Release Notes SanerNow 4.1.1.0

November 22, 2018

Software deployment

1. Deploy Software packages from array of pre-packaged list of Software applications to Saner enabled systems. We have 100's of pre-bundled packages to choose from for Windows, Linux and Mac OS X.
2. Create rules to deploy Software packages for new devices while new systems are being provisioned. All your pre-selected Software packages are deployed at one go. This helps making your systems ready to use with all essential software.
3. Create your own deployer package and roll out across all Saner enabled endpoint systems. The deployer packages can be exe, MSI, archived files with script and other installers or it can even be a download URL.
4. Uninstall Software applications across endpoint systems to remove rogue applications, blacklisted applications, license violating applications or unauthorized software at one go across all affected systems.

Real-time communication

- Continuous, real-time visibility is a must for security operations. With new, web-socket based communication between the agents and the server, everything becomes instant. Sending a scan request, performing a query, monitoring system activities, scheduling an Action in response to a security event are all immediate.

Live system health

- System details now include trending graphs showing CPU, RAM, Network and Disk usage. Click on a device to witness live data from an endpoint, the most simple and sophisticated means to monitor system health.

Role based user access

- Introducing Role-based User Access – to delegate users to handle one or more Saner services across multiple accounts.

Password protect Saner agent service

- The Saner agent service is now password protected. Any unauthorized uninstallation of Saner agent is prevented unless configured password is supplied.

Others

1. Account administrators can alter device subscription limit for accounts and extend account expiry date
2. Improved Microsoft patching
3. Endpoint Protection Software displays devices without Anti-Virus software installed in addition to devices that are under risk
4. Performance improvements
5. Saner agent upgrade and scan optimization on agents
6. Bug and security fixes