

Laptop Lockdown with Kaseya



“When it comes to objects wonderfully suited to being lost or stolen, it's tough to beat a laptop computer.

The stats reveal a widespread, costly problem: 81% of 484 IT pros surveyed say their company lost at least one laptop with sensitive information in the past year, according to security consulting firm Ponemon Institute. About 1,500,000 laptops were stolen in 2008, says Absolute Software. FBI stats show that 97% of stolen computers aren't recovered. More than half of identity theft-related data breaches stem from theft or the loss of a laptop or storage device, according to Symantec.

Yet most companies aren't locking down every laptop as if they knew one was likely to go missing. That indifference might make sense for some--maybe the data isn't worth the price of securing the computer. But for the majority of companies that will end up putting sensitive data on these machines, there are no excuses. The options for securing laptops aren't perfect, but they're expanding and in many cases getting more practical for broader use.” – Information Week

Kaseya's Virtual System Administrator

In the past six months Kaseya has seen record levels of adoption from IT personnel for this component as well as our ability to liberate them from the daily, menial tasks of monitoring and managing their ever-growing IT environments.

Kaseya provides the ability to automate delivery of IT Services to machines that they manage on and off the network as well as the IT framework to automate their daily preventative maintenance. We've seen that this enhances the stability of their network, ensures compliance and highlights the value your team brings to the organization.

Theft Protection – A thief's worst nightmare is a stolen computer that contains a Kaseya Agent. The next time this machine turns on within the vicinity of an Internet connection (WiFi, Hotspot etc), we can;

- Alert that the machine has come back online
- Identify what IP address the machine is checking in from... and provide this to authorities
- Retrieve critical data from the device
- Immediately log user out, change admin privileges and password.
- Delete or encrypt sensitive files, directories or drives
- Capture short movie, images or audio clip from built in camera and mic.
- Disable Software VPN software that might allow access to the main Network
- Deploy keyboard loggers
- Destroy all data on the machine

Through a single, web-based view you will also have:

- Inventory - Complete hardware and software auditing along with discovery.
- Software Deployment - Remote install of applications across groups of machines.
- Laptop Lockdown – Proven, developed scripts that can lockdown any laptop anywhere in the world if compromised.
- Monitoring - SNMP, WMI, Windows Services and Processes. Monitoring alarms can drive self-healing actions.
- Automation - Automated self healing scripts and procedures triggered by schedules or events: VBS, WSH Batch etc
- Patch Management - Centralized management of scanning, distribution and installation.
- Remote Control – Connect anywhere in the world while being impervious to firewalls
- Reporting - Built in report writer with graphics and dozens of templates.

Kaseya recovers stolen laptops: <http://www.crn.com.au/News/153253.kaseya-tracks-down-stolen-laptop-in-melbourne.aspx>
2) <http://www.itworld.com/mobile-amp-wireless/80106/happy-ending-how-two-stolen-laptops-were-recovered-kaseya>