



---

Organisations Under Threat  
*Securing IT Availability*

---



## Organisations Under Threat!

Every organisation is highly dependent on its IT and network. Today's IT Manager has become both guardian and service delivery specialist.

As the guardian, the IT Manager has to ensure all elements of the network are available and secure. The state of non-productivity is one that threatens every organisation; servers go down, switches fail and services become unavailable, the network lacks resilience; the network is misused creating bandwidth issues and security incidents, the efficiency expected of IT is compromised; and the loss of data, theft of corporate information and unauthorised intrusion at the end-point robs organisations of competitive intelligence, operational knowledge and commercial records.



Network management, network behaviour analysis and endpoint security, the Emereo Solutions portfolio provides the answers to keep IT available and resolve service issues. All of which maintains the organisation in an optimum operational state.

What's more Emereo Solutions are rapid to deploy and delivers sustained low cost of ownership with immediate realisation of business benefit.

“From a management perspective what we lacked was one single view of all network based issues facing the business. In short without this view how could we claim to be in control?”

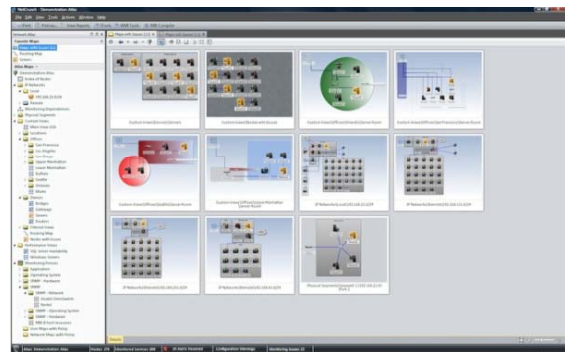
Dave Thornley, Sheffield Hallam University



Availability of services and applications is what the business demands. It's the responsibility of IT to ensure there is resilience across the network which hosts the servers and switches to ensure services and applications remain available.

Emereo |NMS is a solution where consulting services adhere to the best practice framework of ITIL, allows for integration with the IT service desk to enhance incident, problem and change management processes and provides a management reporting suite to not only satisfy day-to-day availability management needs but also aids capacity forecasting for more strategic decision support and budgeting.

Core to Emereo |NMS is NetCrunch, a cross-platform network monitoring and management system. NetCrunch accurately maps your network topography to account for devices and illustrate their relationships and dependencies with other devices, systems, services and applications. Consequently NetCrunch allows you to predict and manage the impact of downtime across the network.



NetCrunch lets you **visualise, monitor, analyse** and **report** on all aspects of your network from one intuitive interface. NetCrunch lets you avoid costly downtime, optimise asset utilisation and manage network transition.

**Custom Views** – NetCrunch generates specific views of the network to satisfy the information needs of specialist support groups and management - by platform, application or service.

**Monitoring** – With NetCrunch you can select the range of critical devices for specific performance monitoring. This allows support teams to take proactive management of failing devices at times of poor status and availability.

**Problem Resolution** – As problems occur with a network device NetCrunch manages its changing status, alerts network analysts and escalates to support groups and management to ensure minimal downtime. NetCrunch generates metrics to measure service level targets and improve problem closure rates.

**Integration** – NetCrunch integrates with desktop management tools to provide complete asset management and device alerts can be logged directly with the service desk to better manage the services delivered to end-users. NetCrunch can also receive SNMP traps from security products, such as DriveLock, to quickly highlight points under attack from unauthorised access or usage.

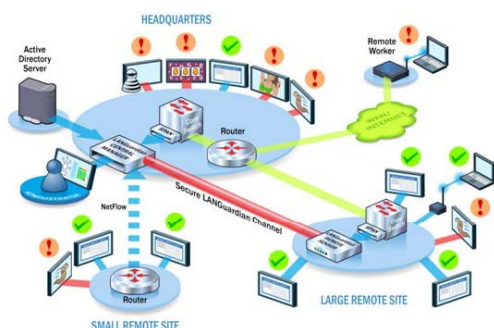
Many organisations have utilised Emereo |NMS because their businesses deserve high network availability.



Having visibility of your networked devices, systems, services and applications is only one part of the equation, user activity is another. Consequently every organisation needs to be able to analyse network behaviour to ensure traffic distribution is not compromised by inappropriate usage.

Emereo|NBA is a solution which helps organisations understand the burden being placed upon the network by user activity, department/office demand or by the services being loaded by a device at a specific IP location. Our consulting services help IT management shape usage policies which can be applied across the organisation.

Central to this solution is LANGuardian, a powerful, cost-effective, all-in-one network behaviour analysis system which gives a single view of all critical network performance data.



LANGuardian provides a comprehensive suite of features in one package, and has the fastest time-to-deploy in the market, ensuring you gain real benefits from day one. So much so you will be reporting on events in less than an hour without the use of agents or clients. Additionally you will find that LANGuardian will:

**Accelerate** troubleshooting via the consolidated view of activity and rapid drill down support rather than provide self governance

**Validate** existing network and security infrastructure and alert on detected anomalies

**Integrate** with leading network and security solutions, such as NetCrunch, enabling LANGuardian to interoperate with and add value to your existing systems

**Support** self governance - a feature which encourages employees to take responsibility for their activity and reduces the need for complete blocking of certain types of network activity

**Retain** data for compliance and forensic purposes

More than 30% of all attacks originate inside the company

*IT blamed for all data breach incidents. Research from security services firm Orthus.*



The final part of the availability equation is securing critical management information sources and systems from unwanted attack. Data theft and loss and unwarranted intrusion can and does cause significant security issues and often the threat is very close and it's the end-points across an IT infrastructure where 'leaks' occur. The fall-out from any of these scenarios will dictate that critical services, applications and information become unavailable as investigation into these events is undertaken.

Understanding the threats is the first step Emereo takes in helping you shape a security policy which is applicable to your organisation and its users. To enable this policy Emereo|EPS is deployed using DriveLock to place controls on devices and applications, in fact anywhere critical information resides electronically, by barring USB devices to hard-disk encryption and white-lists for applications.



**Data Theft** - Criminals can copy large amounts of data to mobile storage devices, and the majority of data theft is perpetrated by insiders. Favourite targets include research data, customer lists, customer credit card info and competitive data. With DriveLock you get complete control over who can copy what to and from USB sticks and other mobile storage devices.

**Data Disclosure** - USB sticks are cheap to replace but the data may be easy to replace and Information disclosure can be very costly. DriveLock automatically and transparently encrypts data on USB sticks and other storage devices to safeguard your data.

**Intrusion** - Uncontrolled peripherals can give intruders access to corporate networks. Mobile devices can also contain viruses and other malware. With DriveLock you can protect your network by gaining total control over the use of all ports on computers in your network.

**System Instability** - Troubleshooting problems caused by the uncontrolled use of peripheral devices becomes time-consuming and expensive. DriveLock ensures that only approved devices are connected to the computers in your network. There's no need to worry about the impact of unapproved devices.

*Emereo Solutions also provide support for Novell Netware and in particular deliver services that enable organisations to securely transition from Novell to Linux or Microsoft Windows.*

## About Emereo Solutions

Emereo Solutions (UK) Limited (formerly AdRem Software UK) was founded in 2004 as a privately held company. Its installed base serves a diverse range of customer types base from Central and Local Government, the NHS, Education, Finance Services, Law firms and many more organisations where the goal is making IT effective and available. Emereo's solutions have been deployed on over 15,000 servers across the UK and Ireland.

Emereo provides rapidly-deployed software solutions for infrastructure management covering network management and monitoring, network behaviour analysis, end-point security and IT service management. Our solutions help organisations secure greater resilience of their enterprise networks so IT can provide better services to the business and operations it supports.

Best-of-Breed products adhere to ITIL and COBIT best practices and ensure compliance with initiatives such as Sarbanes Oxley, FSA, GSI, e-Health and e-Government. The Company's products deliver efficient and effective solutions without prohibitive costs and extended consulting times traditionally associated with enterprise solutions.



**Emereo Solutions (UK) Limited**  
6 Rickett Street  
London SW6 1RU

Telephone: 0871 717 7294  
Facsimile: 020 7385 7183

[www.emereo.eu](http://www.emereo.eu)

©2008 Emereo Solutions (UK) Limited  
This document is written by Emereo Solutions and represents the views and opinions of the Company regarding its content, as of the date the document was issued.  
The information contained in this document is subject to change without notice.

Emereo Solutions encourages the reader to evaluate all products personally.  
Emereo, Emereo|NMS, Emereo|NBA and Emereo|EPS are trademarks or registered trademarks of Emereo Solutions (UK) Limited.  
NetCrunch, LANGuardian and DriveLock are registered trademarks of AdRem Software Inc., NetFort Technologies and CenterTools  
All other product and brand names are trademarks or registered trademarks of their respective owners.

First Published February 2008. Revised July 2008