



Reviewer's Guide

To AdRem NetCrunch

Table of Contents

ABOUT NETCRUNCH.....	3
PRICING AND LICENSING	3
NETCRUNCH EDITIONS	3
FUNCTIONAL OVERVIEW	4
SYSTEM REQUIREMENTS	6
ABOUT ADREM SOFTWARE	7

About NetCrunch

Product name	AdRem NetCrunch
Current version	5.1 released in May, 2008
First released	2002
30-day evaluation version download	www.adremsoft.com/demo/
List of upgrades in the current version	http://www.adremsoft.com/netcrunch/page.php?id=whats-new
NetCrunch White Papers	http://www.adremsoft.com/demo/download.php

Pricing and Licensing

NetCrunch runs on a single workstation and it is licensed by the number of monitored nodes and by the NetCrunch remote connections. The remote connection can be used as Web Access and Notification Client.

The number of monitored counters, services and events is not limited.

The pricing of NetCrunch **Premium XE** edition starts at **\$7,495**, and for the **Premium** at **\$2,595** (both editions include 1 Year Professional Service Agreement with annual Upgrade Protection).

NetCrunch Editions

NetCrunch network monitoring software comes in two editions: Premium XE and Premium. The XE edition is optimized for monitoring of large networks and it is recommended to be run on a dedicated machine.

The types of NetCrunch 5 licenses include:

- NetCrunch 5 Premium 125
- NetCrunch 5 Premium 300
- NetCrunch 5 Premium 600
- NetCrunch 5 Premium XE 1000
- NetCrunch 5 Premium XE Unlimited

Read more about NetCrunch editions at:

<http://www.adremsoft.com/netcrunch/page.php?id=editions>

Functional Overview

NetCrunch in a Nutshell

NetCrunch 5 is a comprehensive network management and application monitoring solution for networks of up to several thousand nodes.

NetCrunch unifies fault management by collecting and alerting on events received from a variety of external sources such as: Windows Event Logs, syslog, SNMP traps.

NetCrunch consists of WMI, RPC, SSH and SNMP monitors for monitoring of diverse operating systems and networking devices. It contains over 65 built-in Network Service monitors and 5 advanced user experience monitors (HTTP/S, POP3, FTP, SMTP, DNS).

Auto Discovery

NetCrunch automatically (and periodically) discovers TCP/IP nodes in order to create an accurate view of the network and to draw maps of logical and physical topologies. To make the network discovery process complete, the program is shipped with predefined filtered views and pre-configured Monitoring Policies. Discovered devices are automatically classified and added to relevant views. After completing the network scan, NetCrunch determines network relations between nodes and intermediate routers to set up monitoring dependencies for each node. Besides finding nodes, the program also detects network services they are providing.

Event Management

NetCrunch processes events coming from a variety of sources. Some of them may be external like *SNMP Traps* or *Windows Event Log* entries and others generated by NetCrunch like *Monitoring Events* (node state changed) or *Atlas Events* (like new node discovered).

Actions assigned to an event can be performed immediately or after some time if the event has not been cleared. Most of the built-in events are correlated and when the event condition changes they are automatically cleared.

Availability Monitoring

Some services (or devices) can be checked by a simple PING where some others can be checked more thoroughly by Network Services monitors. We call these monitors *intelligent pings* because they can check not only connectivity but also response received.

Monitoring of key services can be performed on multiple levels. As the low level checks only basic service answer (it's usually some kind of HELLO), the higher levels of monitoring allow to check for more specific things like authentication (HTTP, FTP, POP3, SMTP) or if the service is operating properly (i.e. downloading file, receiving and sending test email).

Network Performance Monitoring

NetCrunch allows agentless performance monitoring of different network devices (SNMP), operating systems, and applications running on top of Windows or UNIX/Linux. This is realized by monitoring selected performance counters values and triggering alerts. All those values can be collected and stored for later long term trend analysis.

Program enables agentless monitoring of servers (Windows, Linux, Mac OS X, BSD, and NetWare) from a unified interface. NetCrunch requires administrator credentials to connect to servers and gather statistics about performance counters.

Monitoring Policies

Monitoring policies are sets of rules defining events which need to be monitored and which data that should be collected for later reporting. One node can be assigned to multiple policies; it can also have its own policy defined that may override map or atlas policy definitions.

Trend Viewer

Data collected by NetCrunch can be used for reporting or for on demand trend analysis. Performance history of a single counter can be compared across multiple nodes on a single chart to determine under- and over-utilized resources.

The program automatically initiates data collection, based on monitoring policies to generate reports. Reports are also generated on demand or periodically delivered by e-mail to selected recipients.

Users can export the data collected by NetCrunch to an industry standard databases for further analysis and to diagnose with external reporting tools.

Remote Access

Users can access NetCrunch remotely using the web-based client and also receive notifications using the desktop notification client.

The program allows creating profiles for remote users, limiting their access to certain network maps or program functions. All remote access sessions can be logged by NetCrunch, showing what users connected remotely to NetCrunch, from what IP address and what tasks they performed. Fast and secure communication with NetCrunch is possible thanks to the encryption and compression algorithm.

System Requirements

NetCrunch 5 System Requirements

	Minimum	Recommended
Processor	Intel Pentium 4 2.8 GHz or equivalent	Intel Core 2 Duo 2.0 GHz or equivalent
RAM Memory	1 GB	2 GB
Free Disk Space	800 MB	4 GB
Display	1280x1024 True Color	Wide Screen 1680x1050 True Color
Web Browser	Internet Explorer 6, Firefox 2	Internet Explorer 7, Firefox 2
Operating System	Windows XP SP2, Windows Vista SP1 (except Home editions)	Windows Server 2003 x32 (x64 with XE edition)

The recommended system requirements should be applied for monitoring of more than 500 nodes by NetCrunch network monitoring software.

For VMware installation read our [VMware Support Statement](#)

About AdRem Software

AdRem Software provides network management solutions for businesses that seek affordable ways to maximize ROI on IT infrastructures. AdRem's products allow IT departments to graphically represent network infrastructure, address problems in real-time, and perform capacity planning. AdRem's solutions are sold through AdRem's resellers, distributors and system integrators and deployed on servers worldwide.

Company Address

AdRem Software, Inc.
410 Park Avenue, 15th Floor
New York, NY 10022
Phone: +1 (212) 319-4114
Fax: +1 (212) 832-4114
<http://www.adremsoft.com>

E-mail for customer contact:

sales@adremsoft.com

Press Room

www.adremsoft.com/pressroom

Press Releases

www.adremsoft.com/pressroom/all_releases.php

Public Relations Contact

Sylwia Hans
PR Manager
Phone: +1 (212) 319-4114
Fax: +1 (212) 832-4114
pr@adremsoft.com