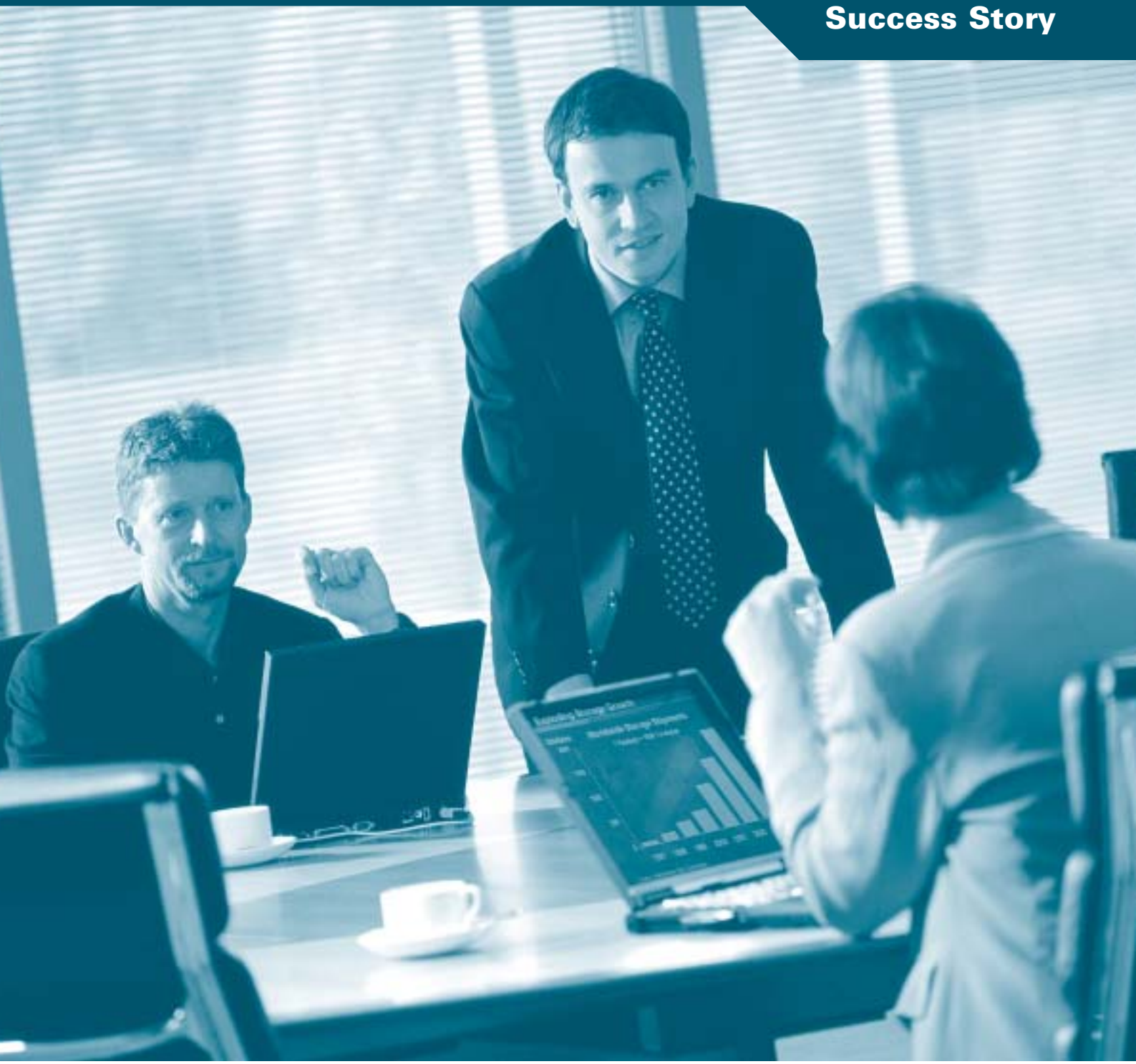
Success Story



The Cisco **Intrusion Detection System** delivers robust security for mission critical eBusiness

Cisco Systems

Background

In 2002 Ipera Information Technology was established with the merger of Hunter Digital and Ipera Network Computing.

Based in the Hunter Valley, Ipera offers a wide range of IP-based services to Newcastle businesses including application hosting, software development, telehousing, hardware and software sales and network management.

Key to their business is the provision of web services to a large number of corporate clients. Ipera have developed a high capacity, robust network delivering fast Internet access, low cost telephony and private data links for corporate Wide Area Networks. To complement this, they provide their customers with a range of services such as the telehousing of servers and a hosted application service and a broadband network at local network speed. Such offerings were previously cost-prohibitive or unachievable over traditional networks.

The Challenge

At the start of 2002, one of Ipera's major clients wanted to progress their business model to incorporate web-based e-commerce. Though the company had a web presence, they had not previously offered their customers the opportunity to purchase products via the web.

One of their major concerns was security. They wanted to ensure that their e-commerce site was protected against Denial of Service (DoS) and general hacking.

Managing Director of Ipera, Chris Deere comments: "Although they wanted a full online e-commerce site where customers could buy securely online in real-time, they felt they didn't have the skills or the solution in place to implement it."

Both Ipera and their client had previously installed a range of different Web servers, which were protected by multiple Cisco PIX firewalls. These provided high levels of security, but no detailed information on attempts made to get past the firewall and if any were getting through.

Ipera provided telehousing for a number of this client's front-end servers on a high performance network connected to the Internet. The back-end data-collection servers were housed with the client.

E-commerce sites tend to attract a higher interest from hackers so Ipera's technical design team knew that the current solution might not be robust enough to prevent an intrusion, especially an undetected one.

"Our client was concerned that a hacker might be able to penetrate the web site undetected, access the core system and either disrupt their business or worse, compromise customer records and payment details."

The client's auditors were also unprepared to back an e-commerce venture without an ironclad security system that would ensure that customer details could never be accessed by a hacker.

In conjunction with Cisco and HP Global Services, Ipera staff spent several months researching what was required to implement a secure end-to-end solution, with a support and service level second to none.

The Solution

In August 2002, Ipera successfully helped launch their client's highly secure e-commerce web site with the technology in place to immediately detect break-ins, track their source, close down attempts and prevent access. This was enabled through the Cisco Intrusion Detection System (IDS) working in tandem with Cisco PIX firewalls.

Ipera and their client are connected via a secure Virtual Private Network (VPN), which provides remote access for Ipera's technical staff so that they can manage the PIX firewall.

The main Network sensor is located at Ipera along with the customer front-end web servers, which are telehoused in Ipera's data centre. The API Server, middleware to run the applications, the backend servers, multiple PIX firewalls and IDS agent sensors are located in the client's server room.

Chris Deere comments: "We looked at two similar products, but we chose the Cisco 4200 Series IDS sensors because Cisco solutions work! They are a trusted supplier and innovator in Internet security technology. Our client also expressed Cisco as a preferred choice because their IDS sensors are purpose-built, high-performance network security 'appliances', that protect against unauthorised and malicious activity such as attacks by hackers.

"Cisco IDS sensors analyse traffic in real-time, processing 45MB data per second, enabling us to quickly respond to security breaches. To do this they use a combination of highly innovative and sophisticated detection techniques, including stateful pattern recognition, protocol parsing, heuristic detection and anomaly detection, that provide comprehensive protection from a variety of both known and unknown cyber threats.

"Furthermore, the Cisco Signature Micro-Engine (SME) allows granular customisation of sensor signatures, resulting in precisely tuned sensors that minimise the occurrence of 'false positives.'

"When unauthorised activity is detected, the sensor can send alarms to our console with details of the activity. The Cisco IDS Active Response System also controls other systems, such as routers, firewalls and switches, and can terminate unauthorised sessions."

Another reason Ipera chose the Cisco solution was the ease of installing and managing of these turnkey appliances. Users have a choice of management solutions, including a Web user interface, a command-line interface (CLI), or Cisco's highly scalable CiscoWorks VPN/Security Management solutions (VMS).

Cisco's IDS sensors can also download hacking profiles and start defending against these kinds of attacks. It can also rewrite the Cisco PIX firewalls on the fly if it detects an unauthorised intrusion.

The Results

"So far," said Chris Deere, "those that have tried to break in have been detected immediately by the Cisco IDS sensors and completely locked out. Our customer is very happy with this solution, as not only is it proving secure, it also generates easy to read reports.

"Each month, we run a diagnostics report which lists all the attacks that have occurred and been prevented. The report also shows various Denials of Service (DoS) such as an attempt to 'flood' the network, preventing legitimate network traffic from accessing the site.

"The DoS reports also provide us with a clear idea of what could have happened without the Firewall in place."

One of the biggest benefits the customer has noticed is the raised awareness of security issues, leading to increased professionalism among staff.

Staff at Ipera also appreciate the flexibility of the Cisco solution that enables them to reconfigure routers and the firewalls on the fly, to increase security even while an attempted intrusion is in process.

> "For the customer, the key result has been peace of mind – and it is certain they would not have proceeded with an e-commerce solution without this high level of robust security in place."
>
> *Chris Deere, Managing Director, Ipera Information Technology*

Chris Deere comments: "For the customer, the key result has been peace of mind – and it is certain they would not have proceeded with an e-commerce solution without this high level of robust security in place."

Partnerships

When implementing an e-commerce solution to one of his biggest clients, Chris Deere at Ipera knew he needed reliable strong partnerships and proven security architecture. With Cisco Systems and the assistance of HP Global Services Division, he had both.

"This was a major installation, and yet it was achieved in a short timeframe with only minor glitches," Chris commented. "When issues did arise, both Cisco and HP Global Service Division responded promptly and were able to resolve them quickly. The HP Global Service Division all hold Cisco Security certifications and our team at Ipera are raising the level of their skill sets and expertise to match. They are all keen to get Cisco Security Certification to meet the growing demand for these kinds of implementations.

"By choosing Cisco I had the peace of mind of knowing I was in partnership with a company that had a strong, viable solution and one that had already been proven at many high-profile, highly secure sites. With something as critical as security it's vitally important to have the backing of quality solutions and support, such as those offered by Cisco."

Corporate 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: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe