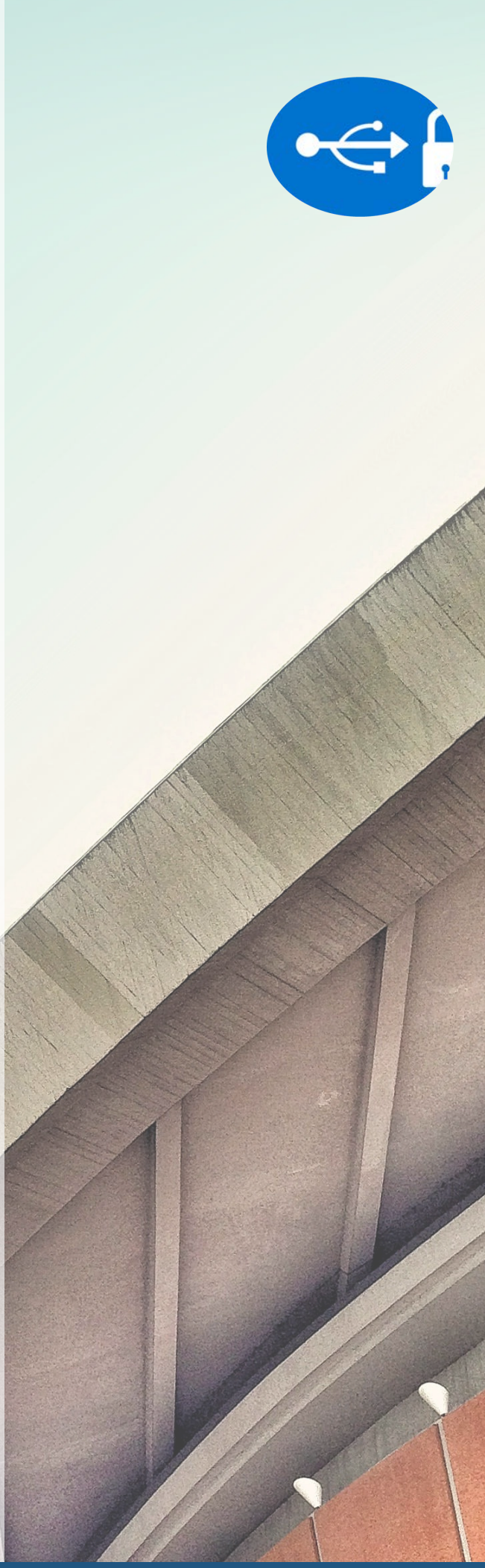
AccessPatrol

ENDPOINT DEVICE SECURITY SOLUTION

- Protect access to endpoint devices including USBs, phones, and iPads
- Create allowed list of company-approved USBs and external hard drives
- Schedule access privileges at specific times of the day
- Device usage reporting to monitor activity



ENDPOINT DEVICE SECURITY SOLUTION

AccessPatrol

SIMPLY THE BEST ENDPOINT RESTRICTION & DATA LOSS PREVENTION TOOL!

AccessPatrol provides a proactive solution for securing company endpoints (USBs, CD/ DVDs, Bluetooth, WiFi, iPhones, Smartphones FireWire, iPods, MP3s) to prevent illicit transfer of data to unauthorized devices.

✓ MANAGE DATA LEAKAGE AND SYSTEM INFECTION

AccessPatrol manages endpoint device access both on and off the network. Unauthorized access or transfer of data through USB flash drives, CDs, iPods, MP3s, FireWire, WiFi, Bluetooth on all company systems, can be managed centrally through AccessPatrol's web console.

✓ SECURITY LEVELS

Security levels to devices include full access, read-only or no access. With a few simple clicks, endpoint security can be readily implemented through the centralized console.

✓ DEVICE USAGE REPORTING

With AccessPatrol's comprehensive reporting utility, an organization can address its security compliance of mobile and storage devices.

✓ EMAIL REPORTS

For additional analysis of removable device access, make use of the handy email reports function. Schedule a time and date for a report to be sent directly to your inbox

✓ OFFSITE DEVICE MANAGEMENT

When a laptop or computer is offsite, AccessPatrol can still manage the security of endpoint devices. If access to blocked devices is legitimately required, then AccessPatrol can be easily configured to grant permissions.

✓ ALLOWED LIST

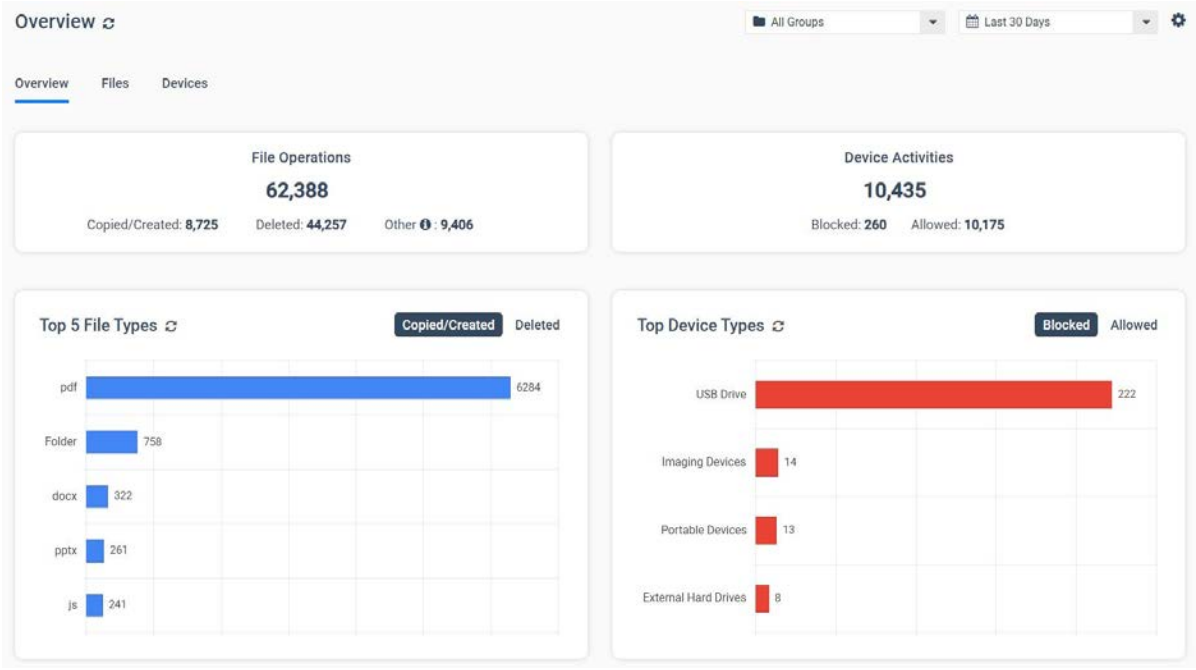
While AccessPatrol can restrict access to all endpoint devices, the Allowed List feature allows access to only company authorized devices of USBs. This minimizes leakage of sensitive data or infection of systems through unapproved or personal employee devices.

FREE TRIAL
14 DAYS - 10 COMPUTERS

WWW.CURRENTWARE.COM/FREE

AccessPatrol

CurrentWare has helped many businesses
enhance security and improve employee productivity



SYSTEM REQUIREMENTS

SOFTWARE REQUIREMENT

Currentware Server-

- Windows 8.1/10/11 : Pro or Enterprise 64-bit
- Windows Server 2012 R2, 2016, 2019

Currentware Client-

- Windows 10 or 11 : Home/Pro/Enterprise
- Windows 8/8.1/ 7 SP1 : Pro/Enterprise
- Windows Server 2012 R2, 2016, 2019

HARDWARE REQUIREMENT

All components of CurrentWare are supported on desktops and servers with the following minimum specs:

- Processor: Any CPU running i3 or similar or faster
- Memory: At least 4GB of RAM
- Disk Space: At least 1 GB of disk space

TESTIMONIALS

“Centralized Endpoint Security with AccessPatrol is a lifesaver. I have found the Centralized Endpoint Security to be the most convenient feature. Having one place to apply policies saves so much time.”

Shoreline Sightseeing

"It works a treat! Simple solution, I managed to install and use within 15 minutes. We needed a simple solution to lock/unlock USB on user PCs but it also has some other features we will use too."

www.softpicks.net