opinion piece

dimension data

Network Access Control Set to Reclaim its Place on the Corporate Agenda

While the buzz around it may not yet have reached full volume, the signs indicate that Network Access Control (NAC) is poised to lift itself out of the trough of disenchantment into which it fell several years ago.

Business have long-acknowledged the need to protect their networks from the uninvited. NAC, sometimes referred to as identity based security, made its debut around 2004 as a tool for businesses to keep out unwelcome network 'guests'. NAC involves leveraging the network to enforce policies that ensure that incoming devices are compliant and users are authenticated. For example, it ensures that devices that are inappropriately patched with the correct security features such as anti-virus and anti-malware are disallowed from accessing the network. Similarly, it makes certain that only authenticated users are able to log onto the system and it further assigns access rights to individuals according to their roles and responsibilities within the organisation. Then, based on the respective risk profiles of devices and users, they are allocated to a specific 'zone' on the network. In this way, organisations can mitigate risks by controlling communications across their various virtual network environments.

While it sounded good on paper, NAC initially failed to deliver to the expectations of the market, and adoption has remained more or less flat over the last several years according to a recent Gartner report*.

What went wrong?

The reasons are many. Early adopters of NAC solutions acknowledged the problem that the technology sought to address … but encountered a plethora of obstacles along the road to implementation. A key challenge was cost. Concerns about the effect on desktop, laptop or network usability (ease of use) as well as the complexity of solutions in heterogeneous network environments added further frustration. Vendor lock-in was another thorn in the side of early adopters, and many objected to being shoe-horned down a particular technology path depending on the nature of their installed base.

> "It just became too complicated, both for the administrator and for the user," explains Wim Cos, Dimension Data's Business Development Manager for Security Infrastructure in Belgium.

> "Organisations felt that their users shouldn't need to be burdened with such complexity and that the technology shouldn't be so difficult to administer. Many businesses bought into a lot of early marketing hype and subsequently decided to take a step back and reconsider if the choices they made several years previously were still serving them well."

NAC is back – why now?

While NAC may have fallen from favour amongst security professionals some years ago, increasingly, organisations are eyeing the new generation of identity based security technologies with renewed interest as they grapple with the realities of a mobile workforce, ubiquitous connectivity and the myriad of connecting devices crossing the threshold of the corporate perimeter.

> "Six or seven years ago, we didn't have the heightened awareness of the risks of revenue loss and damage to corporate reputation associated with data leakage," says Cos.

> "If you consider today's threats, the risks are very different. Attacks are better targeted and are multiplying rapidly."

The drive towards a more mobile workforce has also fundamentally changed the game. Today, employees want and expect to use their Apple iPads®, smartphones and tablets both at the office and while on the road. More and more, businesses are turning towards technology to stay ahead of their competitors and increase time to market with new products. By giving employees remote access, businesses can boost productivity and customer service levels and inject agility into their business model. By opening up their networks to partners, suppliers and customers companies may gain competitive edge.

While joining the mobile movement may be good for businesses, increased mobility also brings increased risk. The growing use of social networking and video-sharing websites within businesses has increased network exposure to viruses and malware. Add into the mix the rise of cloud computing, which involves devices being physically abstracted from data and applications, and you have a situation where the corporate network is potentially being laid bare to a host of new security threats.

> "Simply put, organisations have recognised the need to redefine their security approaches and that NAC is now something they cannot afford to do without," explains Cos.

> "NAC provides a means to open up the network and address evolving the business needs in a mobile age. Organisations realise that simply disallowing the use of mobile devices is not the way to create competitive advantage and attract talented people. NAC empowers IT to make sure that users' expectations can be met in a controlled and secure way. There's also lot more to choice from a product perspective in the market today and vendors have refined their NAC offerings to cater for greater levels of interoperability and automation."

*Gartner Magic Quadrant for Network Access Control, Lawrence Arans and John Pescatore, 2010,

NAC involves leveraging the **network** to **enforce policies** that **ensure** that **incoming devices** are **compliant** and **users** are **authenticated**.

Debunking NAC myths

Despite this progress, what NAC is or is not supposed to be remains unclear in the minds of many IT decision-makers. So let's debunk a couple of the most common NAC myths:

Myth #1: NAC is only a concern for the network team

The risk from threats and ever-increasing mobility of the workforce are concerns for numerous teams within an organisation. Each area has particular NAC problems that need to be solved. So a NAC solution must be versatile enough to address each of these issues.

Security personnel need to identify security risks, control access, while ensuring network performance and availability. Desktop teams must ensure computer health and compliance to maintain user and business productivity. Network teams must stop any unwanted access to the network. They need a solution that works today – without network upgrades.

Myth # 2: Employees must all adhere to the same NAC policy

Today's more sophisticated NAC solutions give businesses the ability to define security and acceptable use policies. It also allows them to specify enforcement actions for discrete user groups. For instance, you can create a policy that ascertains whether your executive teams' antivirus is always up to date, and if it is not, you can update it without even having to knock on their office doors.

You can even create different policies for contractors, consultants and guests. A NAC solution with user-based policy definition provides you with the flexibility to create as many distinct security and acceptable-use policies as you desire.

The way forward

No network is airtight. Despite security teams' best efforts, malware continues to find its way in. Even organisations that adhere to best practices can be struck.

The good news is that the next generation of NAC solutions represent highly advanced, resilient, dependable business tools that offer a sophisticated experience and high levels of interoperability. Technology, business and consumer trends have evolved significantly and all the signs indicate that the market has reached the right level of maturity … and that NAC is set to reclaim its place on the corporate agenda.

That said, organisations considering setting off down the NAC path should not underestimate the importance of proper planning. They need to consider all the technology touchpoints within the organisation, interoperability issues and proactively plug any gaps that could compromise the success of the deployment.

> "For these reasons, many organisations that are weighing up the merits of a NAC deployment opt for Dimension Data's Adaptive Secure Infrastructure Assessment," explains Cos.
>
> "This service provides a succinct but comprehensive vision of the needs of the organisation in terms of the most appropriate technical solution as well as a thorough gap analysis with respect to refinements to the environment that are required to migrate to the new solution. It's a very interactive process and involves interviewing employees from various areas of the business and IT in order to gauge all user profiles and requirements."

Steering ahead – securely

NAC is re-emerging as a key tool for keeping potential attackers off business networks, as well as for managing the more complex web of permissions and authorisations needed for different groups of users and devices to access parts but not all of a network. Given its somewhat chequered past, NAC still has some work to do to prove itself and become fully mainstream. If you are considering testing – or re-testing – the waters of NAC, you don't have to go it alone … remember, there's no shame in hiring an external entity to help, specifically one conversant in a wide range of technology domains beyond just security, and backed, of course, by a sound track record.

About the Adaptive Secure Infrastructure (ASI) Assessment

The ASI Assessment is a consulting framework that Dimension Data applies to assist clients to prepare for a successful NAC rollout. The methodology enables organisations to plan, design and implement secure infrastructures. It is based on the premise that secure infrastructures are supported by four discrete pillars: Identification, classification, isolation and control, ie:

- Connecting devices are CLASSIFIED into the right virtual network environment based on their IDENTITY (i.e what type of device, to whom it belongs and from where it is connecting) and integrity
- Connecting users are CLASSIFIED and according to their role and what type of device they are using
- For each class of risk, a virtual ISOLATED network environment is instantiated
- Risks are mitigated by CONTROLLING communications across virtual network environments

dimension data

MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • CONGO
DEMOCRATIC REPUBLIC OF THE CONGO
GABON • GHANA • KENYA
MADAGASCAR • MALAWI
MAURITIUS • MOROCCO • NAMIBIA
NIGERIA • SAUDI ARABIA
SOUTH AFRICA • TANZANIA • UGANDA
UNITED ARAB EMIRATES • ZAMBIA

ASIA

CHINA • HONG KONG
INDIA • INDONESIA • JAPAN
KOREA • MALAYSIA
NEW ZEALAND • PHILIPPINES
SINGAPORE • TAIWAN
THAILAND • VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES • QUEENSLAND
SOUTH AUSTRALIA • VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM • CZECH REPUBLIC
FRANCE • GERMANY
ITALY • LUXEMBOURG
NETHERLANDS • SPAIN
SWITZERLAND • UNITED KINGDOM

AMERICAS

BRAZIL • CANADA • CHILE
MEXICO • UNITED STATES

For contact details in your region, please visit **www.dimensiondata.com/globalpresence**.

www.dimensiondata.com