



Check Point

# Harmony

## Secure Users & Access

### **Harmony Browse**

### **Implementando Políticas de Controle de Conteúdo**

Autor: Lorena Freitas  
Security Engineering Brazil  
Jun/24

## Implementando Políticas de Controle de Conteúdo no Harmony Browse

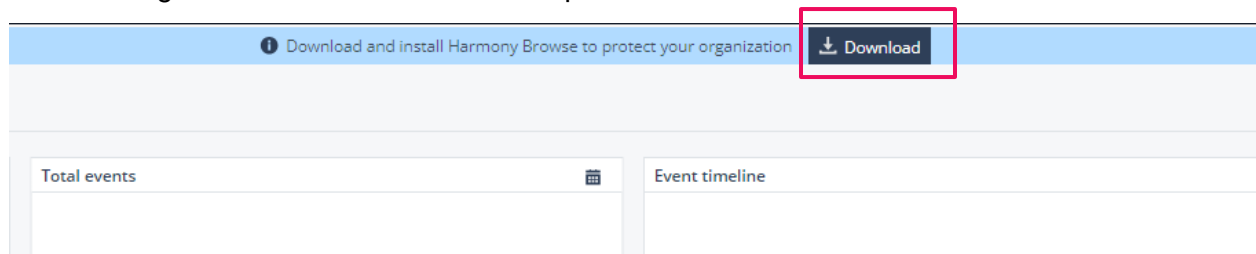
O Harmony Browse é uma solução capaz de proteger as organizações e seus funcionários contra ameaças baseadas na Web usando apenas uma extensão de navegador. A solução evita que os usuários visitem sites de phishing, baixem malware de dia zero, acessem sites indevidos e reutilizem senhas corporativas em contas pessoais.

Ao contrário dos web gateways tradicionais, o Harmony Browse oferece acesso rápido e privado à web sem redirecionar e descriptografar o tráfego SSL na nuvem ou através de dispositivo local, garantindo que não seja adicionada latência à navegação além da privacidade dos acessos.

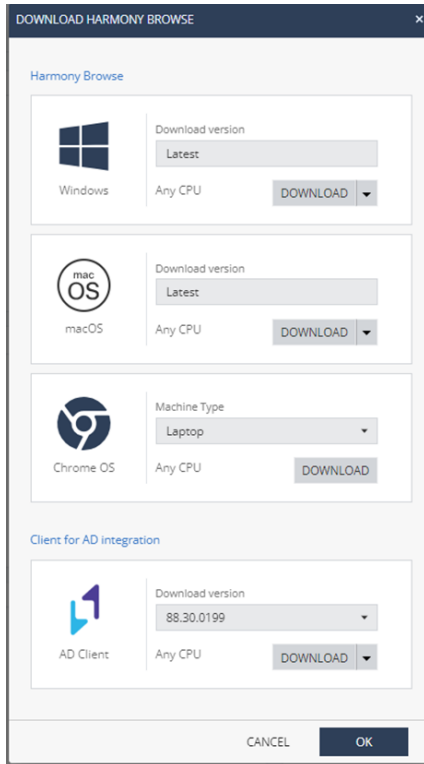
Para este tutorial foram utilizados os seguintes elementos:

- Portal Infinity com licenciamento válido para o Harmony Browse;
- Desktop de usuário com Windows 11;
- Agente Harmony Browse versão 90.09.0031 (instalado no desktop de usuário);

Com a licença do Harmony Browse devidamente habilitada no Portal Infinity, temos o botão de *Download* do agente a ser instalado no desktop do usuário.

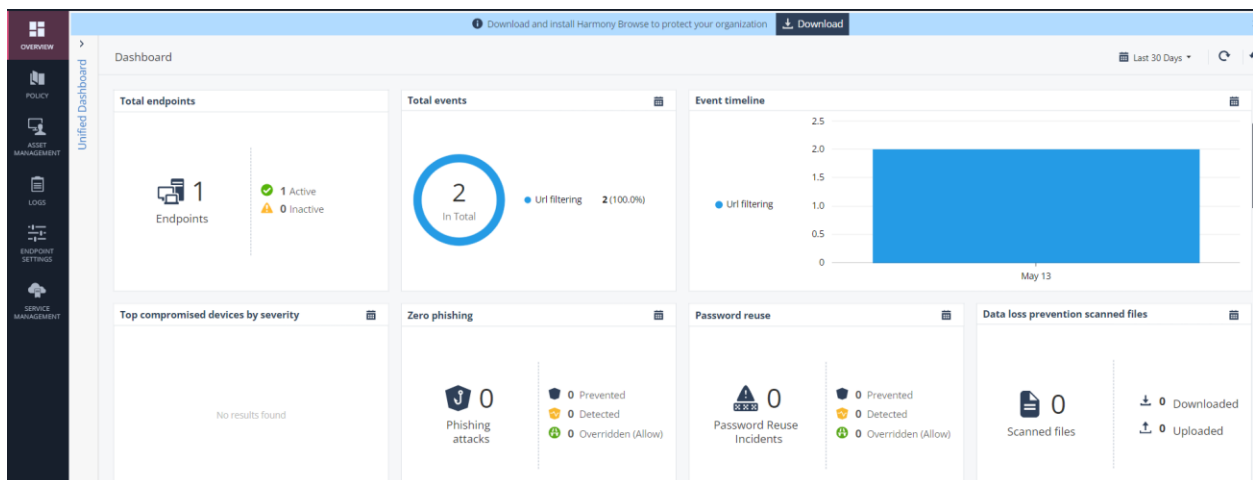


Clicando em *Download* é possível escolher a versão a ser utilizada.

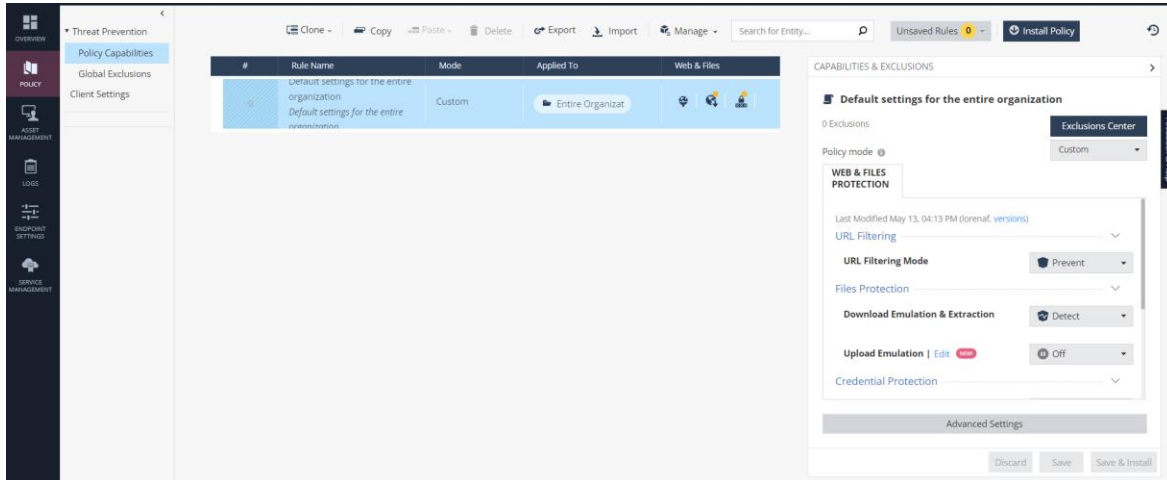


A figura abaixo mostra o menu *Overview* do Harmony Browse, após a instalação do agente concluída.

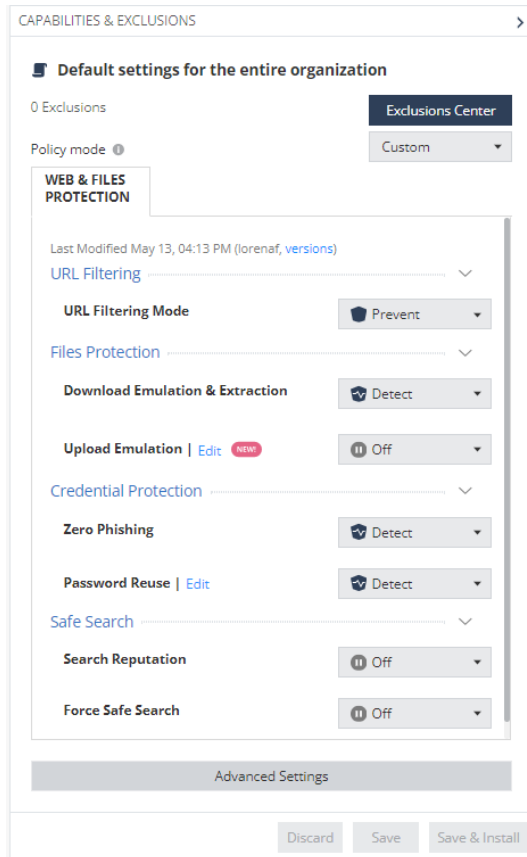
Mais detalhes em: [https://sc1.checkpoint.com/documents/Infinity\\_Portal/WebAdminGuides/EN/Harmony-Browse-Admin-Guide/Topics-HB/Introduction.htm](https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/Harmony-Browse-Admin-Guide/Topics-HB/Introduction.htm)



Para configurar o controle de conteúdo, vamos acessar o menu *Policy > Threat Prevention > Policy Capabilities*, conforme abaixo:



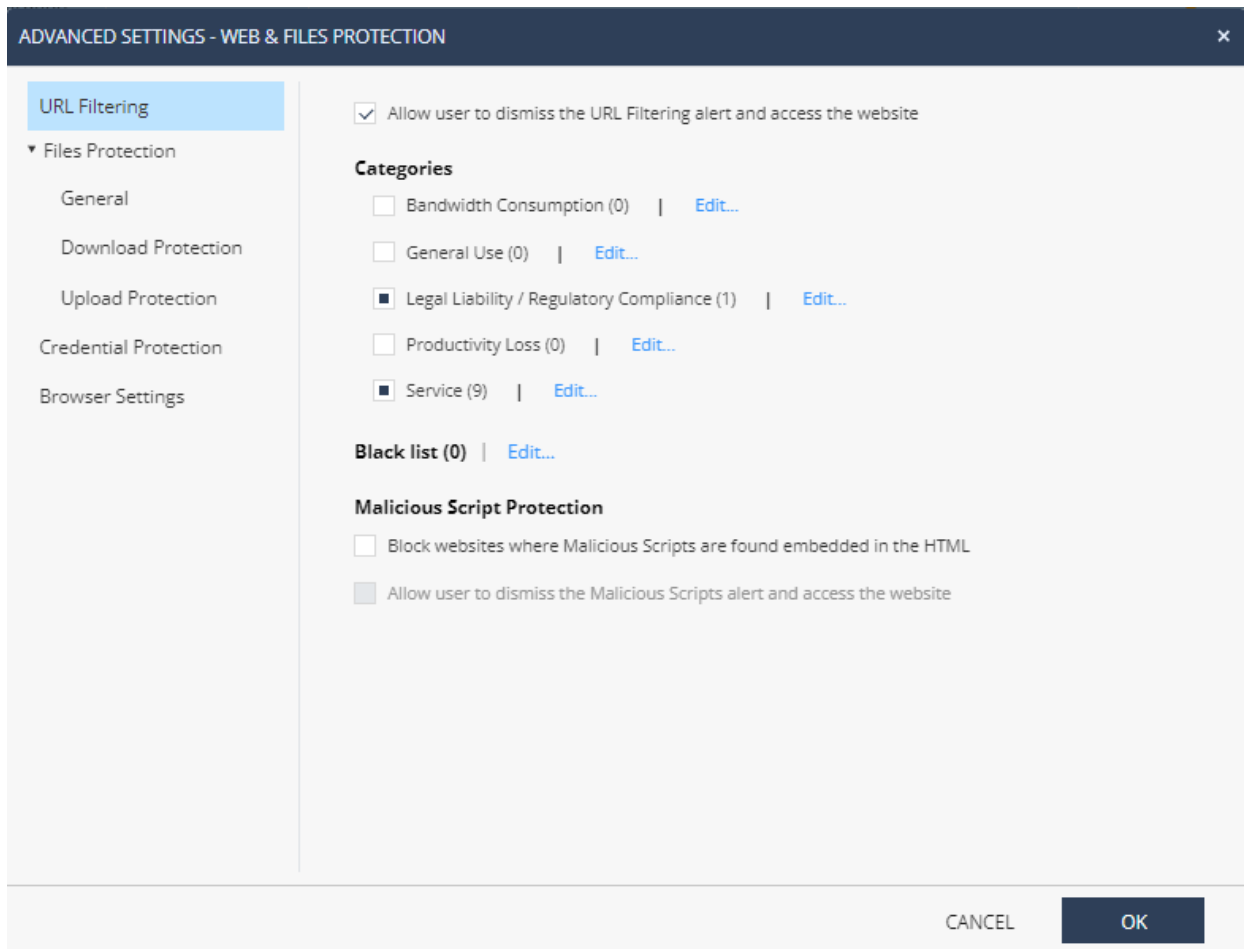
Acessar, então, a aba *Web & Files Protection* no menu *Capabilities & Exclusions* à direita.



Neste menu, é possível configurar as políticas de controle de conteúdo, controle de download e upload de arquivos; proteção contra acesso a páginas de phishing e reuso de senhas corporativas. E também controle de navegação através do Safe Search.

Ao acessar *Advanced Settings > URL Filtering* temos um menu com as categorias de URL's, que pode ser editado de acordo com as políticas de acesso da organização.

Marcar a primeira caixa de seleção, permite que o usuário acesse o website mediante uma justificativa.

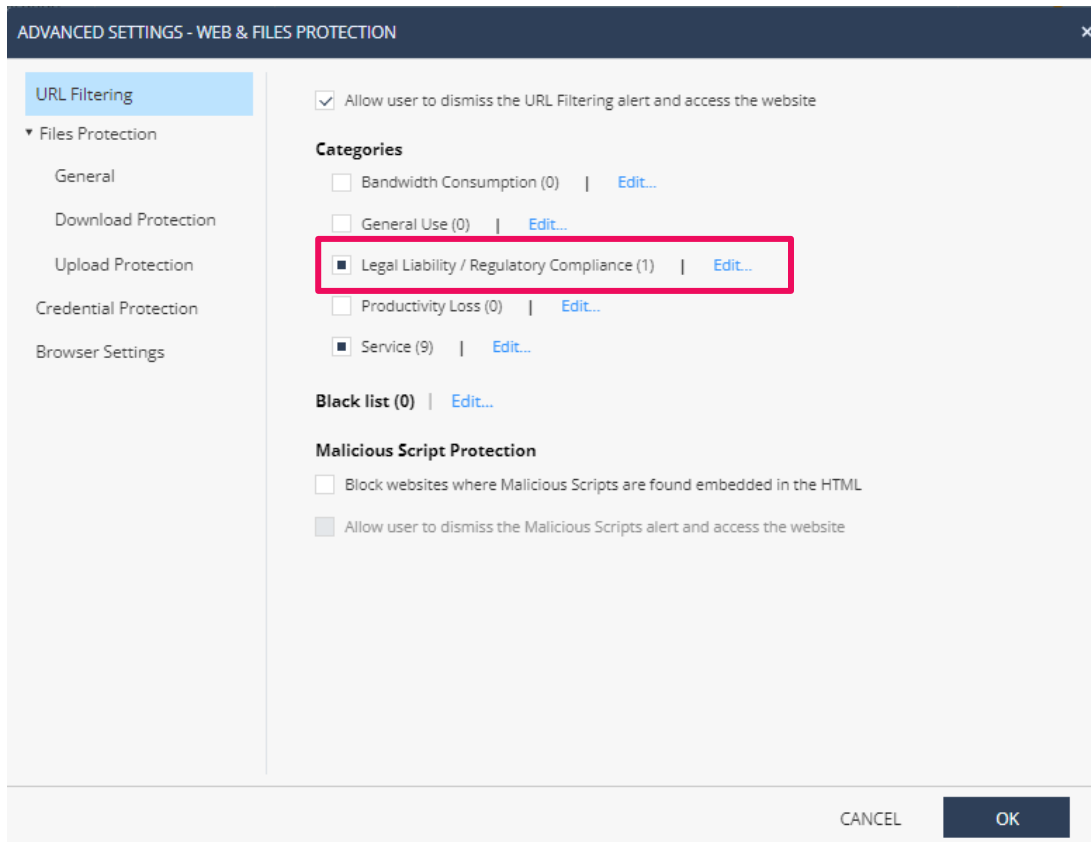


The screenshot shows a window titled "ADVANCED SETTINGS - WEB & FILES PROTECTION" with a close button (X) in the top right corner. On the left side, there is a navigation menu with the following items: "URL Filtering" (highlighted in blue), "Files Protection" (expanded), "General", "Download Protection", "Upload Protection", "Credential Protection", and "Browser Settings". The main content area is divided into several sections:

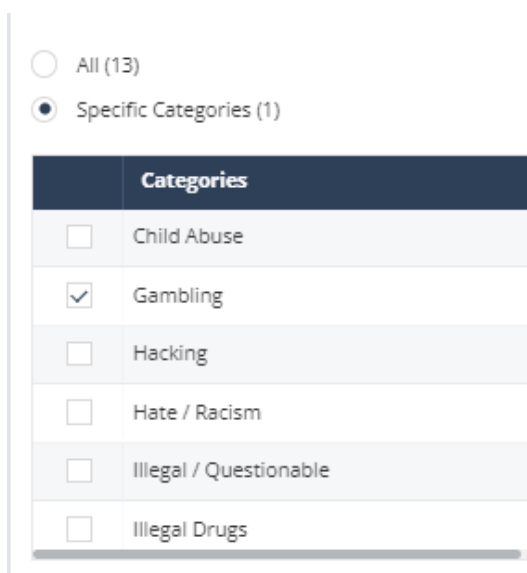
- A checked checkbox:  Allow user to dismiss the URL Filtering alert and access the website
- Categories**
  - Bandwidth Consumption (0) | [Edit...](#)
  - General Use (0) | [Edit...](#)
  - Legal Liability / Regulatory Compliance (1) | [Edit...](#)
  - Productivity Loss (0) | [Edit...](#)
  - Service (9) | [Edit...](#)
- Black list (0)** | [Edit...](#)
- Malicious Script Protection**
  - Block websites where Malicious Scripts are found embedded in the HTML
  - Allow user to dismiss the Malicious Scripts alert and access the website

At the bottom right of the dialog, there are two buttons: "CANCEL" and "OK".

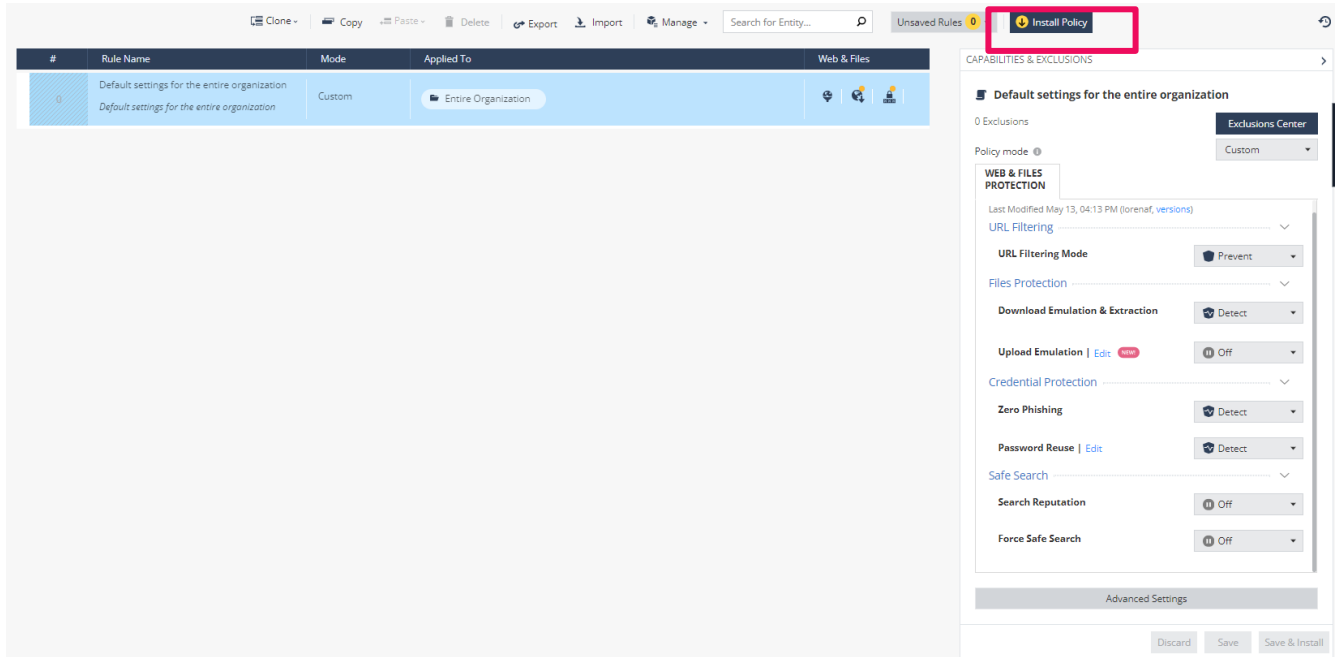
Neste exemplo, vamos bloquear o acesso a sites de jogos de azar, configurando a categoria *Legal Liability/Regulatory Compliance*.



Clicando em *Edit* temos 13 categorias mais específicas, é possível selecionar todas mas para este exemplo vamos selecionar a categoria *Gambling*.



Após selecionar a categoria, clicando em *OK* a política será atualizada. Note que é necessário clicar no botão *Install Policy* para ativar este controle.

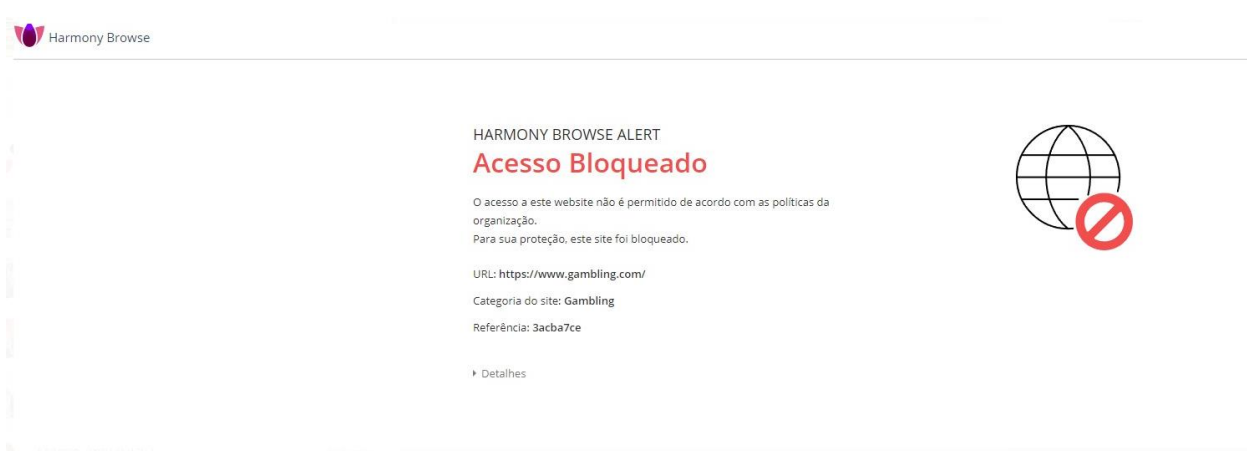


The screenshot shows the Check Point management console interface. At the top, there is a menu bar with options like Clone, Copy, Paste, Delete, Export, Import, and Manage. Below the menu is a search bar and a notification for 'Unsaved Rules 0'. A table lists the policy configuration:

#	Rule Name	Mode	Applied To	Web & Files
0	Default settings for the entire organization Default settings for the entire organization	Custom	Entire Organization	

On the right side, the 'CAPABILITIES & EXCLUSIONS' panel is open, showing 'Default settings for the entire organization'. The 'WEB & FILES PROTECTION' section is expanded, displaying various settings like URL Filtering Mode (Prevent), Files Protection (Detect), Upload Emulation (Off), Credential Protection (Detect), Zero Phishing (Detect), Password Reuse (Detect), Safe Search (Off), and Force Safe Search (Off). The 'Install Policy' button at the top right of the console is highlighted with a red rectangle.

Após instalar a política, ao tentar acessar um site de jogos de azar, o usuário receberá o alerta abaixo.



The screenshot shows a 'Harmony Browse' alert message. The header reads 'HARMONY BROWSE ALERT' and 'Acesso Bloqueado'. The main text states: 'O acesso a este website não é permitido de acordo com as políticas da organização. Para sua proteção, este site foi bloqueado.' Below this, the following details are provided:

- URL: <https://www.gambling.com/>
- Categoria do site: Gambling
- Referência: 3acba7ce

A link for 'Detalhes' is also present. To the right of the text is a red globe icon with a red prohibition sign over it.

Neste exemplo, é possível que o usuário adicione uma justificativa e acesse o site. Essa justificativa aparecerá no log de acesso no Harmony Browse.

## HARMONY BROWSE ALERT

# Acesso Bloqueado

O acesso a este website não é permitido de acordo com as políticas da organização.

Para sua proteção, este site foi bloqueado.

URL: <https://www.gambling.com/>

Categoria do site: **Gambling**

Referência: 3acba7ce

### ▼ Detalhes

Se, ainda assim, pretender aceder ao site bloqueado, por favor adicione uma justificação:

- Preciso de aceder a este website para fins profissionais
- Preciso de aceder a este website para fins pessoais
- Este website não deve ser categorizado como 'Gambling'
- Outro

*Adicione uma justificação*

Para prosseguir (não recomendado): <https://www.gambling.com/>



Card

Log Info

Origin: [LabView/202405131557PM](#)

Time: May 13, 2024 4:11:57 PM

Blade: URL Filtering

Product Family: Endpoint

Type: Log

Log Server Origin: [Redacted]

Log Server ID: [Redacted]

Application / Site

Application Name: www.gambling.com

All Application Categories: Gambling

Matched Category: Gambling

Web Client Type: Chrome

Traffic

Source User Name: [Redacted]

Machine Name: [Security Center](#)

Interface Direction: Inbound

Policy

Action: Allow

Reason: Other (user didn't specify a reason)

Details

All Application Categories: Gambling

Application Name: www.gambling.com

Resource: <https://www.gambling.com/>



O Harmony Browse é uma solução que agrega controles avançados de segurança web, com baixo impacto operacional, pois é instalado através de uma extensão de navegador e gerenciado através do portal Infinity da Check Point.

Seu licenciamento é por quantidade de usuários e pode ser adquirido sozinho ou juntamente com o Harmony Endpoint. Possui compatibilidade com Windows, MacOS e ChromeOS; a lista dos navegadores suportados pode ser encontrada no Admin Guide referenciado acima.

*Este white paper foi escrito em junho de 2024, versões futuras estão sujeitas a alterações.*