VIPRE WEB ACCESS CONTROL

VIPRE Endpoint Cloud Web Access Control gives IT administrators a simple and easy way to prevent users from visiting sites that may be inappropriate or distracting in the workplace environment.

3 REASONS TO USE WEB ACCESS CONTROL

1. **Productivity** – control social media, sports streaming, and online shopping sites to list just a few options

2. **Employer's Duty of Care** – employers have a duty of care to their employees, which means that they should take reasonable steps to ensure their health, safety and well-being by restricting access to inappropriate websites in the workplace

3. **Network Bandwidth** – video steaming services like YouTube, Netflix and Amazon Prime can negatively impact network bandwidth

Website Classification

Receive a continuously updated service that keeps track of websites, old and new, and classifies each website into one or more of 40 content categories

Content-based Website Blocking

Select from over 40 content categories to prevent users from visiting sites in those categories, or select from one of three pre-defined levels of protection
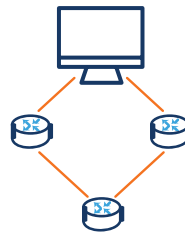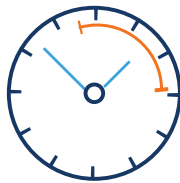
Policy-based Configuration

Easily create individual and group permissions by defining which sites are allowed at the endpoint policy level

Whitelist Allowed Sites

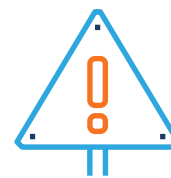Allow exclusions of individual sites within an otherwise blocked category

Custom Timeframe Selection

Grant enhanced access outside of business hours or during scheduled breaks

Agent-based DNS Analysis

No changes to existing DNS infrastructure needed as the VIPRE agent inspects existing DNS requests
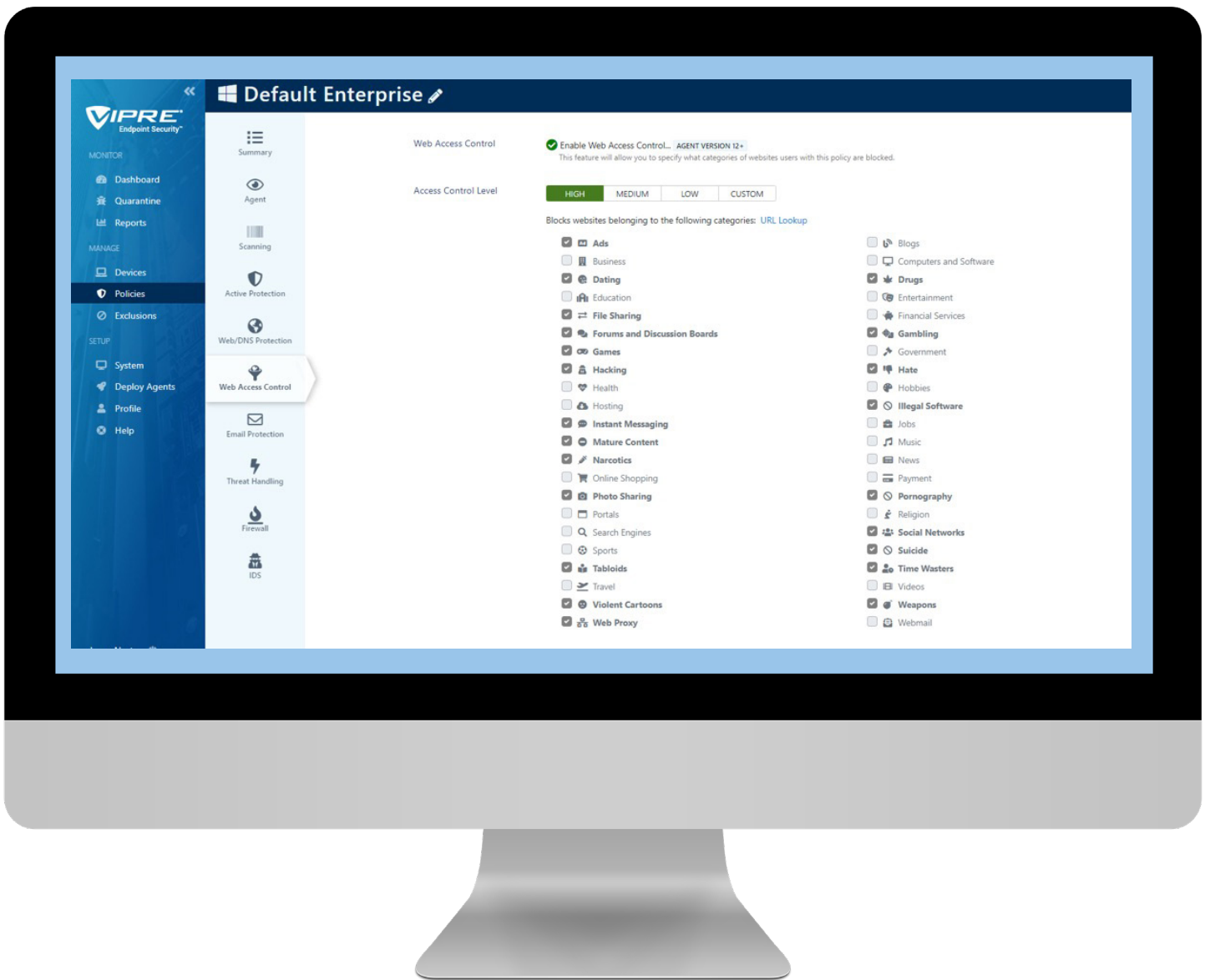
Clear User Warnings and Alerts

Redirects attempts to visit a prohibited website to a clear warning page explaining why the site is blocked and how to request whitelisting

■ VIPRE WEB ACCESS CONTROL

Features and Benefits

- Intercepts DNS requests and classifies attempts to visit websites

- Blocks access to prohibited content

- Policy-level control can be assigned to groups of devices during only certain hours

- Prevents circumvention through switching OS-level DNS provider(s) by using VIPRE's endpoint agent

- Does not replace any existing DNS infrastructure, simply intercepts and analyses DNS queries and classifies website, redirecting undesired web visits to a sinkhole

- Warns users why the requested website can't be visited

- Complete, easy-to-use whitelisting capability handles exceptions

Quickly enable and configure custom or preset access control levels and easy URL lookups from a single interface.