

# Security is Business Issue ... Not a Point Solution



Security is a **revolutionary**, resulting in much of our best efforts to address risks, being reactive in nature. It is possible, however, to get ahead of **anticipated risks** by taking a business decision to **focus security efforts on data**, rather than where it resides or moves. This will give you greater pre-emptive capabilities in preventing its loss.

Security is an issue no forward-looking organisation can afford to ignore. Nearly 90% of malware leverages legitimate sites, particularly news sites and social media. Conventional tools such as URL filtering and signature-scanning simply can't keep up with the fact that thousands of new websites are created every hour. According to Cisco, the daily spam volume doubles every year. There are currently 230 billion spam messages crossing networks every day. According to the US Department of Defence, every 1,000 lines of code contains an average of 15 critical security defects.

It's all too easy to become caught up in the detail. Oftentimes, organisations do not pause long enough to truly understand what to protect, and when and how to protect it optimally. Do you start with your end point devices, some of which is located outside of the organisation's physical boundaries? What about the network itself? What about internal and outsourced processing equipment and storage appliances? Then there are the employees and suppliers that work with your infrastructure – and the authorisation and entitlement management effort they entail. What about web access management for customers and suppliers – and indeed the rest of the extended supply chain?

Perhaps most crucial of all, there's your organisation's data. It's in a constant state of flux, sometimes at rest (in storage), sometimes on the move (across the network), and sometimes being processed (in devices or applications). You need to accelerate to market with products and services that your customers will want to buy. Intellectual property is at a premium – along with the need to protect it.

These are business, not IT issues, which is why the road to effective security management is a one that IT and business leaders need to travel together.

Effective security is about focusing it where it is most needed and integrating it into every business activity. Importantly, this needs to be an ongoing process, not a point solution, given that security mutates. It is seasonal, situational, and company-specific. It is influenced continuously by unexpected, unforced – and therefore highly unpredictable – errors that employees make as it is by malicious electronic intrusion by outsiders and theft of intellectual property by disgruntled employees.

All of which requires that your executive team be willing and able to update and refine its stance on security on an ongoing basis. There will never be a time, in any organisation, when security can be regarded as being 'complete'.

Ironically, when this level of management maturity around security is achieved, the budget devoted to security often decreases. This is because that's when an organisation engages its internal

or outsourced security specialists at the beginning of any operational change. This implies that security is built into any functionality changes from the start; which, in turn, means that security doesn't have to be bolted on as an afterthought. Adding security later, whether it's to a new application written without consideration for coding vulnerabilities or to new video conferencing facilities that are going to save the company a significant amount in travel costs, actually increases the cost of the project. From a business perspective, that's an irresponsible way to manage. No-one would tolerate that from the manufacturing division, or sales. What business logic makes it acceptable in IT security?

Ultimately, effective security comes down to focusing it where it is most needed, incorporating it into everything the organisation does – before it does it, building it on a flexible, dynamic platform that maximises both the organisation's operational and security options, and continuously analysing and assessing it – always from a business perspective.

Effective security is about **focusing it** where it is **most needed** and **integrating** it into every business activity. Importantly, this needs to be an **ongoing process, not a point solution**, given that security mutates.

**MIDDLE EAST & AFRICA**

ALGERIA • ANGOLA  
BOTSWANA • GHANA • KENYA  
MOROCCO • NAMIBIA • NIGERIA  
SAUDI ARABIA • SOUTH AFRICA  
TANZANIA • UGANDA  
UNITED ARAB EMIRATES

**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