Admin By Request
ZERO TRUST PLATFORM

Web Access Management

Executive Summary

Overview

Admin By Request's Web Access Management solution gives IT and security teams centralized control over how endpoint users browse the internet and download executable software, without deploying proxy servers, DNS filters, or additional on-premises infrastructure.

Policy is enforced directly on the Admin By Request agent, so protection follows the device whether it's on the corporate network or not. Trusted sites and software flow without friction through pre-approved rules; everything else is blocked, held for approval, or scanned for malware before it can execute.

The Problem

Endpoints with unrestricted internet access are a significant attack surface. Users can download malicious executables from plausible-looking websites, access phishing infrastructure, run outdated browsers with known vulnerabilities, or install shadow IT that bypasses organizational controls entirely. Traditional network-layer solutions like proxies, DNS filters, and firewall rules also stop protecting the moment a device leaves the corporate network.

The challenge is governing access intelligently: allowing users to be productive while ensuring every download decision is visible, every high-risk action is controlled, and every threat is caught before it can execute.

How It Works

The solution comprises two parts:

- **On-Premises Endpoint Agent (Windows)**
  Enforces browsing and download policy locally on the device. Applies allow/deny rules, performs malware scanning, and routes approval requests to the portal. The agent operates independently of network infrastructure, so no proxy, DNS filter, or firewall rule is required.
- **Admin Web Portal**
  A secure, Microsoft Azure-hosted SaaS environment in which Web Access Management policy is configured and managed. Approval requests appear in the portal's Requests view. All enforcement decisions are recorded in the audit log.

The Solution

GRANULAR CONTROL | HARD-DENY RULES

Admin By Request's Web Access Management gives IT teams granular control over browsing and downloads at the endpoint level. Policies govern which browsers are allowed, which sites can be accessed, and which executable downloads are permitted, blocked, or sent through an approval workflow. Hard-deny rules ensure disallowed software is stopped regardless of other policy settings, while pre-approved rules let trusted sites and software through without friction.

Our Competitive Advantage

No infrastructure required.
Policy enforced at the endpoint, no proxy, DNS filter, or firewall changes needed.

Built for managed endpoints.
Just the controls IT teams need for web access governance, fully integrated with the existing Admin By Request agent.

Ease of use.
Simple to deploy, configure, and manage from the same portal used for EPM and Secure Remote Access.

Core Features

Feature	Description
Browser Lockdown	Define permitted browsers and minimum acceptable versions for Chrome, Edge, Firefox, IE, and in-app controls
Browsing Controls	Block sites by URL, restrict browsing to a pre-approved list, or allow users to request temporary access to blocked sites
Download Governance	Allow, block, require approval, or require written justification for executable downloads before they are released for use
Owner-Only Downloads	Restricts executable downloads to the assigned device owner, designed for shared and kiosk devices
MFA-Protected Downloads	Requires SSO re-authentication (Microsoft 365 / Entra ID) before an executable download is released
Intune Compliance Gating	Blocks downloads on devices that fail Microsoft Intune compliance checks
Pre-Approved and Blocked Rules	Structured allow/deny lists supporting five rule types: source website, direct URL, SHA256 checksum, vendor certificate, vendor + application name
Exportable Rule Lists	Pre-approved and blocked rules exportable to PDF, XLSX, or CSV
Machine Learning Auto-Approval	Automatically approves future requests for applications that have been manually approved a configurable number of times
AI App Auto-Approval	Scores applications 0–100 on popularity and reputation; requests meeting the threshold are auto-approved
AI Vendor Auto-Approval	Scores software publishers 0–100; all applications from qualifying vendors are auto-approved
OPSWAT Malware Scanning	Files are downloaded to the endpoint, scanned through real-time checksum detection plus multi-engine cloud scanning across 30+ engines, and released to the user once cleared
On-Device Inspection	TLS inspection runs inside the agent on the device, with no cloud proxy round-trip
Full Audit Logging	Every browsing block, download decision, approval, and malware detection recorded with user identity and outcome. Logging can be toggled per rule
Email Templates	Fully customizable email templates for all approval outcomes and admin notifications
ITSM Integration	Route WAM events to an external ticketing system via configurable email channel
Sub-Settings	Apply different policy rules to different groups of users or devices without duplicating configuration
User Instructions	Display acceptable-use notices or security reminders to users before browsing or downloading
GDPR Compliance	Choose EU, UK, or US data residency