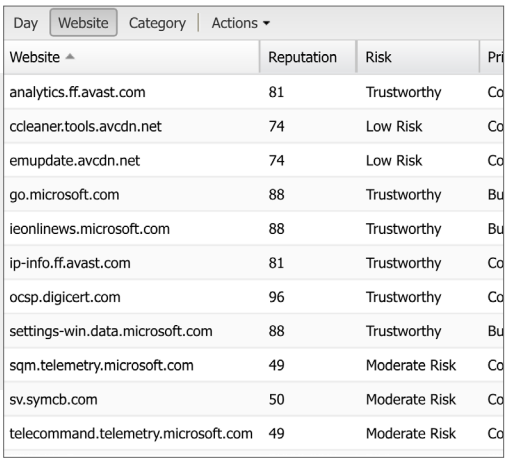
FEATURE SHEET

Web Protection

A feature available with SolarWinds RMM

SolarWinds RMM web protection is a layer of security that complements and goes beyond traditional antivirus and firewalls, helping keep your clients and end users safe and productive as they browse the web.



Website	Reputation	Risk	Pri
analytics.ff.avast.com	81	Trustworthy	Co
ccleaner.tools.avcdn.net	74	Low Risk	Co
emupdate.avcdn.net	74	Low Risk	Co
go.microsoft.com	88	Trustworthy	Bu
ieonlinews.microsoft.com	88	Trustworthy	Bu
ip-info.ff.avast.com	81	Trustworthy	Co
ocsp.digicert.com	96	Trustworthy	Co
settings-win.data.microsoft.com	88	Trustworthy	Bu
sqm.telemetry.microsoft.com	49	Moderate Risk	Co
sv.symcb.com	50	Moderate Risk	Co
telecommand.telemetry.microsoft.com	49	Moderate Risk	Co

With one click, cybercriminals can gain access to your clients' systems, steal sensitive information, and cause catastrophic downtime. A significant data breach could spell ruin for your clients and result in irreparable damage to your reputation.

SolarWinds® RMM web protection helps MSPs gain complete control over web-filtering policies, set website blacklists, and create time- and content-based browsing policies from a single, easy-to-use, web-based console.

DID YOU KNOW?

22% of data breaches involve phishing.*

KEEP CUSTOMERS SAFE

- Access controls – Block malicious sites and keep users safe
- Threat protection – Protect against malware downloads, phishing, adware, botnets, and spam threats
- Monitor bandwidth – Monitor daily usage with automated checks and alerts
- Reporting – View detailed analysis and report on suspicious and blocked sites
- Threat intelligence – Continually updated Webroot® BrightCloud® intelligence keeps protection up-to-date
- Support client HR policies around internet – Block inappropriate content for the workplace, or limit access to social media sites during work hours

STAY IN CONTROL

- Easy administration – Control users' web browsing from a unified, web-based console
- Custom policies – Use the default policies or create your own for desktops, laptops, or servers
- Custom URLs – Add custom URLs to 'dial-in' protection
- Site blacklists – Define and enforce browsing policies that keep users away from social media, web-based personal email, gaming, or other non-work-related sites
- Time-based browsing policies – Modify backlist policies to allow users to visit sites outside of business hours

* "2020 Data Breach Investigations Report," Verizon. https://enterprise.verizon.com/resources/reports/dbir/2020/introduction/ (Accessed May 2020).