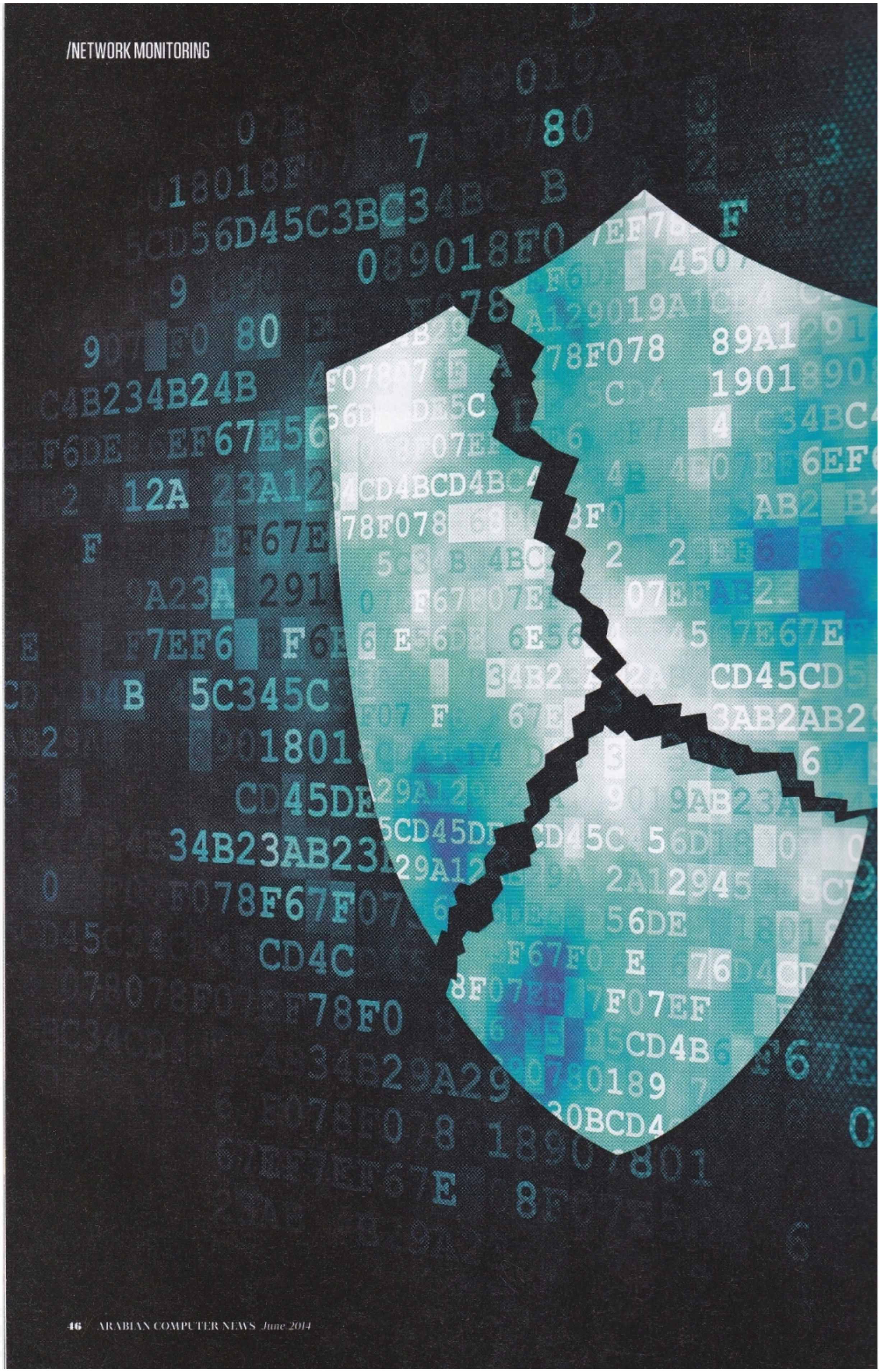
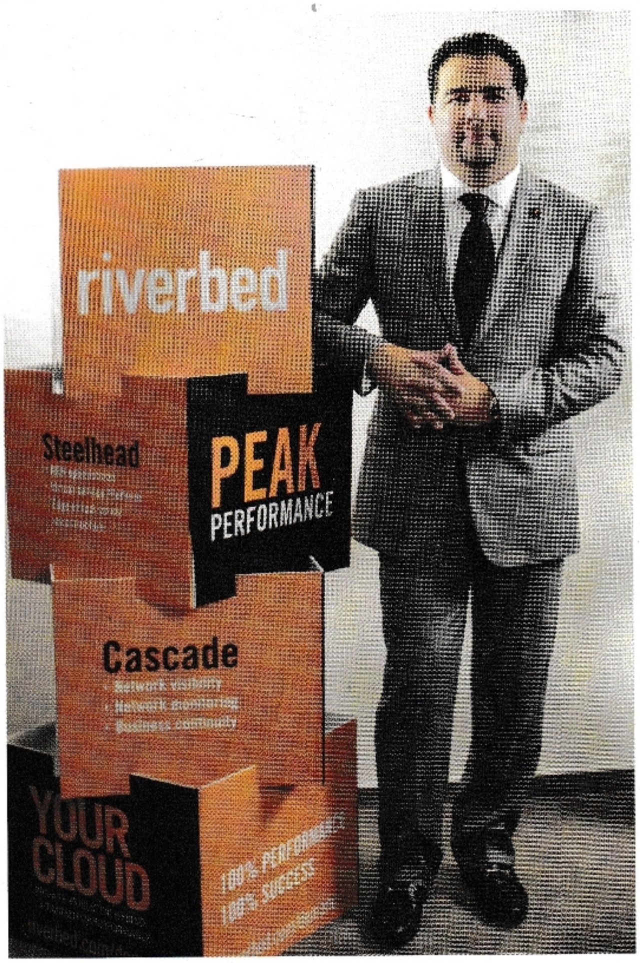


TAKING CARE OF THE NETWORK

Unplanned downtime can be very costly, so organisations are adopting more monitoring to protect the network.

WITH HIGH-PROFILE NETWORK OUTAGES HITTING THE NEWS MORE REGULARLY, IT PROS ARE PAYING CLOSE ATTENTION TO ADVANCEMENTS IN NETWORK MONITORING TECHNOLOGIES. BUT CAN THE LATEST CROP OF SOLUTIONS REALLY GUARANTEE PROTECTION FROM DOWNTIME, AND DO BUSINESSES REALLY NEED TO INVEST IN THE LATEST FUNCTIONALITIES?



The cost of unplanned downtime is increasing as infrastructure becomes more complex, says El-Khayat.

In June 2012, the RBS/NatWest banking group in the UK was hit by an enormous technical outage, affecting millions of customers, who could not receive or make payments for almost a week. The outage was estimated to have cost the firm more than $205 million — a hefty amount for an organisation that, the very same quarter, posted overall losses of $2.46 billion.

Examples of how network outages affect businesses — in very real financial terms — are littered across the pages of technological history. In February 2013, it was reported that a 49-minute outage at Amazon.com cost the company more than $4 million in lost sales. And in 2009, PayPal lost an estimated $28 million in commerce due to a four-hour outage.

As SamerIsmair, MEMA network consultant at Brocade, so eloquently puts it: "Clearly, network downtime impacts profitability."

While these are some of the most extreme examples of what a network outage can result in, businesses find themselves battling against the threat of downtime regularly. Indeed, as businesses become increasingly dependent on their networks, the pressure is on network managers and CIOs to ensure that unplanned downtime is kept as close as possible to — in an ideal world — absolute zero.

"Unplanned downtime, if you look at the latest reports, is something that is costing organisations more and more, as infrastructure is becoming more and more complex," explains Taj El-Khayat, general manager for the MENA region, Riverbed.

As answer to this problem, organisations have turned to increasingly advanced network performance monitoring solutions. The idea is to gain a holistic view of the IT infrastructure, ensuring that any errors can be accounted for and remedied before they begin to cause larger problems. And over the past few years, businesses in the Middle East have begun to pay close attention to developments in network monitoring technologies.

Unfortunately, even the basics are lost on some businesses, as evidenced by the high-profile outages mentioned earlier on. According to Dev Anand, ManageEngine's director of product management, there are a number of key capabilities that a network monitoring solution should provide.

"Network monitoring empowers network admins to proactively monitor the network and receive notifications before the fault turns critical and impacts the business. It provides in-depth visibility and control over the network, and helps admins to take informed decisions without any ambiguity. It eliminates the guess work by allowing them to drill down to the exact root cause of the issue and troubleshoot it quickly," he explains.

"With a comprehensive network monitoring solution, admins can find whether the reason behind the bandwidth spike is due to a wrong configuration change or the live streaming of a football match, and troubleshoot it accordingly. Network monitoring also helps the admins to know how much load their network can handle and optimise it."

There are myriad network monitoring tools available these days, and most comply with this check-list of capabilities. However, vendors are at pains to explain that organisations need to stay up with the latest technologies to stay safe.

For example, Aruba Networks, which specialises in wireless networking, believes that businesses simply cannot ignore the need to monitor their wireless networks. According to Ammar Enaya, regional director at Aruba Networks Middle East and Turkey, this is because wireless networks, which are increasingly becoming as important as wired networks, can be downed by so many different factors.

"Unlike in the wired network, the factors affecting the perfor-

Enaya: Monitoring wireless networks is much more complicated than monitoring fixed infrastructure.

Anand: A good network monitoring solution should provide in-depth visibility and control over the network.

There is a clear link between network downtime and reduced profitability for organisations, says Ismair.

mance and security of a wireless network are far more difficult to track. For example, we have to provide visibility into parameters such as radio frequency, interference, noise and the number of users connected per channel, per access point. Unless this information is available, the administrator would be unable to efficiently manage the wireless network," he says.

Other vendors, meanwhile, are working to provide unified solutions that monitor all aspects of a network. Brocade's Ismair, for example, points towards the Brocade Network Advisor, which he describes as the industry's first unified network management solution for data, storage, application and converged networks. Support is offered for everything from fibre channel SANs and fibre channel over Ethernet (FCoE) networks to IP switching and wireless, he claims.

"It provides end-to-end network visibility across these different network types in a single application. It supports comprehensive lifecycle management capabilities across these different networks via a seamless and unified end-user experience," comments Ismair.

As ever, there is no one-size-fits-all answer to this question, as it entirely depends on what the business needs are. For example, a large e-commerce website, with a vast array of various network functions, may very well need Brocade's all-you-can-eat monitoring bundle. But a small manufacturer, on the other hand, is unlikely to need such a robust solution.

There are, however, new capabilities that most IT departments might at least be interested in, particularly as they find their fields of responsibility increasing at a faster rate than their budgets. According to ManageEngine's Anand, automation of

TOP 10: NETWORK OUTAGES IN 2013

1 **Microsoft Windows Azure:** A sub-component of the system failed worldwide. The outage lasted more than 20 hours.
2 **Google:** Services went down, causing global Internet traffic volume to plunge by about 40%.
3 **Amazon Web Services:** Connectivity issues affected a single availability zone, disrupting a notable portion of Internet activity.
4 **NASDAQ:** Software bug, and inadequate built-in redundancy capabilities, triggered a massive trading halt in the US.
5 **OTC Markets Group:** Network failure prompted a shut-down in over-the-counter stock trading in the US for more than five hours.
6 **Healthcare.gov:** Downtime caused by a service outage at Verizon Terremark data centre in the US.
7 **Amazon.com:** One hour of interrupted service may have translated to $5 million in lost revenue.
8 **Microsoft/Hotmail/Outlook.com:** Firmware update caused servers to overheat. Hotmail and Outlook.com suffered a service loss.
9 **Google Drive:** Slow download times caused by a network control software glitch, resulted in latency and recovery problems.
10 **Gmail:** Slow download times triggered by dual network failure affected 29% of users.

Source: NeverFail Group

troubleshooting is becoming an increasingly popular demand among customers. After all, if a time-consuming process can be automated, it frees up staff for other tasks.

Automation is necessary for doing more with less and eliminating repeated tasks. Most of the network issues have a common set of troubleshooting activities. For example, whenever the network is slow, the admins will be doing a set of actions such as verifying the CPU and memory of the router or switch, verify whether any configuration is modified, and bandwidth utilisation," he explains.

"These steps can be automated so that whenever there is an issue in the network, the network monitoring solution can automatically perform these actions immediately and provide hands-on information."

Naturally, policies need to be defined with any automated product, but the experts believe that it is worth putting the effort in. ManageEngine claims that its solutions provide good functionality out of the box, though naturally users can fine tune the products to provide better insight into the network, as is the case with any modern network monitoring technology. Meanwhile, Brocade's Ismair believes wholeheartedly in investing the time into setting up automated monitoring processes by creating event triggers, particularly if a business is looking for early warnings against failures.

"Event triggering is an essential element in the automation. Triggers can be activated in scenarios such as too many users connected to a single access point, failure of a switch, sudden spikes in bandwidth consumption, et cetera. The triggers provide an early warning against failures and help initiate counteractive measures," he says.

Perhaps the biggest argument for indulging in the newer network performance monitoring technologies, however, can be found in the quest to create a future-proof network. According to Riverbed's El-Khayat, a robust network monitoring solution is essential if organisations want to experiment with new trends such as software-defined networking (SDN) or the software-defined data centre (SDDC).

"For example, if you want to do better capacity planning, if you want to do a what-if analysis, or if you want to do even better on end-user experience – all of these are features beyond the traditional network performance monitoring tools, and it is the foundation for adoption of the new trends and the future trends around cloud and virtualisation," he says.

"If you look at those three key trends – SDN, SDDC and cloud – it's key to have solutions like this. What happens with the monitoring tools and application performance monitoring tools, the purpose of them is to give you end-to-end visibility, and give you this type of analysis."

Other vendors agree that the latest generation of networking monitoring technologies will help ease the transition to the likes of SDN and cloud. However, with such trends still taking baby steps in the Middle East, it may be a while before network managers are convinced.

What is quite clear, however, is that the base requirements must be covered by a network monitoring solution. As any number of high-profile network outages will attest, businesses can rarely afford to deal with the consequences of unplanned downtime. And a good network performance monitoring solution should, at the very least, help to mitigate the risk. ■

[redacted]

"NETWORK MONITORING EMPOWERS NETWORK ADMINS TO PROACTIVELY MONITOR THE NETWORK AND RECEIVE NOTIFICATIONS BEFORE THE FAULT TURNS CRITICAL AND IMPACTS THE BUSINESS."

RELIANCE ON ETHERNET

According to Andrew Lane, European marketing manager at Ideal Industries Networks, organisations that rely heavily on Ethernet need to be able to troubleshoot quickly and effectively to avoid downtime.

"Any user of Ethernet has to accept that there will inevitably be network problems from time to time; devices can't always connect to other devices, there can be IP (Internet Protocol) address conflicts, servers can go down and of course, the network can run slowly," he says.

"Critically, there are always going to be cabling problems. In fact around 70-80 per cent of network issues relate to cabling. For example, two very common problems in an office environment which can affect data transmission are a) damaged cables – often caused by mice chewing through them – and b) disorganised and untidy patch panels."

Lane admits that Ethernet and cabling problems are almost impossible to avoid sometimes, but as a way to ensure that the effects of downtime are kept to a minimum, he suggests investing in a purpose-built troubleshooting tool.

"Since we know that network issues will invariably occur, and they need to be rectified as soon as possible, it makes sound commercial sense to invest in a purpose-designed troubleshooting tool," he explains.

[redacted]

[redacted]