



MANAGED WORKPLACE®

Network Audits

Nine Reports that Demonstrate
Immediate Value to New and
Existing Customers.

Feature Summary

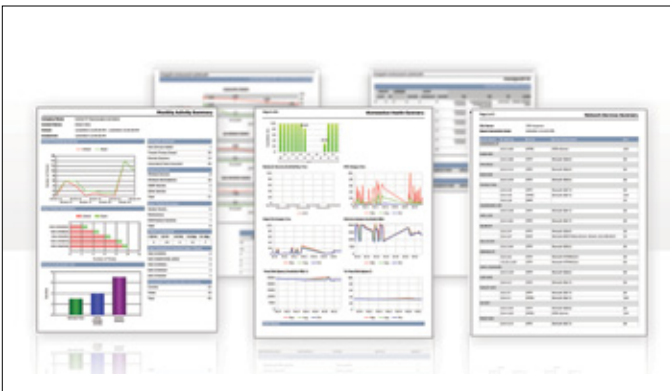
Running a Network Audit lets you rapidly identify and address critical—and potentially costly—issues for your clients. Designed specifically for Managed Services Providers, these reports provide you with insight into your client's IT environment, identifying pain points and security gaps, and providing you with the opportunity to make an immediate positive impact on their operations. This positions you as a trusted advisor rather than just another service consultant and provides the foundation for deeper relationships between you and your clients.

Benefits:

- Close new business by demonstrating immediate value to your prospects/clients
- Establish a foundation of trust based on empirical and actionable data
- Increase your revenue by identifying and addressing potential trouble spots

Steps to Proven Value:

- Deploy Onsite Manager on customer network
- Run automated IT asset discovery
- Provision Managed Workplace for proactive monitoring and management
- Produce out-of-the-box audit reports
- Review the audit results with prospects and clearly communicate the value of your services



"We use Network Audits and Managed Workplace as a really good way to demonstrate our value to prospective clients. When you can go in and show someone a software inventory report that lists the 3200 pieces of software installed on their network—there is immense power in that."

-Brendan Howe, Managing Director, TDCNet

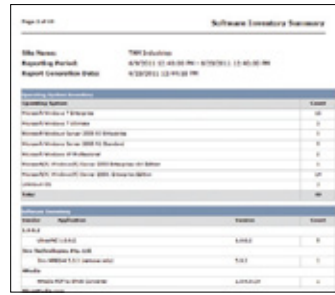
See All. Manage All. Service All.
www.levelplatforms.com

LEVEL
PLATFORMS



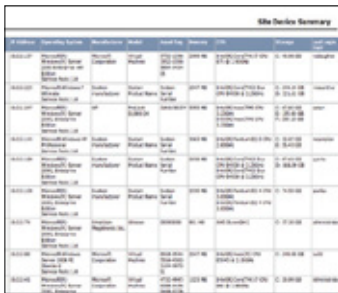
Hardware Inventory Summary

Provide a comprehensive record of all hardware (workstations, routers, network printers, switches, and more) discovered by Managed Workplace. Discover the diversity of the environment and identify obsolete equipment.



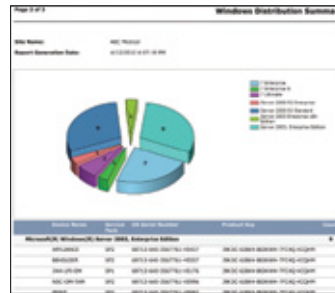
Software Inventory Summary

Provide a detailed inventory of all applications on each workstation or server, all operating systems and hotfixes, and then identify unauthorized software that needs to be removed or out-of-date software that needs upgrading.



Site Device Summary

Get quick access to device, memory, CPU and storage information that can represent up-sell and refresh opportunities.



Windows Distribution Summary

Identify upgrade and site standardization opportunities for Windows operating systems, reduce security risks by ensuring Service Packs are up-to-date, and spot possible compliance issues.



Server Health Summary

Identify all servers and assess Key Performance Indicators (KPIs) such as installed memory, CPU performance, server uptime and disk utilization.



Workstation Health Summary

Assess KPIs such as CPU uptime and disk utilization for each workstation on the site to identify opportunities for optimization.



Windows Security Audit

Identify all current security issues including missing security updates, weak passwords, and firewall and access vulnerabilities.



Network Services Summary

Identify all services active on all devices, including potential trouble spots such as a web servers with open FTP.



Site Warranty Summary

Discover which devices at the site are under warranty and which are not, and from there identify upgrade opportunities, or get critical infrastructure protected under a custom warranty from you.

© 2012 Level Platforms Inc. All rights reserved. Level Platforms, Managed Workplace, Onsite Manager, Service Center and the Level Platforms logo are the exclusive properties and trademarks of Level Platforms Inc. All other brands, product names, company names, trademarks, service marks, images, and symbols are the properties of their respective owners.