Firewall Managed Service
BACKGROUND

Caretower Managed Security Service provides remote managed security services for customers. We have extensive experience of partnership with all major security vendors and provides vendor approved support for a range of security technologies and products.

This document describes our Firewall Managed Security Services for all major vendors' firewalls.

CARETOWER MANAGED SECURITY SERVICE

The Managed Service operates through our SOC (Secure Operation Centre) on the principle of proactive security management, deploying a Network Management System (NMS) that processes notifications and auto-generates tickets for proactive remote management. This facilitates proactive incident management and also incorporates a change management component. Our infrastructure is housed in a hosted environment, in redundant configuration. Connectivity with the customer is achieved by a remote encrypted connection to the managed device(s). Customers can raise tickets by email or phone or by logging onto our Managed Service web portal.

SECURITY OPERATIONS CENTRE (SOC)

Our SOC is manned 24x7x365 by experienced firewall engineers. The SOC is secured with swipe card access control and only authorised personnel have access. Physical and logical access is controlled via a list of authorised personnel. SOC engineers remotely manage and monitor customer devices proactively. Our managed services follow laid down procedures, within the ITIL model.*

*Caretower will not be responsible for failures or degradation beyond our reasonable control, such as customer infrastructure, cabling, telecoms service/equipment, power provision, utility suppliers, ISP etc.

If you would like more information on any of our services, please speak to your dedicated Caretower Account Manager or if you don't have one, email: info@caretower.com
CARETOWER’S SERVICE ELEMENTS

24X7 MANAGEMENT
The Managed Security Services are delivered through our Security Operations Centre (SOC), which operates 24 hours a day, 7 days a week, 365 days a year.

CO-MANAGE
The customer may retain admin privileges to the managed device - if not on a fully managed contract.

SYSTEM AVAILABILITY CHECKS
Caretower SOC is available to monitor and manage security devices 24x7x365.

CONFIGURATION BACKUP
Where possible a configuration backup of the device shall be made.

REPORTING
Monthly reports will be provided for the managed device(s).

PORTAL
A Web Portal is provided to the customer to interface with the Managed Service. The customer CSM/CSO may access the Web Portal through the Caretower Managed Service web site. Access to the Web Portal is encrypted, additional Web Portal accounts can be requested but these incur a one-off charge and should be ordered through the Caretower account manager.
Changes are managed to completion within the change management system, and are requested via the Web Portal. If either Caretower or the customer wishes to make a change to the configuration of the managed device(s), Caretower or the customer shall provide in the request a description of the proposed change.

If Caretower requests a change, the customer shall not unreasonably withhold or delay consent to it, however the customer can reject the change.

If the customer wishes Caretower to proceed with the change, the customer must approve the change.

If Caretower does not proceed with a change requested by the customer, Caretower will document and communicate the reasons why it will not proceed and may provide counter-proposals for the customer’s consideration.

24 changes per year are included in the service, and additional changes in bundles of 10 can be purchased subsequently (£250 per bundle of 10). In accordance with ITIL, non-impact changes do not need to go through change control.

INCIDENT MANAGEMENT

For the purposes of this specification, reference to an 'incident' generally means an incident in ITIL, which is an unplanned interruption to an IT service or a degradation of the quality of an IT service. Reported incidents will be responded to within 30 minutes.
MANAGED FIREWALL SERVICE ELEMENTS

<table>
<thead>
<tr>
<th>Services</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/7 Monitoring</td>
<td>✓</td>
</tr>
<tr>
<td>24/7 Management</td>
<td>✓</td>
</tr>
<tr>
<td>Co-Manage</td>
<td>OPTION</td>
</tr>
<tr>
<td>System Availability Checks Visual management console</td>
<td>✓</td>
</tr>
<tr>
<td>Configuration Backup via management console before and after change implementation</td>
<td>✓</td>
</tr>
<tr>
<td>Reporting</td>
<td>✓</td>
</tr>
<tr>
<td>Portal</td>
<td>✓</td>
</tr>
<tr>
<td>Security Appliance (VM)</td>
<td>OPTION</td>
</tr>
<tr>
<td>Security Appliance (HW)</td>
<td>OPTION</td>
</tr>
<tr>
<td>Rulebase Audit via management console</td>
<td>✓</td>
</tr>
<tr>
<td>Rulebase management via management console, includes 24 changes, with additional bundles of 10 changes chargeable</td>
<td>✓</td>
</tr>
<tr>
<td>Platform Management Operating system and firmware, via management console</td>
<td>✓</td>
</tr>
<tr>
<td>SLA</td>
<td>✓</td>
</tr>
<tr>
<td>Fully Managed Customer has read only access</td>
<td>OPTION</td>
</tr>
</tbody>
</table>
Prior to the Managed Service go-live, an audit of the customer’s rulebase is carried out, in the case of existing firewalls. For new firewall installations, these are built at Caretower, and shipped to site for installation. All of these activities are scoped within the setup costs, to determine the number of days required for build and/or site visit.

1 RULEBASE AUDIT
We will undertake an assessment of current policies and rules and contrast that with the enterprise objectives and compliance requirements. In addition we will optimise the rulebase, simplifying on-going management and minimising misconfiguration.

2 RULEBASE MANAGEMENT
If the customer wishes us to make configuration changes to the Security Device policy/rulebase, then this will be done in accordance with the ‘Change Control’ process detailed. The CSM/CSO or designated person will need to provide sufficient network detail in order to design and implement the changes.

We will use reasonable commercial effort to perform all maintenance and configuration management activities remotely.

3 SLA SUMMARY

Single Device
We shall ensure that the device under contract is up (available) for 99.8% of the time over a one year (365 day) period except in those situations described below*.

High Availability
We shall ensure that the device under contract is up (available) for 99.9% of the time over a one-year (365 day) period, except in those situations described. A high availability system is one that is configured in active/active or active/passive which is designed to come active automatically. It does not include systems that have a cold/warm standby, or which need to be manually switched to active. In this situation these would be considered as single devices and so a lower SLA applies.

*We will not be responsible for failures or degradation beyond our control, such as customer infrastructure, cabling, telecoms service/equipment, power provision, utility suppliers, ISP etc.

WE WORK WITH ALL MAJOR VENDORS, SOME OF WHICH ARE:

- Intel
- Check Point
- Dell SonicWALL
- Sophos
BENEFITS OF CARETOWER’S FIREWALL MANAGED SECURITY SERVICE

**SPEED OF IMPLEMENTATION**
Our Managed Security Firewall Service seamlessly integrates with your network and can be up running within days, not months. We deliver instant results through visibility of events and analyse on a live dashboard with in-depth reporting.

**ROBUST REPORTING**
Our Managed Security Firewall Service brings you comprehensive technical, operational and trend reports that communicate security status and satisfy compliance requirements.

**24/7 CARETOWER SECURITY OPERATION CENTRE**
Our Managed Security Firewall solution allows you to be a Firewall service user, not an administrator. This means that you have access to Firewall service to view the data and run required reports whilst maintaining a certain level of privileges. The Firewall service is constantly monitored by our 24/7 Security Operations Centre where the team will carry out monitoring, management and incident response to security events and alerts.

“We will evaluate which of our services suit you best and customise it to make sure that it fits your business needs.”
WHY CARETOWER?

As an independent IT security specialist, with over 17 years experience, we provide comprehensive solutions to individual problems, thus allowing our recommendations to be unbiased. Over the years, we have quickly established many long standing relationships with all of our vendors, achieving the highest status within these organisations based on the level of expertise within our internal sales, support and professional services teams.

This relationship ensures we provide our customers with key changes within the industry which assists in their on-going security management strategy.

- Live global 24/7 Firewall Managed Service
- Dedicated GIAC Certified Digital Forensic Security Engineers (SANS (SysAdmin, Audit, Networking, and Security) Institute)
- Full-onsite and hosted architecture options, depending on your requirements
- We are CSA (Cloud Security Alliance) member and ISO 27001 Accredited

GET IN TOUCH:

020 8372 1000
INFO@CARETOWER.COM
WWW.CARETOWER.COM