

Cisco and Dimension Data



With a relationship that spans over 20 years and extensive experience in planning, building, supporting and operating large complex networks, Dimension Data and Cisco offer solutions that help clients achieve self-defending and secure infrastructures.

The Partnership

About Cisco:

Cisco, founded in 1984 and headquartered in San Jose, USA, is the worldwide leader in networking that transforms how people connect, communicate and collaborate.

Today, with more than 57,000 employees worldwide, the tradition of innovation continues in the company's core development areas of **routing** and **switching**, as well as in advanced technologies such as IP Communications, Wireless LAN, Storage Area Networking, Video Systems and IT Security.

- ▲ Cisco has over 70% market share in routers and switches worldwide
- ▲ Cisco is one of a handful of vendors rated as "Positive" by Gartner in their report "Marketscope for NAC, 2007"

About Dimension Data:

Dimension Data has more than 10 years experience in the Global Security Solutions market and employ in excess of 350 security experts around the world.

This expertise, in combination with more than 20 years experience in planning, building and managing complex network infrastructures, puts Dimension Data in an optimal position to successfully build security solutions into clients' IT strategies.

- ▲ Dimension Data has more than 5,000 security clients worldwide
- ▲ In 2006 Dimension Data was named Cisco Security Partner of the Year in Germany, Belgium, Luxembourg, India and the UK.

Joint success:

Mazda Australia needed to consolidate and improve its IT security management infrastructure while remaining fully compliant with auditing requirements. Dimension Data was able to recommend an integrated solution that worked with Mazda's existing IT infrastructure, based on the Cisco Security MARS (Monitoring, Analysis and Response System) appliance. The new system was installed and configured with no disruption to Mazda's operations, not only freeing up in-house IT staff to work on value-adding projects but also providing all the necessary information to meet audit requirements.

Dimension Data's Secure Infrastructure

The classic security defence model focused on defending the 'trusted' internal network from the 'enemy' outside. This won't work for today's corporate network.

The only way to protect yourself is to integrate security into all your technologies and devices. By building an inherently secure and adaptable network, using Cisco's market leading technology and Dimension Data's expertise, you can protect your organisation against multiple threats on numerous fronts.

To achieve a **Secure Infrastructure** we believe organisations need to incorporate the following functionality: Content Security, Access Management, Perimeter Security and Intrusion Management. Cisco Integrated Services Router (ISR) is an example of a device that incorporates a wide variety of core functions.

Cisco Integrated Services Router (ISR)

Cisco Integrated Services routers embed comprehensive security services and by combining proven Cisco IOS Software functions and LAN/WAN connectivity with network security features, they enable organisations to:

- ▲ Add new security features on the router through Cisco IOS Software without deploying additional hardware
- ▲ Apply security functionality, such as firewall, intrusion prevention (IPS), and VPN, anywhere in the network
- ▲ Deploy best-in-class security functions at all entry points into the network
- ▲ Reduce the number of devices and lower operational costs
- ▲ Protect routers from attacks that are targeted directly at the network infrastructure such as distributed denial-of-service (DDoS) attacks



Cisco and Dimension Data



Content Security

Data remains an organisation's most valuable asset. Research estimates that the combined value of data/ intellectual property exceeds the value of the organisation. Organisations should therefore be cautious and take an information-centric approach: protect yourself from malicious content entering and being stored on your network, or confidential information leaving your network.

Cisco Adaptive Security Appliances (ASA)

Cisco ASA Appliances is a modular appliance that can adapt as an organisation's needs evolve, giving businesses the ability to integrate intrusion prevention, antivirus, antispam, antispysware, URL filtering, and other advanced content security services for additional layers of protection.

Cisco ASA Appliances are built on the market-proven capabilities of the Cisco PIX® Family of security appliances and its features include:

- ▲ Flexible policy capabilities that prevent unauthorised access to network resources or vital corporate information
- ▲ Advanced application control capabilities that help businesses effectively control the use of peer-to-peer file sharing, instant messaging, and other non-corporate applications-thus improving employee productivity and reducing wasted Internet bandwidth

Access Management

In the old days, organisations could rely on passwords to protect their IT assets from access by unwanted outsiders. Passwords alone are no longer effective enough as access requirements become more role based and granular. Furthermore, with the increase in mobile workers, it has become extremely difficult to ensure that the devices they are using to gain access to the network have appropriate versions of patches installed to meet security policies and not pose a threat to the organisation.

Cisco NAC Appliance

Cisco NAC Appliance is a Network Admission Control (NAC) product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With NAC Appliance, network administrators can authenticate, authorise, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and also repairs any vulnerabilities before permitting access to the network.

Cisco NAC Appliance extends NAC to all network access methods, including access through local area networks (LANs), remote-access gateways, and wireless access points. Cisco NAC Appliance also supports posture assessment for guest users.

“Cisco and Dimension Data share the vision of security as an integral part of any IT infrastructure. As a systems integrator, Dimension Data offers organisations a combination of technical excellence and focus on customer success – a great value add to Cisco's leading technology”

Susan Don, Director WW Channels - Security



Cisco and Dimension Data



Installation, Integration and Support

Dimension Data has been a Cisco Gold Partner on five continents since 2000 and leveraging our unrivalled skills and experience around Cisco technology, organisations can look to Dimension Data to plan, supply and deploy their overall IT environments. across multiple regions.

A good place to start - Secure Cisco IOS Network Assessment

Enterprises running the Cisco Internetwork Operating System (IOS) – the operating system that drives the majority of routers and switches – need to be aware of the increase in potential vulnerabilities in IOS-based devices.

Secure Cisco IOS Network Assessment is a network and security assessment service that discovers, catalogs, and provides remediation recommendations for Cisco hardware and software.

The service ensures that organisations do not expose themselves to unnecessary risk by keeping products up to date and assisting with the alignment of their Cisco estate to configuration, security, and patch management best practices.

Implementing Cisco NAC - Dimension Data's Adaptive Secure Infrastructure (ASI) Framework

Dimension Data's ASI Framework is both a consulting methodology and risk management framework, ideally suited for implementation of NAC Appliances, overall information security policies and improved risk management.

The ASI framework is designed around a four-phased approach:

- ▲ **Identification** – Dimension Data analyses the existing environment to establish the number of users, systems or even applications connected to it. Such elements as computer, user role, health status, access method and location are part of the identification process and together they form the 'entity'. This phase is critical to achieve control based on context and relationships, which is the end goal.

- ▲ **Classification** – Dimension Data defines risk profiles for each entity. The classification process takes a series of factors into account, such as the protection mechanisms deployed at the entity and the value of the data that will be accessed. Based on the identity of the entity and a risk profile, an appropriate corporate information security policy is developed.
- ▲ **Isolation** – Entities are separated into different groups, based on their risk profiles. Entities with similar profiles are not authorised to communicate with entities with a different profile. The same segregation is further utilised to separate entities with similar profiles to reduce the propagation of any threat and the implementation of end-to-end security.
- ▲ **Control** – The system is secured by implementing appropriate and specific security measures within the overall IT architecture. Targeted control is applied to all flows of data which are scanned and filtered by the appropriate security tools.

Contact us:

Raoul Tecala – Dimension Data: raoul.tecala@us.didata.com

For more information, please visit: www.dimensiondata.com or www.cisco.com

Did you know? Dimension Data employs in excess of 350 security experts around the world, including BS7799 Lead Auditors, 35+ CISSP's, 50+ CCSA certifications, 60+ CCSE certifications.

