Admin By Request
ZERO TRUST PLATFORM

Web Access Management

The Basics

Who We Are

Admin By Request creates Zero Trust SaaS-based solutions that eliminate the friction of managing endpoint privilege and access, helping organizations improve productivity, reduce support overhead, and stay secure and audit-ready.

What the Product Is

Our Web Access Management solution controls how users browse the web and download software at the endpoint. IT teams can enforce browser restrictions, block or allow sites, govern executable downloads, require MFA for risky actions, and malware scan before downloads are permitted for use. Trusted sites and downloads can be pre-approved to reduce friction, while high-risk activity is blocked, audited, or routed through approval workflows.

Why You Need It

Downloads are one of the primary entry points for ransomware and malware. Traditional security relies on scanning files after they arrive, which leaves a window where damage can already be underway. Email attachments bypass filters, users grab files from unknown websites, and outdated browsers create vulnerabilities that attackers exploit regularly.

Current solutions tend to go one of two ways: block everything (frustrating users and overwhelming IT) or detect threats reactively (too late to prevent initial compromise). Shadow IT thrives when employees work around restrictions using personal accounts & unapproved services. Organizations need visibility into what's being downloaded, from where, and by whom, without creating productivity bottlenecks.

When You Need It

- When ransomware enters through downloads and you need prevention, not just detection
- Before compliance audits that scrutinize download controls and web access policies
- When shadow IT creates blind spots in your security posture
- When users need flexibility to download files without compromising security
- When outdated or unapproved browsers create unmanaged attack surfaces

Where It Works

Web Access Management controls executable downloads at the endpoint across browser and application-driven workflows, including non-browser and in-app contexts. Controls apply on the device, so policy follows the user regardless of network.

Because enforcement lives on the endpoint rather than a network choke point, the same policy applies to office, remote, and shared or kiosk devices alike. No proxy, DNS filter, or firewall changes are required, and protection does not drop off when a device leaves the corporate network.

How It Works

When a user downloads an executable, Web Access Management checks it against your configured policy, based on rules you set (source website, URL, checksum, or vendor certificate). Depending on those rules, it flows through, is blocked, or is held for approval.

Files are held in a protected area on the endpoint and can be scanned through OPSWAT MetaDefender before release. Auto-approval settings clear trusted software automatically, and browser controls enforce permitted browsers and versions.