DATA LOSS PREVENTION INFORMATION SENSITIVE SYSTEMS NETWORK STORED LEAKAGE

Case study: Symantec helps enterprises prevent data loss

Challenge

Today, enterprises increasingly recognize the need for security as the amount of data generated and gathered increases exponentially. The necessity of protecting intellectual property (IP) and customer information is a huge, if not the top, priority amongst IT executives. But as we use devices and networks outside of IT's control, the risk of data loss increases dramatically. Not only do the number of data sources increase, but the amount of data to be monitored also grows dramatically. The task of gathering data and assessing data loss becomes increasingly difficult.

Solution

Symantec is acclaimed by Gartner's Magic Quadrant as a leader in Data Loss Prevention (DLP) solutions. Their Network Monitor allows an enterprise to assess exactly where the data loss lies and define future prevention. The solution passively monitors data traversing the network without impacting daily operations. Powered by Napatech's FPGA-based SmartNIC hardware and software, Network Monitor can reveal the extent of data loss with exceptional accuracy.

Benefits

Napatech SmartNICs ensure that all packets traversing the enterprise network are captured and timestamped with nanosecond precision. Subsequently, Symantec Network Monitor can inspect all relevant data captured and the enterprise can gain a comprehensive picture of its data loss risk.

The benefits of this solution apply across industries:

Case 1

With the emergence of electronic health records (EHR), ensuring patient confidentiality is of the utmost importance in US healthcare. While electronic records help medical practitioners in delivering and streamlining comprehensive services by allowing healthcare facilities to quickly access a person's health history, personal health information (PHI) is mandated by law to remain private via the Health Insurance Portability and Accountability Act (HIPAA).

Unauthorized access to personal health information will not only leak private data (date of birth, social security number), but also diagnoses

Challenge

The risk of data loss increases dramatically as we use devices and networks outside of IT's control. Meanwhile, gathering the data necessary to assess data loss becomes increasingly difficult.

Solution

Powered by Napatech's FPGA-based SmartNICs, Symantec Network Monitor seamlessly and accurately detects confidential data sent outside of the corporate IT network.

Benefits

Powered by Napatech SmartNICs, Symantec Network Monitor provides full visibility into all business communications, enabling identification of any high-risk users that mishandle sensitive information, putting enterprises at risk of data loss.

that legally can only be shared between doctor and patient. If, say, an insurance company requests information from the healthcare provider to verify a patient's coverage, the healthcare provider may, unauthorized, send a patient's unencrypted files to expedite the request. But with Network Monitor in place, this communication would automatically be flagged as non-compliant in real-time, allowing the provider to take immediate action.

Case 2:

In the retail sector, the risk of data loss is easily translated into potential lost revenue, as companies need to protect their IP to remain competitive. With today's biggest retailers serving customers worldwide, they must share IP with numerous local distributors. This exchange must be secured to minimize the risk of data leakage that competitors could abuse to their advantage, e.g. theft.

Envision a scenario where a distributor needs updated pricing for a client meeting but cannot access the pricing repository while in the field. The distributor therefore requests that the retailer sends the information directly via email or ftp, thereby compromising security. Powered by Napatech, Symantec Network Monitor will capture such

instances of non-compliance, thus avoiding that the IP is made vulnerable to theft.

Case 3:

Higher education institutions must also concern themselves with data loss. Take a university generating IP through research sponsored by both government agencies and the private sector. Working under tight budgets, universities may not have the time or resources to implement a comprehensive DLP solution.

Powered by a Napatech SmartNIC, Network Monitor can assess the actual DLP risk in a timely manner. The efficient packet capture allows the university to fully comprehend the extent of the data loss risk, providing the foundation for a DLP architecture and a realistic plan to address issues in both the short and long-term without excessive pressure on time or resources.

For further information on Symantec Data Loss Prevention, visit:
go.symantec.com/dlp

Napatech

Napatech helps companies to reimagine their business, by bringing hyper-scale computing benefits to IT organizations of every size.

We enhance open and standard virtualized servers to boost innovation and release valuable computing resources that improve services and increase revenue.

Our Reconfigurable Computing Platform™ is based on a broad set of FPGA software for leading IT compute, network and security applications that are supported on a wide array of FPGA hardware designs.

Find out more at:
www.napatech.com

Find more case studies at:
www.napatech.com/resources/case-studies