



## Fully secured Cisco solution helps Austrian aircraft specialist maintain altitude over rivals

International airplane manufacturer Diamond Aircraft, specialising in advanced single-seater planes, is poised to reach new heights when its first jet takes off in 2008. The company started in Austria but has since opened plants in Canada and China. It has a very fast engineering and design development cycle, at about one-fifth of the time taken by most companies to launch a new plane. It needed a total security solution to protect its data, its network and – above all – its hard-won market lead.

### EXECUTIVE SUMMARY

#### Customer Name

Diamond Aircraft Industries GmbH

#### Industry

Manufacturing

#### Business Challenges

- Protect valuable intellectual property for advanced aircraft design projects
- Maintain market position based on a fast engineering development cycle
- Create high-security production model for use in other plants abroad

#### Solution

- Phased implementation plan starting with upgrade to an all-Cisco network
- Cisco Security Manager strengthening Cisco PIX solution with firewall and VPNs
- Upgrade to full Cisco security monitoring system with network admission control

#### Business Results

- Integrated security for fast-track development work to keep ahead of competition
- High network availability sustains project productivity as staff numbers grow
- Security solution template for future implementation in Canada and China plants

#### Business Challenges

Taken over in 1989 by CEO Christian Dries at Wiener Neustadt, near Vienna, Austria, Diamond Aircraft serves the global aviation market. It aims to combine peak performance with lightness and elegance of design, using ultra-modern composite construction methods based on fibreglass and carbon fibre, intelligent avionics, and new engine technologies that can cut fuel consumption by up to 40 per cent.

Its product range includes three single-engine propeller-driven and one twin-engine model and, from 2008, a new single-engine jet. To date, the company has shipped more than 3,500 planes worldwide. Diamond Aircraft is growing at home and abroad, with its Austrian complement increasing from 600 to 1,400 employees worldwide.

Diamond's Chinese joint venture is intended to serve the entire Asian market. It also has a distribution plant and maintenance hangar in Germany, as well as a general agency for England and Ireland offering similar service facilities in the UK.

Diamond has developed a fast-track design and development process, taking on average two years instead of the ten that is more usual in the aircraft industry. For a company at the cutting edge, total data security is vital to future success. The risks of industrial espionage, as well malicious hacking and other

external threats, are high – and the costs could run into tens of millions of euros. When Diamond Aircraft wanted to ensure it had the very best security on the market, it turned to Cisco as the company most capable of providing a complete, end-to-end security solution.

**“In the airplane business, it generally takes about ten years to conduct the engineering and development for a new plane. At Diamond, the time taken is approximately two years. It's a great success to build airplanes in such a short time, but it's also dangerous in terms of rival companies spying on us and other threats.”**

—Hans-Peter Planer, Head of IT, Diamond Aircraft

### Solution

From the time he arrived at the company early in 2005, Diamond Aircraft's Head of IT, Hans-Peter Planer, was set on a Cisco solution to fulfil the company's network and data security needs at its Austrian plant. His first move, working with an international partner, was to strip out all non-Cisco components from the network. The project began with the replacement of ten switches, using mainly Catalyst Series 3750 switches with some Catalyst Series 3560s, to lay the foundation for a new, in-depth security solution. The main value of the change was in creating an integrated Cisco network.

At that point, the company's network and data security was based on the Cisco PIX 500, an effective appliance-based approach capable of providing multiple integrated security and networking services. When a new partner, the European integrator and security specialist, Osiatis was chosen to take the network on the next level, Hans-Peter Planer opened discussions on the value of an even more comprehensive solution. This would employ Cisco's Self-Defending Network framework at Diamond and ultimately use the full resources of Cisco's Security Monitoring, Analysis and Response System (MARS).

Hans-Peter Planer explains: “In the airplane business, it generally takes about ten years to conduct the engineering and development for a new plane. At Diamond, the time taken is approximately two years. It's a great success to be able to build airplanes in such a short time, but it's also dangerous in terms of rival companies spying on us and other threats.” A company whose development cycle is up to eight years ahead of competitors is a natural target for data theft by third parties for clandestine sale to unscrupulous rivals.

The Cisco Self Defending Network is a long-term strategy to protect an organisation's business processes and data security by identifying, preventing, and adapting to threats from both internal and external sources. This protection helps organisations take better advantage of the intelligence embedded in their network resources, thus improving business processes and cutting costs. It has three principal characteristics:

- Integration of security throughout all dimensions of the network
- Collaborative processes between the various security and network elements
- The ability of the network to adapt to new threats as they arise.

By the autumn of 2005, in collaboration with Osiatis, the company was ready to start adding further Cisco components that would be essential to enhance its defences. These included three Catalyst 2960 Intelligent Ethernet switches, offering integrated security with the further possibility of switching on Network Admission Control (NAC) capabilities at a later date; a content engine, permitting secure web-caching as well as increasing productivity; and one more Catalyst 3560 switch with 48 ports.

**“With Cisco Security Manager, we can split the office area from the secure area. Access to the secure files used by the development team is forbidden in Outlook – it's not possible for people to send any files from the secure environment.”**

—Hans-Peter Planer, Head of IT, Diamond Aircraft

Two more Catalyst 3750 switches were installed in early 2006 to improve operating efficiency in Diamond's Austrian LAN. In addition, the new switches were intended to enhance virtual segmentation of the LAN into VLANs, thus enabling Diamond to segregate its secure design areas from general office functions without needing to install separate computer networks or create separate domains.

By July 2006, it was time to embark on the next key step. This consisted of implementing Cisco Security Manager, a powerful but easy-to-use solution for central provisioning of all aspects of device configurations and security policies for Cisco firewalls, VPNs and Intrusion Prevention Systems, coupled with Cisco Security Agent software, which protects server and desktop systems by identifying threats and preventing malicious behaviour. It mitigates new and evolving threats without requiring reconfigurations or emergency patch updates, providing robust protection with reduced operational costs.

Both the Security Manager and Security Agent applications were expected to go live by the beginning of October 2006 after the proving and testing periods were completed. “With Cisco Security Manager, we can split the office area from the secure area,” comments Hans-Peter Planer. “Access to the secure files used by the development team is forbidden in Microsoft Outlook – it's not possible for people to send any files from the secure environment.”

Another key aspect of this stage in Diamond's network evolution was to install two Cisco Secure Access Control servers, which enable a centralised identity networking solution with a simplified user management experience across all Cisco devices and security management applications.



Finally, Osiatis added a CiscoWorks LAN Management Solution (LMS), with a suite of powerful management tools to simplify the configuration, administration, monitoring and troubleshooting of Cisco networks. LMS integrates these capabilities into complete solution for improving the accuracy and efficiency of operations staff, increasing overall availability of the network through proactive planning, and maximising network security.

**“We need solutions offering a very high level of security, which we are also developing for our plants in Canada and China. Cisco makes it easy for us to protect the data and the networks”**

—Hans-Peter Planer, Head of IT, Diamond Aircraft

### Business Results

Once the Cisco Network Admission Control and Cisco MARS capabilities in Diamond's network are switched on, the aircraft company will have in place the most up-to-date and fully integrated network security solution currently available. Network Admission Control is a Cisco-sponsored industry initiative which uses the network infrastructure to enforce security policy compliance on all devices attempting to access network computing resources, while Cisco MARS (Monitoring, Analysis and Response system) recognises and correlates actual network attacks and then defines how to stop them.

These final elements will provide an exceptionally powerful defence in conjunction with Cisco Secure ACS, which functions as a policy decision point in NAC deployments by evaluating credentials, determining the state of the host, and sending out per-user authorisation to the network access devices. While Diamond acknowledges that its security requirements are very high, it is far from the only company – or indeed the only industry – where the potential threats of network attack and industrial espionage need to be neutralised in the most effective way possible. Both are on the increase.

In the context of Diamond Aircraft, the vital importance of strong security will be underlined when the company establishes VPN connections to Canada, China, England and Germany. At present, each site works on discrete engineering and development projects, so there is no need for remote collaborative working between engineering teams based on different continents. However, the company is taking its first steps towards sharing of PDF files among project teams on an individual site basis.

“We need solutions offering a very high level of security, which we are also developing for our plants in Canada and China. Cisco makes it easy to protect the data and the networks,” says Hans-Peter Planer.

While the main thrust of the project undertaken by Diamond, in conjunction with its partner, Osiatis, has been directed at improving security, the value of the all-Cisco network has proved itself in other ways. Because Diamond Aircraft has engineered its design and development processes to run much faster than the industry average, it requires a network that is always available and always running at maximum efficiency.

For Hans-Peter Planer, the other key benefit of a Cisco network is the very high level of network availability it assures, coupled with Quality of Service. “It is essential for us to have a highly available network – this is fundamental for our engineers and developers,” he says. “Cisco maintains excellent levels of network availability for our business.”

**“It is essential for us to have a highly available network – this is fundamental for our engineers and developers. Cisco maintains excellent levels of network availability for our business.”**

—Hans-Peter Planer, Head of IT, Diamond Aircraft

### Technology Blueprint

The first phase of the project – an upgrade to an all-Cisco network as an integrated foundation for the security solution – involved installing ten Cisco Catalyst 3750 and Catalyst 3560 Series switches. The next step was to add three Cisco Catalyst 2960 Series Intelligent Ethernet switches, one further Catalyst 3560, and integrate a Cisco CE-511 content delivery engine into the system.

After the addition of two further Cisco Catalyst 3750 Series switches, Osiatis was in a position to move on to the next key phase of the security implementation – the addition of two Cisco Secure Access Control Servers, along with Cisco LAN Management Software (LMS), Cisco Security Manager, and Cisco Security Agent Software. The full suite of up-to-date Cisco security products will be complete with the introduction of Cisco Network Access Control and Cisco MARS.



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)