



Endace 2011 Network Visibility Monitor

Why 10 gig breaks corporate security guidelines

INTRODUCTION AND BACKGROUND

With 71% of organisations surveyed confirming that they have already made the transition to 10Gb/s networking it's fair to argue that high-speed networking is now mainstream. And with 43% of organisations confirming that they have plans to adopt 40Gb/s or 100Gb/s networking, it's clear that ultra-high-speed networking is definitely on the planning horizon. But it's not all plain sailing.

According to this study there are both visibility and security holes appearing left, right and centre as speeds increase. The higher network speeds are challenging organisations' ability to manage their networks and by all accounts, the incumbent set of network monitoring and security vendors aren't coming to the rescue.

METHODOLOGY

Between February and June 2011 we conducted more than 200 telephone interviews with networking and security professionals from nearly 100 organisations across North America. The object of the study was to try to understand what impact 10-gigabit-per-second networking is having on their operations and how it is affecting their ability to measure, monitor and protect their mission-critical networks, systems and data.

The research was conducted by an independent research agency based in North America. Senior networking, operations and security professionals were targeted based on their job titles and descriptions as listed in publicly available sources. Interviews were unsolicited, conducted anonymously and took, on average, approximately 10 to 15 minutes each to complete. Respondents were not incentivised to participate, other than a verbal commitment from the interviewer that their identities would be protected and the high-level results of the survey would be shared with them at a later date.

Companies were selected from a wide variety of industries including tier-two telcos, online service providers, retailers, manufacturing companies, health service providers and gaming companies. To qualify for inclusion organisations needed to have an annual revenue of at least \$10 billion and to have an international footprint. A minimum of two interviews per-company was required in order for them to be included. Forty percent of organisations contacted agreed to participate in the survey, which is surprisingly high given the potentially sensitive nature of some of the questioning.

HYPOTHESIS

We went into the research with the following high-level set of suppositions about the general market based on our own experience with customers we work with:

- Monitoring, measuring and protecting a 10Gb/s network is significantly more challenging than monitoring a 1Gb/s network
- As a result of the shift to 10Gb/s, organisations now have significant network security blind-spots that are exposing them to unacceptable levels of risk
- The sheer volume of data involved in 10Gb/s environments presents significant challenges to the solutions currently available from traditional vendors
- The shift to the cloud has raised the profile and importance of network performance, network security and application performance monitoring tools across the organisation
- The recent spate of high-profile security breaches has sharpened organisations' awareness of preventative network security issues and raised the security issue up to board-level
- Organisations are not asking the right questions of application vendors and are at risk of investing in technology that won't scale to meet their needs as they move to 10Gb/s networks and beyond.

10 GIGABIT NETWORKING—A MARKETING STUDY



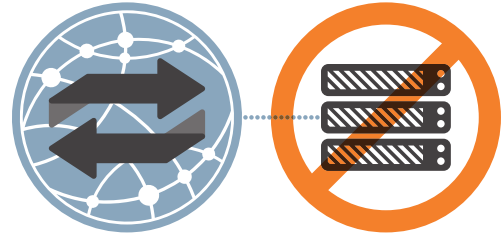
78% of organisations recognise 'strong correlation' between network security and their ability to satisfy government-mandated information security requirements (compliance)



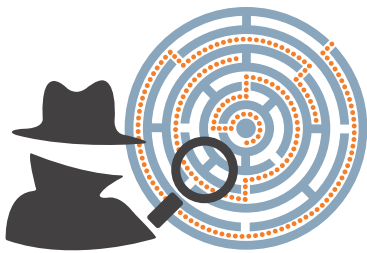
84% of respondents have concerns about their incumbent vendors' abilities to manage 10Gb/s throughput environments



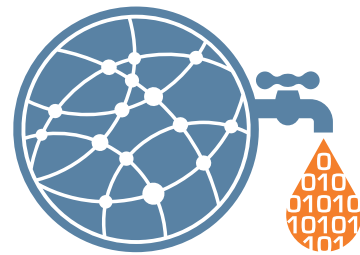
47% of respondents believe that they are missing potentially significant network events due to failing or under-performing systems



65% of organisations surveyed do not record network traffic for the purposes of forensic analysis of network events



43% of organisations report experiencing "significant difficulties" investigating and remediating network events



33% of organisations reported experience with some kind of data loss in the past 12 months, with 39% being unable to accurately identify what was lost



42% of organisations admitted to having been the victim of a cyber-attack in the past 12 months, with 67% of those admitting to serious problems investigating the attack.

HEADLINE RESULTS

The aggregated results of this survey reinforced much we already suspected about the high-speed / ultra-high-speed network monitoring and recording market opportunity:

78% of organisations recognise ‘strong correlation’ between network security and their ability to satisfy government-mandated information security requirements (compliance)

84% of respondents have concerns about their incumbent vendors’ abilities to manage 10Gb/s throughput environments

47% of respondents believe that they are missing potentially significant network events due to failing or under-performing systems

65% of organisations surveyed do not record network traffic for the purposes of forensic analysis of network events

43% of organisations report experiencing “significant difficulties” investigating and remediating network events

33% of organisations reported experience with some kind of data loss in the past 12 months, with 39% being unable to accurately identify what was lost

42% of organisations admitted to having been the victim of a cyber-attack in the past 12 months, with 67% of those admitting to serious problems investigating the attack.

HEALTH WARNING

Endace is a vendor that traditionally sells into relatively niche markets. We commissioned this research to help us understand whether the problems we are exposed to on a daily basis in the industries in which we work are prevalent in other industry verticals where we don’t have such deep visibility. It was not, and is not, our intention to hide the fact we are a vendor from either survey respondents or readers of this report. We feel it’s essential to provide full disclosure on all aspects of this survey so that readers can judge for themselves the validity of our findings and make their own assessments as to its value.

CONCLUSIONS AND IMPLICATIONS

1. Security blindness is real, it’s a problem and it’s getting worse not better.

The number of respondents that admitted to network security blind spots is worryingly high. In today’s climate, organisations have a moral, legal and commercial obligation to their customers to protect their details (not to mention their own corporate IP) and that requires investing in the right systems and tools to ensure that security blindness is minimised.

The fact that organisations aren’t, for whatever reason, embracing the concept of network recording is equally concerning. Conscious awareness that you’re missing threats is one thing, but not having the ability to go back

in time and find out what you’ve missed after the fact is quite another.

We strongly advocate that organisations regularly audit the performance of their network security systems to find out exactly what they can and can’t see. The tools to accurately test the true breakpoints of network security systems (IDS and IPS) exist in the market today and organisations that knowingly elect not to do this are arguably being negligent. In addition, the tools to accurately record network traffic (as part of an integrated security solution) exist and have proven themselves to be an extremely powerful way of providing post-security attack forensics, including the ability to understand what data may have been lost and how.

2. Scalability is the next big battle ground

The volume of data being carried by data networks is exploding. At the same time, the time-sensitivity and criticality of data (think VoIP) is also growing, but the industry’s ability to provide solutions that can keep up appears to be severely challenged. What’s of most concern is that the amount of data being carried and organisations’ ability to deal with it appear to be diverging, rather than converging. Our survey clearly indicated that many vendors are already struggling to meet the demands of true 10Gb/s environments, while many organisations are already developing solid plans to deploy 40Gb/s and 100Gb/s networks inside the next investment period (for some this will happen before their next planned cycle of system refreshes). This should be ringing alarm bells for organisations. They need to be asking challenging questions of their incumbent vendors about their 40Gb/s and 100Gb/s roadmaps now, rather than waiting until it’s too late to find out that their ‘strategic partner’ vendor has nothing to offer that will scale to 40Gb/s and beyond.

A big part of the problem faced by organisations is system fragmentation and a lack of compatibility and integration between disparate monitoring systems. In our view, there’s only one way to provide the levels of required visibility across a network and that’s to deploy a single pervasive monitoring and recording fabric that captures a perfect record of every



packet at strategic points across the network. With the right fabric, organisations can select the tools that work for them, in the knowledge that their selected monitoring tools will see every single packet.

3. Data loss is more common than you think

What the media gets hold of and what's really happening are turning out to be two quite different things. In this survey, 33% of organisations admitted data loss and nearly 40% admitted to having serious issues remediating their losses. That's serious cause for concern in our opinion. Organisations cannot expect to maintain trusted, on-going relationships with their customers if they are not able to guarantee the protection of sensitive customer information. Simply meeting compliance requirements (e.g. PCI, HIPAA, SOX, PCI) is no longer sufficient. Organisations must have a robust information security policy, and teams that work cross-functionally with the right tools that enable them to protect what matters. In addition, organisations need to think very carefully about how to respond when systems are compromised.

The reality is that malicious attacks on corporate infrastructures aren't going to stop anytime soon and there's no way that organisations can fully protect themselves against every type of attack all of the time. Of course, organisations need to do everything that they can to prevent exploits occurring in the first place, but they also need to recognise that at some point they will get breached and they will have to clean up afterwards. The ability to replay and recreate attacks on critical systems is fast becoming an essential part of the corporate security tool kit and the costs of this infrastructure pales into insignificance when compared to the true financial, brand and reputational costs of a breach are considered.

4. Risk, reputation & reward are the driving force for change

There's an indisputable relationship between the tools and organisation uses to measure, monitor and protect its network and that organisation's ability to manage and protect its corporate reputation in the marketplace. The recent spate of attacks at the hands of LulzSec has provided ample evidence of this. This and other high-profile security breaches are causing organisations, at the most senior levels, to wake up to the risk that failing to adequately protect their critical network assets from attack can have severe and potentially catastrophic implications for share price, brand reputation and even, in the most severe cases, personal liberty. What's encouraging is that organisations are starting to recognise that the network and the tools that protect it are within their circle of influence and are actively trying to do something about it.

The reality is that being 'Good enough' is no longer good enough. Enough said.

An exercise we do with many customers is to encourage them to build a traffic usage x time graph that plots data volumes over the past five years and then extrapolates it out over the next five years. With this information organisations can see (with surprising accuracy) at what point they will saturate their various vendor systems and when they will need to look for alternative solutions.

At speeds over 3Gb/s software-based packet capture solutions start to become vulnerable to packet loss due to processor clock-speed limitations. In our experience, at speeds over 3Gb/s the only truly reliable way to ensure that the application sees every packet is to deploy a purpose-built, hardware-based packet capture solution.

ABOUT ENDACE

Endace manufactures ultra-high-performance network monitoring and recording systems that form the basis for network security and monitoring solutions. The Endace Platform, on which all Endace Systems are based, guarantees to capture 100% of traffic from the network and make it available to a range of network monitoring and security applications. Our technology is used by some of the largest organisations in the world to measure, protect and monitor some of the most complex networks on the planet.

Endace Systems scale from 10Mb/s to 100Gb/s and incorporate a number of native applications, including a high-performance network intrusion-detection system, a market-leading network analytics and visualisation system and the ability to capture every packet to local disk for retrospective forensic analysis and investigation. Sitting

alongside that native functionality is a high-performance virtual application hosting environment – Application Dock – that enables organisations to deploy up to six different monitoring and security applications of their choice on each System, all leveraging the same source of 100% accurate captured network traffic.

When deployed as part of a network-wide monitoring and recording fabric, Endace Systems provide unparalleled visibility into all aspects of network activity. They enable organisations to reduce the data centre footprint of their network monitoring, recording and security applications and improve their performance by ensuring each application can see every relevant network packet.

Only an Endace Monitoring and Recording Fabric gives you the ability to see everything on your network.

For more information on Endace products visit www.endace.com or email us at info@endace.com