

# THE BUSINESS CASE FOR MANAGED NEXT GENERATION FIREWALLS

SIX REASONS WHY  
IT DECISION MAKERS  
SHOULD SIT UP AND  
TAKE NOTICE



## THREATWATCH

- CYBER THREATS COST THE UK ECONOMY 27 BILLION POUNDS A YEAR
- 92 PERCENT OF BREACHES ARE PERPETRATED BY OUTSIDERS
- 66 PERCENT OF BREACHES TAKE MONTHS OR MORE TO FIND AND 69 PERCENT ARE DISCOVERED BY EXTERNAL PARTIES

## YOUR BUSINESS NEVER STANDS STILL AND NEITHER SHOULD YOUR SECURITY

The Security landscape is constantly evolving with threats becoming more sophisticated and targeted. With the rise of apps, mobility and cloud computing your security needs are ever changing. It's no surprise that your first and best line of defence – your firewall - should always be evolving as well to keep up with emerging threats and attack vectors.

A firewall refresh should happen every 3-4 years, but it isn't about adding hundreds of new security features you'll never need. When you refresh your firewall, the end-game isn't just better protection from threats; it's about providing security that delivers real, measurable business benefits. Enter managed next generation firewalls (MNGFs) and six business reasons for upgrading.



## STEP ONE

# SIMPLIFY IT SECURITY FOR BUSINESS AGILITY

Multiple security devices providing multiple functions such as Firewalls, IPS, Content Filtering and Threat Prevention can provide good security, but at a cost. Multiple security devices require multiple support contracts, diverse levels of skills and knowledge. More importantly, each has its own set of metrics and dashboard which limits real end-to-end visibility of data leaving and entering the network at the perimeter. By consolidating multiple security features into a single device, a Managed Next Generation Firewall will reduce hardware complexity; provide greater visibility, reduce TCO and simplify security management.

A unified vendor approach means less complexity, less diversity of skills required and one integrated management interface. With only one platform to configure and monitor for security risks, it's far easier to locate and resolve problems or assess your entire security posture at a glance. With centralised security visibility, what's then needed is continuous monitoring and alerting.

### A FIREWALL FROM ONE VENDOR IMPROVES SECURITY

- THROUGH 2018, MORE THAN 95 PERCENT OF FIREWALL BREACHES WILL BE CAUSED BY MISCONFIGURATIONS, NOT FIREWALL FLAWS
- HAVING TWO DIFFERENT FIREWALL PLATFORMS GREATLY INCREASES THE CHANCES OF HUMAN ERROR AND MISCONFIGURATIONS
- ONE BRAND OF FIREWALL IS A BEST PRACTICE FOR MOST ENTERPRISES THE CHANCES OF HUMAN ERROR AND MISCONFIGURATIONS

GARTNER REPORT: ONE BRAND OF FIREWALL IS A BEST PRACTICE FOR MOST ENTERPRISES, 2012



## STEP TWO

# REAP THE BENEFITS OF EXPERT ADVICE

You know the value of expert knowledge - your business depends on it. So why leave your security in the hands of people who aren't dedicated security professionals, or who don't have time to keep eyes on it at all times?

Expert security management guarantees your next generation firewall is always correctly maintained and configured. Security specialists can also analyse your existing firewall rules and then define new, fine-grained policies that better support your business needs. For instance, allowing access to Facebook, but blocking Facebook games and ensuring there are no duplicate and contradictory rules in force.

Best of all, expert advice is always just moments away. There's only one point of call for supporting your managed next generation firewall and not ten contacts that will play "pass the buck" instead of solving your problem.



## STEP THREE

# REFOCUS IT RESOURCES ONTO STRATEGIC PROJECTS

Firewall management, monitoring and maintenance are essential, but it's also a time-consuming drain on your resources. By out-tasking day to day operations such as policy changes, applying updates and patches, you can free up IT team resources to refocus on projects that deliver real business benefits. From big data to mobility, security should become an enabler of the business not a limitation.

There's also no need for your staff to undergo long, complex training to manage the intricacies of a firewall transition and consolidation of security features. Complex and time-consuming tasks like migrating policies from one platform to another can all be managed externally and expertly.

## 24X7 FIREWALL MONITORING DRIVES BUSINESS BENEFITS

- CONTINUOUS FIREWALL MONITORING BY YOUR SERVICE PROVIDER KEEPS CRUCIAL BUSINESS PROCESSES RUNNING SMOOTHLY
- CHECK THE AVAILABILITY OF ESSENTIAL IT SYSTEMS LIKE DISK SPACE, IN REAL TIME
- REGULARLY TEST BUSINESS CRITICAL ACTIVITIES LIKE PAYMENT PROCESSING AND ORDER RECONCILIATION
- SPOT AN ISP FAILURE

## STEP FOUR

# REDUCE SECURITY INCIDENTS AND BUSINESS DOWNTIME

Modern businesses need continuity and uptime to keep customers happy, employees productive and revenues strong. Unfortunately, new security threats can appear any time of the day or night, when your IT team isn't available. With a Managed Next Generation Firewall, experts are continuously on hand, pro actively detecting threats and mitigating problems. Security specialists can also analyse threats and advise you on the best approach to help mitigate them that's most suited to your business.

Today, most firewall breaches are caused by misconfigurations. This is often due to human error, with teams struggling with the complexity of managing different security appliances from separate interfaces. A single firewall management console significantly lessens the chance of any error, as does 24x7 firewall monitoring by outside security experts.

A Managed Next Generation Firewall doesn't just monitor technology, it can also check crucial business processes are working. For instance, submitting dummy orders to test payment processing and order reconciliation. The firewall also provides detailed reports on a whole range of business systems, from disk space to equipment availability. This means potential issues can be intercepted early on and IT systems are optimised to best support the business.



## STEP FIVE

# SPEND LESS ON SECURITY, BUT INCREASE BUSINESS PROTECTION

It's a security no-brainer: spend less to improve your security, visibility and management. A Managed Next Generation Firewall will not only offer the latest security features but will also deliver major cost savings on hardware, power and cooling, training, support and management.

Out-tasking firewall management also means you don't need to expand your internal IT team to benefit from continuous monitoring and maintenance. Better yet, there's no need to pay for advanced security training for your staff, as you already have immediate access to expert security advice, 24x7.

The reduction in expenditure is dramatic. A SME with 500 users that chooses a consolidated MNGF over a separate firewall, IPS and content filtering solution would save over £60,000 - or 37% of its budget - across three years. For a major enterprise with 3000 users this saving leaps to over £107,000.

### FIREWALL COST COMPARISON: CONSOLIDATION VS. BEST OF

- A CONSOLIDATED MNGF WILL DRAMATICALLY CUT EXPENDITURE OVER THREE YEARS COMPARED TO SEPARATE FIREWALL, IPS AND CONTENT FILTERING SOLUTIONS
- A SME WITH 500 EMPLOYEES WILL REDUCE ITS FIREWALL COSTS BY 37%, SAVING £60,878
- AN ENTERPRISE WITH 3000 EMPLOYEES WILL REDUCE FIREWALL EXPENDITURE BY 10%, SAVING £107,596
- A SINGLE VENDOR RELATIONSHIP CAN YIELD EVEN GREATER DISCOUNTS AND LOWER CONTRACT ADMINISTRATION OVERHEADS

IN SMALL WRITING, PLEASE ADD THE SOURCE BELOW:  
SECUREDATA FIREWALL COST COMPARISON, 2014



## STEP SIX

# SUPPORT BUSINESS TRANSFORMATION TO THE CLOUD

Deploying a MNGF service with cloud-based reporting can showcase the benefits of out sourced IT services to your business: access to specialist expertise, reduced costs, greater efficiency and simplified management.

Once the MNGF is in place and delivering business benefits, your service provider can recommend other security features areas to integrate into the solution such as web filtering or IPS. This is a simple process with no need to purchase or install additional hardware.

It's vital to understand that bringing in Next Generation Firewall technology to your business is only a part of the security picture – rules still need managing, patches need applying and most importantly alerts need to be monitored and remediated. This requires time and expertise. Whilst considering upgrading your security features, think about the bigger picture too. Partnering with a security services provider that understands your business, people and processes will transform not only your technology, but your visibility and ability to detect threats earlier.

# BUSINESS CASE COST ANALYSIS

500 USERS

	PRODUCT	HARDWARE, SOFTWARE SUPPORT	MANAGED SERVICE	TOTAL COSTS	DIFFERENCE	SAVING
NEXT GENERATION FIREWALL WITH CONSOLIDATION	£ 57,187.50	£ 22,843.13	£ 25,515.00	£ 105,545.63	- £ 60,877.50	36.58%
PERIMETER FIREWALL WITH IPS	£ 57,187.50	£ 14,107.50	£ 18,225.00			
CONTENT FILTERING SOLUTION	£ 60,353.13	£ 28,962.50	£ 12,150.00			
		£ 136,048.13	£ 30,375.00	£ 166,423.13		

The following table provides an indication of the likely cost savings that can be achieved based on scenarios of user numbers, and with the assumption of using next generation firewall technology, and deploying additional features.

## 3000 USERS

NEXT GENERATION FIREWALL WITH CONSOLIDATION	£ 579,375.00	£ 215,728.13	£ 184,800.00	£ 979,903.13	- £ 107,596.19	9.89%
PERIMETER FIREWALL WITH IPS	£ 311,731.25	£ 130,808.06	£ 132,000.00			
CONTENT FILTERING SOLUTION	£ 304,462.50	£ 176,337.50	£ 32,160.00			
		£ 176,337.50	£ 164,160.00	£ 1,087,499.31		

Cost analysis numbers are based on current pricing for industry available hardware and software. These costs are indicative and SecureData reserves the right to vary these costs according to individual customer requirements.

## CONCLUSION

Security is a complex challenge and companies need expert partners to extend their capabilities beyond what is possible with in-house resources. A Managed Next Generation Firewall service provides more than just improved security. It turns IT security systems from a necessary evil into a business enabler, helping companies become more cost-effective and agile across every IT function of the organisation.



# SECURE:DATA

SecureData House,  
Hermitage Court,  
Hermitage Lane,  
Maidstone,  
Kent ME16 9NT

T: +44 (0)1622 723400  
F: +44 (0)1622 728580

E: [info@secdata.com](mailto:info@secdata.com)  
[www.secdata.com](http://www.secdata.com)

Follow us on Twitter: [@secdataeu](https://twitter.com/secdataeu)