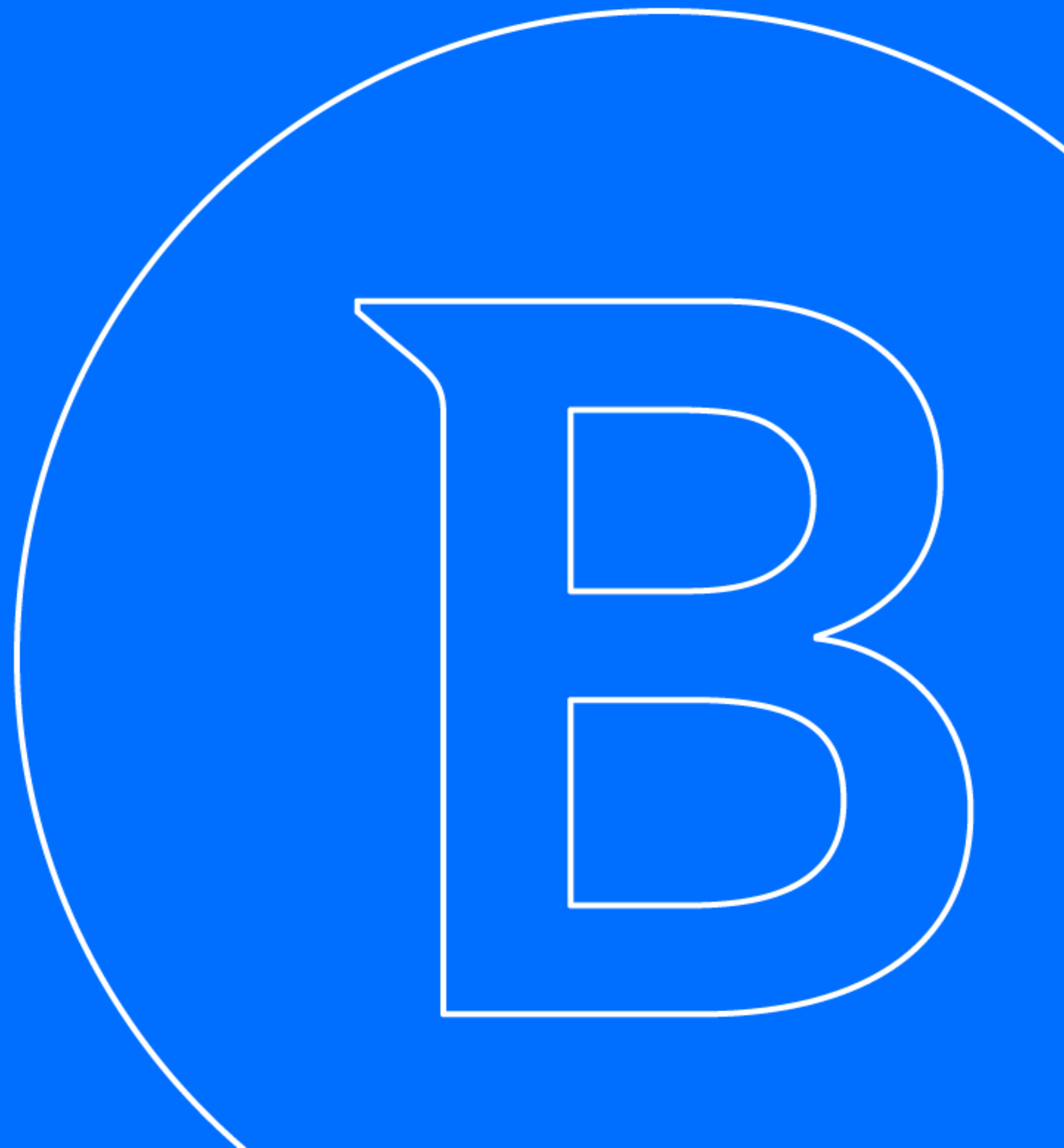


Bitdefender GravityZone

Risk Management - Analisi del
rischio e compliance
NIS2\GDPR\DORA

Cesare Vellani - PreSales - Avangate Security



Agenda

1. ERA (Endpoint Risk Analytics): scenario e certezze
2. I pilastri della sicurezza Bitdefender
3. Normative: da GDPR a NIS2 e DORA
4. Perché un'organizzazione ha bisogno di una soluzione come ERA
5. Requisiti critici della sicurezza degli endpoint
6. Cosa può fare realmente per l'azienda Bitdefender ERA
7. In pratica...



ERA: scenario e certezze

Il rischio informatico è la combinazione di **probabilità** e **impatto** di una perdita di dati o di un danno operativo a causa di incidenti di sicurezza

Certezza 1 -> I moderni criminali informatici hanno **innumerevoli opportunità** per violare con successo i sistemi informativi aziendali: vulnerabilità OS\app e configurazioni errate su tutte.

Certezza 2 -> Rafforzando le difese, le organizzazioni possono

- **ridurre la probabilità** di una futura violazione.
- **ridurre i premi assicurativi** delle cosiddette “cyber-assicurazioni”
- **ridurre il** rischio di sanzioni normative



I pilastri della sicurezza Bitdefender

LE NOSTRE AREE DI INTERVENTO

Prevenzione

Controlli proattivi per **limitare la superficie di attacco**.



CONTROLLO
DISPOSITIVO



GESTIONE
DELLE PATCH



GESTIONE DEL
RISCHIO DEGLI
ENDPOINT E DEGLI
UTENTI



CONTROLLO
APPLICAZIONE



CRITTOGRAFIA
DELL'INTERO
DISCO



CONTROLLO E
FILTRAGGIO DEL WEB E
DEI CONTENUTI

Rilevamento

Strumenti avanzati per **rilevare le minacce**.



TUNABLE MACHINE
LEARNING



DIFESA DAGLI
ATTACCHI FILELESS



MITIGAZIONE
RANSOMWARE



PROTEZIONE
DEL PROCESSO



DIFESA DAGLI
EXPLOIT



DIFESA DAGLI
ATTACCHI DI RETE

Risposta

Utilizzo di **risposte contestuali** nell'incidente identificato.



EXTENDED
DETECTION AND
RESPONSE



VISUALIZZAZIONE
DEGLI INCIDENTI



DIFESA DALLE
ANOMALIE



INCIDENT
ADVISOR



RISPOSTA
GUIDATA



RICERCA IN
DIRETTA

Normative

GDPR

Cercava di migliorare gli standard di privacy e sicurezza a livello dei dati degli utenti.

NIS2 (Network Information & Security)

Cerca di migliorare gli standard di privacy, gestione del rischio e sicurezza per le aziende e le organizzazioni nel loro insieme.

DORA (Digital Operational Resilience Act)

Vuole creare un quadro normativo vincolante e uniforme per la gestione del rischio tecnologico e delle comunicazioni ICT nel settore finanziario.



Normative – NIS2 (18/10/2024)

Secondo l'articolo 21, gli Stati Membri devono assicurare **che le entità importanti e quelle essenziali prendano le adeguate e proporzionate misure tecniche, operative e organizzative per gestire i rischi relativi alla sicurezza della rete e ai sistemi informativi utilizzati per le loro operazioni o per erogare i loro servizi, per prevenire o minimizzare l'impatto degli incidenti sui destinatari dei loro servizi e su altri servizi**. Queste misure dovrebbero essere basate su un **approccio che consideri tutti i rischi** con lo scopo di proteggere i sistemi di rete e informativi, l'ambiente in cui operano tali sistemi e infine dovrebbe includere almeno i seguenti punti:

- Policy sull'analisi del rischio e sulla sicurezza dei sistemi informativi;
- Gestione degli incidenti;
- Continuità operativa, come gestione dei backup, disaster recovery e gestione delle crisi;
- Sicurezza della supply chain, tra cui aspetti legati alla sicurezza riguardanti il rapporto tra ogni entità e i suoi fornitori diretti o service provider;
- Sicurezza nell'acquisto, nello sviluppo e manutenzione dei sistemi di rete e informativi, inclusa la gestione e la comunicazione della vulnerabilità;
- Regole e procedure per valutare l'efficacia delle misure di sicurezza informatica relative alla gestione dei rischi;

- Pratiche di "igiene informatica" di base e formazione sul tema della sicurezza informatica;
- Policy e procedure riguardanti l'uso della crittografia e, laddove necessaria, encryption;
- Sicurezza delle risorse umane, policy di controllo degli accessi e gestione degli asset; laddove opportuno, autenticazione multi fattore o soluzioni di autenticazione continua; comunicazioni vocali, scritte e video protette; sistemi di comunicazione di emergenza protetti all'interno dell'ente.

Normative – NIS2 – Soggetti interessati

A quali realtà si applica la NIS2?

- Tutte le aziende che rientrano nelle definizioni di “**Entità importanti**” o “**Entità Essenziali**”. Vi rientrano aziende di **tutti i settori**, con dimensioni da **>50 addetti/10M** bilancio e **250 addetti/50M** bilancio rispettivamente.
- Rientrano anche aziende con numeri inferiori, se si tratta di un “fornitore unico” fondamentale dal punto di vista sociale o economico per i paesi membri UE.

Sebbene siano ancora previste modifiche a NIS2, riteniamo che NIS2 possa applicarsi a qualsiasi azienda che operi all'interno dell'UE.

Normative – NIS2 – Soggetti interessati

Settori ad alta criticità (Soggetti essenziali)



Altri settori critici (Soggetti importanti)



Normative – DORA (17/01/2025)

- Cos'è DORA?
- Quali sono le caratteristiche salienti di DORA?
 - DORA introduce **standard tecnici**
 - DORA **armonizza**
 - **A chi** si applica DORA?



Normative – NIS2 e DORA – Differenze

	NIS2	DORA
OBIETTIVO	SICUREZZA INFORMATICA	SICUREZZA INFORMATICA
APPROCCIO	DIRETTIVA	REGOLAMENTO
AMBITI DI APPLICAZIONE	VARI SETTORI CRITICI	SETTORE FINANZIARIO

Normative – NIS2 e DORA – Cosa si deve fare?

Inventario - Creare un inventario completo di tutti gli asset IT

Igiene informatica - Migliorare le pratiche della cosiddetta “igiene informatica” e la consapevolezza dei dipendenti

Gestione delle vulnerabilità - Implementare una gestione efficace delle vulnerabilità

Incident detect and response - Sviluppare un sistema di rilevamento e risposta agli incidenti

Gestione del rischio - Integrare procedure di gestione del rischio nei processi aziendali

Perché un'organizzazione ha bisogno di una soluzione come Endpoint Risk Analytics?

NON SI PUÒ CORREGGERE CIÒ CHE NON SI VEDE

L'esfiltrazione dei dati è un **obiettivo chiave** dei criminali informatici che può portare a tattiche di estorsione.

Gli incidenti di sicurezza sono **spesso** causati da:

- Mancata osservanza **delle “best practices”**
- Mancata **applicazione** degli aggiornamenti in modo tempestivo
- Errore\fattore **umano**



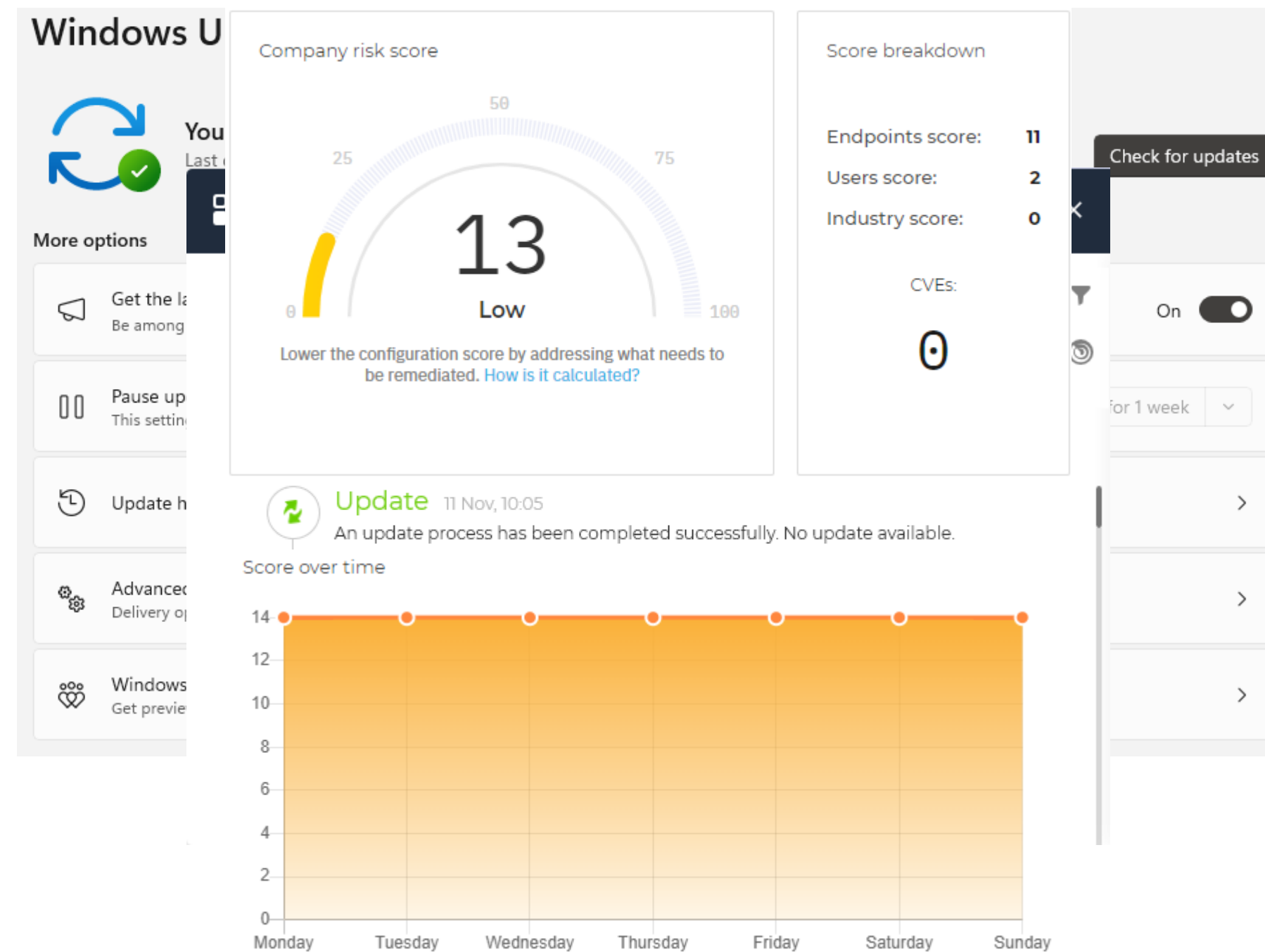
Requisiti critici della sicurezza degli endpoint

CREARE COMPRENSIONE

Per proteggere l'organizzazione, è necessario comprendere la **superficie di attacco**.

Endpoint Hardening: è un processo di riduzione della superficie di attacco dell'endpoint attraverso:

- Hardening del **sistema operativo**
- Hardening delle **applicazioni**
- **Analisi dettagliata** degli endpoint



Cosa può fare realmente per me Bitdefender ERA?

La console Bitdefender GravityZone **fornisce alle organizzazioni gli strumenti** per affrontare i rischi.

Bitdefender ERA può **aiutare le organizzazioni** con:

- Identificazione del rischio
- Valutazione del rischio
- Priorità del rischio
- Scansioni del rischio
- Azioni di riparazione

The screenshot displays the Bitdefender GravityZone console interface. At the top, there are filters for 'All misconfigurations', 'FIX RISKS', 'STATE', 'WATCHLIST', and 'SCAN'. Below these are dropdown menus for 'Misconfiguration name', 'Risk score', 'Device name', and 'Misconfiguration type'. The main table lists various misconfigurations, with 'Encryption Support' highlighted. To the right, a detailed view of the 'Encryption Support' risk is shown, including its status, state, OS, mitigation type, compliance, and watchlist status. Below this, the 'DETAILS' section explains the policy setting and its impact. At the bottom, the 'RISK MITIGATION' section provides instructions on how to set the policy to 'Enabled: Use TLS 1.1; Use TLS 1.2'.

Misconfiguration name	Risk score ↓	Affected devices	OS	Misconfiguration type	Mitigation
☒ Encryption Support	High (98%)	10 17	Windows	Browser	Automatic
☐ Server Certificate Revocation	High (98%)	10 17	Windows	Browser	Automatic
☐ WinRM Service RunAs Credentials	High (98%)	10 17	Windows	OS	Automatic
☐ Windows Ink Workspace	High (98%)	10 17	Windows	OS	Automatic
☐ Boot-Start Driver	High (98%)	10 17	Windows	OS	Automatic
☐ Client Digitally Sign Communications	High (98%)	10 17	Windows	Network	Automatic
☐ Credential Delegation	High (98%)	10 17	Windows	Network	Automatic
☐ Security Zones Change Policies	High (98%)	10 17	Windows	Browser	Automatic
☐ Run Software if Signature Invalid	High (98%)	10 17	Windows	Browser	Automatic
☐ WinRM Client Digest Authentication	High (98%)	10 17	Windows	OS	Automatic
☐ Anti-Spoofing	High (98%)	10 17	Windows	OS	Automatic
☐ ActiveX Protected Mode	High (98%)	10 17	Windows	Browser	Automatic
☐ Download Enclosures	High (98%)	10 17	Windows	OS	Automatic
☐ Internet Explorer: Turn on Protected...	High (98%)	10 17	Windows	Browser	Automatic
☐ Security Zones Only Machine Settings	High (98%)	10 17	Windows	Browser	Automatic
☐ Downloaded Programs Signatures	High (98%)	10 17	Windows	Browser	Automatic
☐ Install ActiveX	High (98%)	10 17	Windows	Browser	Automatic

Encryption Support

GENERAL

Misconfiguration type: Browser

Risk score: High (98%)

Status: Detected

State: Active

OS: Windows

Mitigation type: Automatic

Compliance: CISv8

In watchlist: No

[View devices](#) [Add to watchlist](#)

DETAILS

Verifies the local group policy **Turn off encryption support**, located in **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Page**. This policy setting allows you to turn off support for Transport Layer Security (TLS) 1.0, TLS 1.1, TLS 1.2, Secure Sockets Layer (SSL) 2.0, or SSL 3.0 in the browser. TLS and SSL are protocols that help protect communication between the browser and the target server. When the browser attempts to set up a protected communication with the target server, the browser and server negotiate which protocol and version to use. The browser and server attempt to match each other's list of supported protocols and versions and they select the most preferred match.

- If you enable this policy setting, the browser negotiates or does not negotiate an encryption tunnel by using the encryption methods you select from the drop-down list.

Compliance: CISv8

Data Protection: [Encrypt Sensitive Data in Tra...](#)

RISK MITIGATION

Set this policy to **Enabled: Use TLS 1.1; Use TLS 1.2**

[Fix risk](#) [Ignore risk](#)

Identificazione del rischio

QUALI RISCHI SONO PRESENTI NELLA MIA ORGANIZZAZIONE?



L'identificazione dei rischi è il primo passo per affrontare i problemi.



Una scansione dei rischi popola il cruscotto, fornendo consapevolezza dei rischi elencati.



Fornisce visibilità alle configurazioni insicure e alle vulnerabilità.

All misconfigurations*

FIX RISKS

STATE

WATCHLIST

SCAN

Misconfiguration name

Risk score

Device name

Misconfiguration t

All

100 - 0

All

All

☐ Misconfiguration name

☐ Internet Explorer: Allow cut, copy or paste operations from the clipboard via script (Internet Zone)

☐ Internet Explorer: Include local path when user is uploading files to a server (Internet Zone)

☐ Server Certificate Revocation

☐ Downloaded Programs Signatures

☐ Internet Explorer: Run .NET Framework-reliant components not signed with Authenticode (Internet Zone)

☐ Certificate Address Mismatch Warning

☐ Internet Explorer: Launching applications and files in an IFRAME (Internet Zone)

☐ Boot-Start Driver

☐ Internet Explorer: Allow scriptlets (Internet Zone)

☐ Security Zones Change Policies

☐ Windows Ink Workspace

☐ Internet Explorer: Web sites in less privileged Web content zones can navigate into this zone (Internet Zone)

☐ Internet Explorer: Allow scripting of Internet Explorer WebBrowser controls (Internet Zone)

☐ Internet Explorer: Logon options (Internet Zone)

☐ Internet Explorer: Allow loading of XAML files (Restricted Sites Zone)

☐ Internet Explorer: Allow drag and drop or copy and paste files (Restricted Sites Zone)

Valutazione del rischio

FORNIRE INFORMAZIONI SUI RISCHI



Fornisce automaticamente informazioni per comprendere l'impatto organizzativo.



I rischi evidenziati nella dashboard possono essere di tipo utente o endpoint.



Alcuni settori sono obbligati per legge a condurre periodicamente un'analisi dei rischi.

DETAILS

Verifies the local group policy **Web sites in less privileged Web content zones can navigate into this zone**, located in **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone**.

This setting allows managing whether Web sites from less privileged zones, such as Restricted Sites, can navigate into this zone.

- If you enable this setting, websites from less privileged zones can open new windows in or navigate into this zone. The security zone will run without the added layer of security provided by the Protection from Zone Elevation security feature.
- If you select **Prompt** in the drop-down box, a warning is issued to the user that potentially risky navigation is about to occur.
- If you disable this setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by the Protection from Zone Elevation feature control.
- If you do not configure this setting, websites from less privileged zones can open new windows in or navigate into this zone.

Compliance

CISV8

Email and Web Brows...

[Ensure Use of Only Fully Sup...](#)

Priorità al rischio

DA DOVE INIZIARE?



I rischi identificati e le informazioni contestuali consentono di definire le priorità dei rischi.



La dashboard Risk Management assegnerà automaticamente la priorità fornendo un punteggio di rischio.



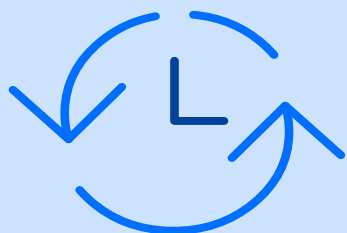
La definizione delle priorità dei rischi può consentire ai team di sicurezza di coordinare un piano per risolvere i rischi identificati.

☐ Misconfiguration name	Risk score ↓	Affected devices
☐ Internet Explorer: Allow cut, copy or...	● High (100%)	10 17
☐ Internet Explorer: Include local path...	● High (100%)	10 17
☐ Server Certificate Revocation	● High (100%)	10 17
☐ Downloaded Programs Signatures	● High (100%)	10 17
☐ Internet Explorer: Run .NET Framew...	● High (100%)	10 17

☐ Application name	Risk score ↓	CVEs	Affected devices
☐ webkitgtk4 2.28.2-2.el7	● High (100%)	17	1
☐ webkitgtk3 2.4.11-2.el7	● High (100%)	19	1
☐ firefox 68.10.0-1.el7.centos	● High (100%)	15	1
☐ firefox 115.6.0-1.el8	● High (100%)	16	1
☐ coreutils 8.22-24.el7	● High (100%)	2	1

Scansioni del rischio

VOGLIO ESSERE AGGIORNATO



La gestione del rischio all'interno dell'organizzazione non è un'azione una tantum: un piano di gestione del rischio efficace **verifica costantemente la presenza di nuovi rischi.**



Garantire **la sicurezza** degli endpoint **in tutte le fasi del ciclo di vita delle risorse.**



Scoprire **nuovi rischi** o **vulnerabilità** nella rete organizzativa.

☒ Risk Management

Enables recurrent risk scanning on target endpoints. This means you can schedule scanning for security risks, such as Automatic Updates or User Access Control settings.

[Read the full description of indicators of risk and the available fix actions.](#)

SCHEDULER

Start date and time:

14 Nov 2024



10

:

00

Recurrence

☐ Schedule task to run once every:

1

days

☒ Run task every:

Sun

Mon

Tue

Wed

Thu

Fri

Sat

☒ If scheduled run time is missed, run task as soon as possible

Azioni di riparazione

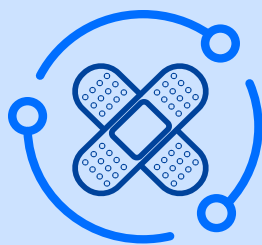
RIDURRE ATTIVAMENTE IL RISCHIO



Ora che i rischi sono stati **identificati e classificati**, possiamo risolverli.



La console GravityZone può **risolvere i rischi in remoto** apportando modifiche al registro di Sistema (NEWS: **Rollback disponibile!**).



Per risolvere alcuni rischi può essere necessario applicare patch al sistema operativo o alle applicazioni, il che richiede **l'acquisto del modulo Patch Management**.

RISK MITIGATION

Set this policy to **Enabled**.

[Fix risk](#) [Ignore risk](#)

RISK MITIGATION

Apply all patches for webkitgtk4 2.28.2-2.el7 to mitigate 17 known vulnerabilities affecting your endpoints.

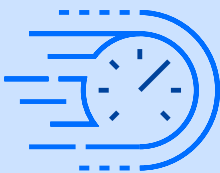
[Patch app](#) [Ignore application](#)

Sintesi

AFFRONTARE IN MODO PROATTIVO I RISCHI DI SICUREZZA



Bitdefender GravityZone fornisce potenti strumenti per **identificare le vulnerabilità della sicurezza** nelle loro organizzazioni.



La gestione dei rischi consente ai team di sicurezza di **riconoscere i rischi ad alta priorità** che devono affrontare per primi.



Un solido strumento di prevenzione può far **risparmiare tempo e risorse** e potenzialmente mitigare un disastroso attacco informatico.

All misconfigurations

FIX RISKS

STATE

WATCHLIST

SCAN

Misconfiguration name

All

Risk score

100 - 0

Device name

All

Misconfiguration type

All

Misconfiguration name	Risk score ↓	Affected devices	OS	Misconfiguration type	Mitigation
☒ Encryption Support	High (98%)	10 17	Windows	Browser	Automatic
☐ Server Certificate Revocation	High (98%)	10 17	Windows	Browser	Automatic
☐ WinRM Service RunAs Credentials	High (98%)	10 17	Windows	OS	Automatic
☐ Windows Ink Workspace	High (98%)	10 17	Windows	OS	Automatic
☐ Boot-Start Driver	High (98%)	10 17	Windows	OS	Automatic
☐ Client Digitally Sign Communications	High (98%)	10 17	Windows	Network	Automatic
☐ Credential Delegation	High (98%)	10 17	Windows	Network	Automatic
☐ Security Zones Change Policies	High (98%)	10 17	Windows	Browser	Automatic
☐ Run Software if Signature Invalid	High (98%)	10 17	Windows	Browser	Automatic
☐ WinRM Client Digest Authentication	High (98%)	10 17	Windows	OS	Automatic
☐ Anti-Spoofing	High (98%)	10 17	Windows	OS	Automatic
☐ ActiveX Protected Mode	High (98%)	10 17	Windows	Browser	Automatic
☐ Download Enclosures	High (98%)	10 17	Windows	OS	Automatic
☐ Internet Explorer: Turn on Protected...	High (98%)	10 17	Windows	Browser	Automatic
☐ Security Zones Only Machine Settings	High (98%)	10 17	Windows	Browser	Automatic
☐ Downloaded Programs Signatures	High (98%)	10 17	Windows	Browser	Automatic
☐ Install ActiveX	High (98%)	10 17	Windows	Browser	Automatic

Encryption Support

GENERAL

Misconfiguration type

Browser

Risk score

High (98%)

Status

Detected

State

Active

OS

Windows

Mitigation type

Automatic

Compliance

CISv8

In watchlist

No

View devices

Add to watchlist

DETAILS

Verifies the local group policy **Turn off encryption support**, located in **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Page...** This policy setting allows you to turn off support for Transport Layer Security (TLS) 1.0, TLS 1.1, TLS 1.2, Secure Sockets Layer (SSL) 2.0, or SSL 3.0 in the browser. TLS and SSL are protocols that help protect communication between the browser and the target server. When the browser attempts to set up a protected communication with the target server, the browser and server negotiate which protocol and version to use. The browser and server attempt to match each other's list of supported protocols and versions and they select the most preferred match. - If you enable this policy setting, the browser negotiates or does not negotiate an encryption tunnel by using the encryption methods you select from the drop-down list.

Compliance

CISv8

Data Protection

Encrypt Sensitive Data in Tra...

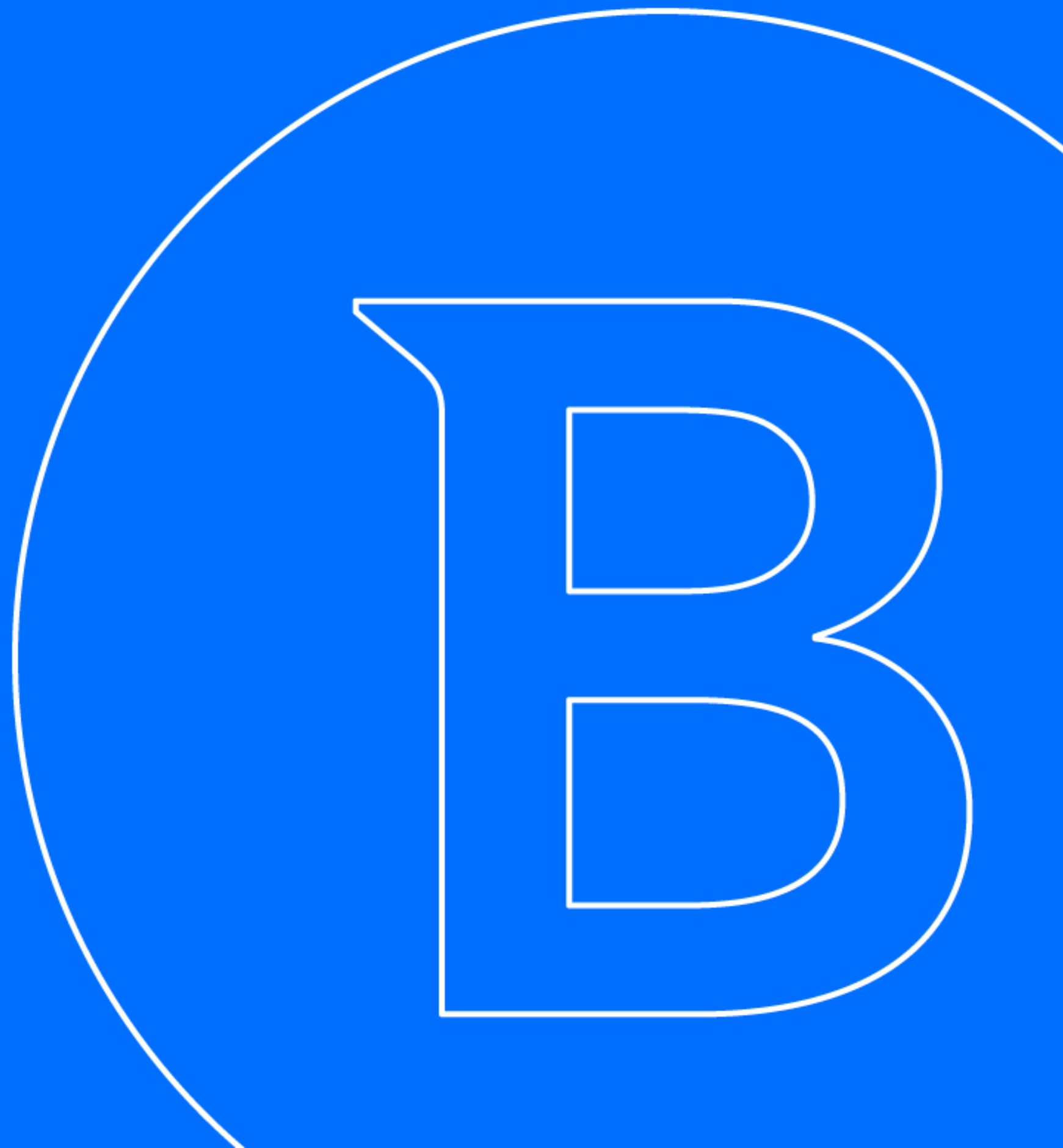
RISK MITIGATION

Set this policy to **Enabled: Use TLS 1.1; Use TLS 1.2**

Fix risk

Ignore risk

In pratica...



Agenda

- Ultime novità
- Procedura di implementazione
- Panoramica in console GZ Cloud
- Prossimo futuro (EA): Compliance, EASM, PHASR

Ultime novità

- **Settembre 2024:** The Risk Management feature has been completely redesigned and restructured
- **Novembre 2024:** The Risk Management feature has been redesigned and several pages have been renamed for better cross feature uniformity:

The Misconfigurations page is now called Findings.

The User behavior risks page is now called Identity risks.

The Devices page is now called Resources.

The Users page is now called Identities.

⚡ Risk management	⚡ Gestione dei rischi
Findings	Riscontri
Vulnerabilities	Vulnerabilità
Identity risks	Rischi per l'identità
Resources	Risorse
Identities	Identità
Companies view	Visuale aziende

- **Novembre 2024:** The Roll back fix option is now available, allowing you to revert fixes applied for findings and resources.
- **Novembre 2024:** The Compliance feature is available for Early Access (EA).
- **Febbraio 2025:** Compliance (still in EA) - A new compliance report is now available for the Risk Analytics feature: Digital Operational Resilience Act (DORA).

Procedura di implementazione

ERA (**disponibile solo per GZ Cloud Console**) raccoglie e analizza i dati attraverso attività di scansione dei rischi eseguite su dispositivi selezionati nella rete.

ERA è gratuito, a prescindere dalla modalità di licenziamento

1. Accedere a GravityZone Control Center e andare alla pagina **Policy** dal menu a sinistra.
2. Scorrere fino alla policy **Gestione dei rischi** e selezionarla.
3. Selezionare la casella di controllo per abilitare le funzioni di **Risk Management** e iniziare a configurare le policy che definiscono come eseguire l'attività di **Risk Scan**.

Successivamente, seguire questi passaggi per eseguire le attività di risk scan:

1. Eseguire un risk scan sugli endpoint. È possibile farlo utilizzando uno di questi metodi:
 - 1. Su richiesta:** selezionando gli endpoint dalla pagina **Rete** e inviando un'attività di **scansione dei rischi** dal menu.
Nota: affinché la scansione dei rischi venga eseguita su un endpoint, è necessario che su di esso sia applicato un criterio che abbia abilitata la funzione **Gestione dei rischi**.
 - 2. Su programmazione:** configurando un'attività di scansione dei rischi dalla policy che viene eseguita automaticamente sugli endpoint di destinazione a intervalli definiti.

Prossimo futuro (attualmente in EA)

- Compliance
- EASM (External Attack Surface Management)
- PHASR (Proactive Hardening and Attack Surface Reduction)



Thank you

