Kaseya White Paper

Know Your Endpoints

Audit Tools Provide Visibility and Help Protect Endpoints, File Shares and User Accounts

Kaseya

www.kaseya.com

What IT managers don't know can hurt them, and more often than not, a lot happens on IT networks that escapes the eye of administrators. That's because IT environments tend to grow in unplanned ways as organizations expand over the years. Endpoints are added within network walls and at remote locations that are not properly tracked. Users create accounts and file shares sometimes without the administrator's knowledge, potentially opening security holes and affecting overall network performance.

Meanwhile, some systems grow obsolescent and sit forgotten somewhere on the network. File shares created for specific tasks are left unattended and unprotected, too often containing data that should be hidden from prying eyes. The same happens with user accounts that employees create for temporary purposes, or for guests on the network, but never get around to closing when no longer in use.

All of these unmonitored activities add up to a big problem – and frustration – for the administrator. Even though administrators are responsible for securing the IT environment, they cannot do so effectively without full visibility into network assets and activities. Obsolescent, unpatched machines and forgotten file shares and accounts create the conditions that hackers seek when trying to steal data and disrupt networks.

Ending these unsafe practices is paramount. IT managers need control over endpoints, user accounts and file shares, which are virtually impossible to control manually as networks expand and grow more complex. Taking control, however, is possible through effective, reliable IT audit tools that automatically track and report on systems, file shares and accounts, letting administrators manage everything from a central dashboard with full visibility into the network.

Growth Hazards

IT networks traditionally have expanded, not according to some visionary grand plan, but in a helter-skelter manner as businesses make short-term decisions to accommodate growth and leverage technology advances.

Workstations and notebooks are deployed either under the same roof or in different locations, sometimes running on different operating system releases. As assets proliferate, incompatibilities hinder communication between systems. IT managers lose track of where systems are and what they are running. Even conducting an audit to gather information on the machines administrators know about is a challenge because much of it is available only through vendor-specific interfaces at each machine.

A complete picture of which laptops and workstations access which printers, disks and components, and which users are associated with which machines, is essential, but most administrators lack that kind of visibility. In fact, a recent study found that 66 percent of IT managers admit they don't know how many IT assets are under their care.

Further complicating matters, employees in recent years have started tapping into networks with personal mobile devices that may or may not be secured. As a result, auditing endpoint devices across the network becomes even more time-consuming and complicated, especially in IT environments spread over multiple locations.

"Obsolescent, unpatched machines and forgotten file shares and accounts create the conditions that hackers seek when trying to steal data and disrupt networks."

Kaseya

Unknown, untracked endpoints contribute to the challenge of keeping track of network assets. IT budgets swell and security suffers as inefficiencies and complexity grow. As a result, organizations cannot achieve cost optimization with their IT investments. Depending on the size of the organization, this can lead to thousands or hundreds of thousands of dollars in write-offs yearly. Add to that the potential cost of a security breach, and it's obvious why businesses need better endpoint control.

Shares Without Care

IT problems tend to build on each other: Poor endpoint tracking creates the conditions for unsafe practices, such as unmonitored, unsecure file shares, which in turn exacerbate management challenges. Of course, if you can't track all the endpoint devices on your network, you cannot get a full picture of file-sharing activities.

For the most part, users set up file shares with good intentions, typically to grant peers access to Excel spreadsheets, Word documents or PDFs as they work on projects together. That's the good part of file sharing; it empowers employees with greater access to information, improves peer collaboration, and ultimately leads to higher productivity. The flip side is users often share files with little or no thought to following protocols or complying with corporate policies.

Sharing often is informal, with data flowing from endpoint to endpoint, and possibly in and out of networks, without proper controls because IT managers don't know it is happening. At times files are left on servers after users share them. Those files may consist of important documents with trade secrets or private customer information. Abandoned, they create security holes because users haven't followed set permissions properly and encrypted sensitive data. In some cases, users set up files to be shared with guest accounts without passwords, potentially leaving them wide open to hacker exploits.

The absence of file-sharing protocols causes other problems: Users leave files in hard-to-find resources and later can't remember where they are, wasting time searching for them. Potentially even more damaging, users forget the shares, which can result in data loss, theft or corruption. This translates to productivity and profit losses.

Unused User Accounts

With file sharing, good intentions without the proper controls can hurt network performance and create security risks. The same is true of user accounts activated to grant guests access to information. If the data isn't properly controlled or tracked, the potential for a security breach increases. In addition, activated guest accounts that are left unused provide a gateway to hackers into the network.

As with file sharing and unknown endpoints, the lack of a consolidated view of these user accounts, which may have different permissions levels, complicates the lives of IT administrators. Accounts created across multiple sites are invisible to administrators from remote locations, which means if administrators cannot see them, they cannot manage them.

Automation and Centralized Management

When it comes to IT tasks, manual processes considerably reduce the chances of an ideal outcome. Manual tasks are time-consuming and prone to error, burdening IT staffs with repetitious, everyday work when their time would be better spent on strategic projects and long-term planning.

The answer is to leverage a tool that automates tasks and centralizes management. When auditing endpoints, and the file shares and user accounts associated with them, such a tool is invaluable. The Kaseya Computer Audit tools automate these tasks, letting administrators collect detailed information. Computer Audit simplifies management and addresses the security issues created by unknown – and uncontrolled – hardware, file shares and user accounts.

To keep things simple and prevent heavy resource consumption, Kaseya's cloud-based architecture takes care of these tasks without having to deploy servers on site, dedicated hardware or appliances. With a simple lightweight download, administrators gain a consolidated view of their entire network to audit and report on endpoints, file shares and user account policies. Armed with this information, administrators can implement and enforce user policies that protect data and prevent network leaks.

> "In fact, a recent study found that 66 percent of IT managers admit they don't know how many IT assets are under their care."

> "Manual tasks are time-consuming and prone to error, burdening IT staffs with repetitious, everyday work when their time would be better spent on strategic projects and long-term planning."

Kaseya

With Kaseya's automated audit capabilities, managers gain the following capabilities:

- Real-time access to computer information, regardless of location and online connection status
- Minimal setup requirements and resource consumption
- Detailed audit information to keep networks well-managed and secure

Hardware

The Kaseya framework's Endpoint Share Audit capabilities let IT administrators maintain reliable, accurate records on hardware deployments, updates and replacement schedules. This removes potentially dangerous guesswork and uncertainty while helping to plug security holes.

Administrators can collect information on endpoint attributes and organize them in reports or grid-based views for easy consultation. Error-prone, inefficient manual processes are replaced by automated collection of data about machines, their locations and age.

Everything administrators need to know about endpoints becomes visible and reportable: hardware brands, system models and versions, serial numbers, bus speed, memory, chassis type, processors, number of ports, and the versions, brands and serial numbers of motherboards. System inventory capabilities also provide aggregated hardware views with details on IP and DNS/DHCP server information, disk volumes, PCI and drive models, CPU speeds and models, installed RAM, as well as printer information.

File Sharing

Kaseya also offers administrators a reliable and efficient File Share Audit tool to determine what file shares have been created on each computer and who has access to the files. Through a web-based interface, administrators get visibility into all file-share activities, and discover and plug security holes that result from unmonitored sharing practices. In this way, administrators are able to set and enforce file-share policies that prevent users from unwittingly creating potentially harmful security risks.

With File Share Audit, administrators can:

- Identify user shares across all managed machines
- Examine hardware policy issues
- Inventory computers without interrupting users
- Pinpoint failures by manufacturer and model
- Create reports and organize data as they see fit

User Accounts

Kaseya gives administrators control over user accounts through the User Audit tool, providing them with a consolidated view of custom user accounts, regardless of permission levels. As with the file-share audit tool, User Audit helps address security vulnerabilities by letting administrators collect information on accounts that, if left untracked, can be exploited by hackers trying to steal data.

Conclusion

Kaseya's Computer Audit tools are a must-have for administrators seeking full visibility and control of endpoints on their networks, as well as the file-share activities and user accounts associated with those endpoints. When not properly logged and managed, these areas of IT expose networks to hackers because they open vulnerabilities that cyber criminals exploit to get into networks. What IT administrators don't know can hurt them, but with Kaseya's audit tools, they stand a much better chance at gaining control of the endpoints under their care.

"Everything administrators need to know about endpoints becomes visible and reportable: hardware brands, system models and versions, serial numbers, bus speed, memory..."

"Kaseya's Computer Audit tools are a must-have for administrators seeking full visibility and control of endpoints on their networks, as well as the file-share activities and user accounts associated with those endpoints."

About Kaseya

Kaseya is the leading global provider of IT Systems Management software. Kaseya solutions empower virtually everyone — from individual consumers to large corporations and IT service providers — to proactively monitor, manage and control IT assets remotely, easily and efficiently from one integrated Web-based platform.

Kaseya

www.kaseya.com