

NETCONNECT PRIVATE

TOP FIVE BENEFITS OF A FULLY MANAGED SECURITY SERVICE

There are many players and options in the enterprise security market; however, Vertel's ability to deliver a fully managed service allows us to stand out from the crowd. Below are the **top 5 benefits** of going with a fully managed security service over a self-managed option.

Self-Managed Solution	Fully Managed Solution
1. Headcount: no need to employ a dedicated security expert (s)	
<p>A self-managed solution requires the customer to employ a dedicated security subject matter expert(s), incurring upwards of \$100k of cost per person.</p> <p>This person can become a single point of failure in the solution as the personnel cannot physically be available 24/7.</p>	<p>A fully managed service supported by a whole team of experts – providing accessibility to virtual SOC team. This means 'proactive' support 24/7/365.</p> <p>Additionally the chance of human error is greatly reduced as analysis is based on multiple people looking at the logs.</p>
2. Reporting: receive it straight to your inbox	
<p>Generating reporting internally is a time consuming and a tedious manual process. It often requires product expertise which means the team or person requires product expertise and training.</p> <p>The individual in charge of the self-managed service will need to take time out of their schedule to learn, create and distribute this reporting.</p>	<p>Weekly reports as well as customised ones are provided as part of the standard service offering.</p> <p>Any queries are fed back to the provider and do not add to the workload of the customer's ICT team.</p>
3. Financials: no need for huge capital outlay	
<p>A self-managed solution means paying upfront for the hardware, software and required licenses - a significant capital expense (CAPEX).</p> <p>This is then followed by annual maintenance costs for patches, device upgrades and other ongoing costs.</p>	<p>A fully managed solution doesn't require any huge upfront capital outlay. Instead, a singly monthly payment is made which includes all necessary upgrades and patches.</p> <p>This OPEX approach makes it easy to manage budgets without sacrificing the overall solution.</p>
4. Crisis Management: rapid response team on hand	
<p>When crisis strikes (security breaches), it can be any time of day or night. Those running a self-managed service must rely on their sole security expert being available to manage the crisis.</p> <p>The management of the situation is limited by the skills and knowledge of the individual. Getting an external contractor support in will means an hourly cost of at least \$400-\$600 per person. It also involves additional time (means additional \$\$) for evaluating the right contractors and once they are on board, they need to understand the network and security configuration.</p>	<p>A rapid response team is available 24/7/365 as part of the managed service. This team is dedicated to enterprise security and trained to manage the latest threats and attacks by proactive monitoring.</p> <p>In the event of crisis, a team of experts are available at hand for resolution and remediation[*]; this saves time spent on contractor evaluation. Also the team already has knowledge on the network and security configuration; this reduces the learning curve.</p>
5. Maintenance: proactive upgrades to ensure the best protection	
<p>Setting up an enterprise security solution is only the first step. Ongoing maintenance and management of it is required to ensure an adequate level of protection which includes patching, appliance management and signature updates etc.</p> <p>When running a self-managed solution the customer needs to be pro-active at ensuring the SME's knowledge is up to date and they have installed all the latest updates and patched to their solution.</p>	<p>As a standard inclusion to a fully managed service the solution will be kept up to date and properly maintained with the latest updated. No need to worry about patching, appliance management and signature updates; all are included.</p> <p>In addition, you have access to support team who are security certified professionals who undergo ongoing training to ensure they're fully across the latest nuances of the solution.</p>

* Remediation of the problem caused by a security breach or attack incurs additional charges for professional services required for remediation; the number of hours of professional services required depends on the severity of the breach or attack.