



Managed Security Services

Managed Security Service is an integral data security service that satisfies the needs of the whole company for secure electronic data exchange both internally and with external parties, including over the Internet.

Managed security is comprised of two components:

1. VPN and firewall hardware and software, supplied by the Service Provider, that reside at the customer's premises often referred to as CPE (Customer Premise Equipment).
2. Remote monitoring and management of the VPN and firewall using a security management solution that resides at the Network Operations Centre.

It is possible to conditionally divide the life cycle of the service into several phases:

1. Preparatory phase which in turn is divided into:
 - a. Definition and documentation of security policy;
 - b. Installation and / or integration.
2. Day-to-day operation.

Depending on the needs and present situation of the specific company the scope of these phases may be different.

Definition and documentation of the security policy

One-time activities do not ensure secure data communication. In order to ensure the security of data communication it is necessary to carry out constant monitoring and update the security solutions depending on the development of new technologies and, naturally, depending on the detected types of attack. But before it is possible to take measures for implementing the security policy, the security policy has to be defined and also documented according to standards. For this purpose an expert analysis is carried out in order to assess the data security requirements of the company.

In the course of defining the security policy:

- All users are classified into groups similar by nature on the basis of their rights and the resources used by them;
- The resources of the company are classified on the basis of how critical the specific data is – business critical data (for example, financial data, customer offers, etc.) and less critical resources (for example, the web page, etc.);
- The resources of the company are classified on the basis of their accessibility;
- The users are classified on the basis of their access rights – access only within the Intranet, access only from the outside into the Intranet, etc.;
- It is classified to which resources access only from the Intranet is allowed, to which both from the Intranet and the external network;
- User authorisation mechanisms and their security are defined.

In addition, in order to minimise the security risks, recommendations are given with regard to the other IT segments of the company, for example the infrastructure, used private channels, etc.

Documentation:

The security policy of the company is documented on the basis of everything that has been described above and as a result of this a Security Profile is obtained. This Security Profile constitutes a basis



for specifying the requirements and parameters of the security solution if a new security solution is developed. However, this Security Profile will be in any case used afterwards for managing the entire security solution. Naturally, the Security Profile is constantly improved and updated.

In addition, forms and rules are established as to how the information exchange between the Customer and the Service Provider is going to take place, who has a right to address inquiries to the Service Provider during rendering the Full Firewall Management Service, who has a right to give instructions to add users or modify the rights of the users. Specific forms are established for use by the Service Provider in order to inform the Customer of the attacks directed against the Customer.

Preparatory phase of the service

There are basically two versions depending on the firewall solution used by the Customer previously:

1. Starting from scratch with the development of a new solution; or
2. Upgrading the solution used with components required for rendering the service.

Structure of the greenfield solution

Optimum components are chosen for the security solution depending on the compiled or existing Security Profile:

- Suitable firewall software;
- Suitable firewall hardware;
- If necessary, components required for duplicating the solution;
- Required VPN (virtual private network) components for connecting the branch offices of the company;
- Required VPN components for the people working from home or mobile workers;
- Required means are selected for authorising the users both from the Intranet and, if necessary, from the external network;
- Required management software;
- Other required components.

A selection of the above-specified components is installed in the office and / or branch offices of the Customer and, if necessary, also in the laptop computers of the people working from home and mobile workers. The security solution is set up according to the requirements established with the Security Profile.

Migration from existing solution

According to the compiled or existing Security Profile the firewall solution is supplemented with the required missing components:

- Suitable firewall software;
- Suitable firewall hardware;
- If necessary, components required for duplicating the solution;
- Required VPN components for connecting the branch offices of the company;
- Required VPN components for the people working from home or mobile workers;
- Required means are selected for authorising the users both from the Intranet and, if necessary, from the external network;
- Other required components.



In addition, the following modules required for rendering the Full Management Service are replaced or upgraded:

- Service provider management console;
- Service provider monitoring console;
- Others.

A selection of the above-specified components is installed in the office and / or branch offices of the Customer and, if necessary, also in the laptop computers of the people working from home and mobile workers. The security solution is set up according to the requirements established with the Security Profile.

Run-time phase of the service

After the installation and set-up the solution is put into operation. The run-time phase of the service consists of the management of the following day-to-day routines:

- Solution monitoring;
- Addition of software updates;
- Addition of software updates developed by the producer for preventing new attacks;
- Addition of users according to the instructions given by the Customer;
- Modification of the user rights according to the instructions given by the Customer;
- Addition of new resources according to the instructions given by the Customer;
- Regular security policy assessment;
- If necessary, renewal of the used hardware;
- Steps necessary for ensuring the service parameters established with the SLA (service level agreement). For example, the replacement of hardware within the prescribed time and arrival of a specialist in the office of the Customer, if this turns out to be necessary.
- Documentation of modifications that have taken place.
- Constant updating of the Security Profile according to the tasks carried out and the modified list of users and user rights.
- Archiving the logs concerning the Customer.

Depending on the needs and wishes of the Customer some components of the management may be divided between the specialists of the Customer and the Service Provider. For example, the addition of new users and modification of user rights may belong to the tasks of the Customer specialists. In such a case, Adventus fulfils the above-mentioned function, if the specialist of the Customer is away for a prolonged period or if fulfilling this function is more efficient and quick when the service offered by Adventus is used. At the same time, documentation of the modifications would be the task of Adventus.

Advantages of the Full Firewall Management Service

The Full Firewall Management Service is a perfect solution for the company:

- That has decided to specialise in a narrow business area;
- That has recognised a need for a high level security of data exchange, but does not have IT security experts on the payroll;
- That has recognised a need for a high level security of data exchange, but prefers to find alternatives to high initial investment in the security solutions;
- That wishes to supplement the security management ensured by their IT specialists with the support of experts;

That wishes to minimise the risks associated with new technologies and solutions in the rapidly changing world of information technology.



It is easy to start using the Full Firewall Management Service. It requires only a clearly expressed wish to own a top-level security solution with expert management.

The Full Firewall Management Service contains all obligatory components of the security policy and security management that often remain uncovered in small and middle-sized companies due to the inadequate training, inadequate experience and very often also due to the shortage of time of the IT specialists. The Full Firewall Management Service comprises the following:

- Development of the security policy;
- Control over users and user rights, conformity of the user rights to the selected security policy;
- Access rules for different resources;
- Periodical analysis of the security risks;
- Documentation of the entire solution and the changes and modifications that have been made.

This service is also suitable for current CheckPoint users. Even if the company is a user of the Full Firewall Management Service, the Customer does not lose its previous investments, as it is possible to use most of the components in case of the Full Management Service also. In such a case, the service charge of the Full Management Service decreases for the Customer, since the risks of the Service Provider related to investment will be lower as only management modules have to be added.

If a Customer moves on along the development spiral of the company and reaches a point where it is necessary or justified because of some other considerations to hire their own experts and a management team, the Customer still benefits from the previous use of the Full Firewall Management Service. Namely:

- There is no need to write off investments made during previous periods.
- When taking over the management, it is possible to take over a completely operational system and there is no need to invest in the development of a new security concept.
- A completely documented solution is transferred to the Customer.
- A documented history is transferred to the Customer.
- It is possible to redeem the components of the solution used by the Service Provider for their salvage value.

Versions of the Full Management Service

It is possible to render the Firewall Management Service on the basis of two models.

In the first case a Full Management Service is rendered where the entire required solution and know-how comes from the Service Provider, including the required software modules and hardware.

In the second case a segmented service is rendered which means that depending on the established security policy the management duties and management rights are divided between the Service Provider and the specialists of the Customer. This version is suitable for customers who want to own licenses and equipment or who already use the CheckPoint firewall solution, but wish to delegate some or all management procedures to specialists of Service Provider – Adventus Solutions.