



**Securing SAP/ERP with AppGate  
Unified Access Solution**



## Executive summary

SAP/ERP systems can provide considerable benefits for medium and large organisations but they can also introduce significant risk to the security of critical data and resources. The risk is frequently not acknowledged or managed effectively when SAP/ERP systems are deployed.

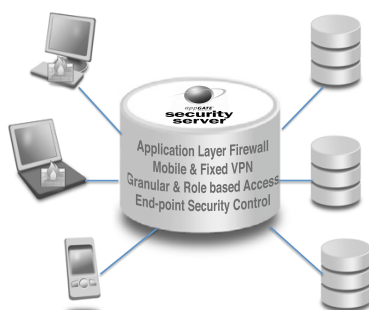
Central to ERP is the commitment of all business function resources and information to a central 'resource planning' platform. Centralising information is essential for sharing data across the organisation but, should any malicious user gain access, the threat to the business is much greater.

What is surprising is that information security is not a central consideration as part of a standard SAP/ERP deployment. Instead, it tends to be treated as an after-thought. The result is that network security is inflexible or ineffective leaving corporate data and assets vulnerable to attack. Holes in the network perimeter via 'backdoor' access routes are not closed off, internal security risks are overlooked, usernames and passwords are passed un-encrypted. Where attempts are made to provide security, users face inflexible procedures that make SAP applications difficult to use and the user less productive.

The costs to business as a result of unauthorised access to corporate information are well documented and include not only direct costs but also a drop in share price and loss of customer loyalty. For organisations implementing and running SAP/ERP, information security should be recognised as a strategic issue.

By managing user access needs for the SAP/ERP system as a whole, including at the deployment stage, the relevant security issues can be fully addressed whilst also helping users make full use of the ERP environment. "Unified Access" is an information security model that aligns very closely with the SAP/ERP model, allowing security and user access policies for the whole system to be managed through a centralised access control platform. AppGate's Unified Access solution delivers high performance in terms of protection of corporate assets, and, like ERP, can improve productivity, speed up service delivery and reduce errors.

AppGate's Unified Access enables information security to be a central component of SAP/ERP implementation, delivering the secure working environment needed to let users fully leverage the system whilst also fully protecting corporate assets.



## 1. Background

Many large organisations rely on ERP (Enterprise Resource Planning) solutions such as SAP to coordinate all the resources, information and activities necessary to automate and manage business processes such as order fulfilment or billing.

Central to SAP/ERP is the creation of a single, shared database that contains all data for the various business functions across the organisation, enabling improved operational efficiency, productivity, tracking and planning.

A typical SAP/ERP system will be accessed by a wide range of users – employees working in the office or off-site, and external users including suppliers, customers and 3<sup>rd</sup> party companies that provide systems support and development. Provisioning access to this wide range of users clearly increases the risk of an unauthorised user gaining access to the company's core information and resources. With the computing needs of the company integrated into a single SAP/ERP system, the problem is magnified – a malicious user can now gain access more easily to all information and systems.

The security risks should not be underestimated. Potential attackers continually change their strategies, looking for vulnerabilities and applications that are less protected and which will yield high returns. SAP/ERP systems are increasingly being seen as potential soft targets.

## 2. Information security and SAP/ERP

ERP systems are typically complex and involve significant organisational and operational change. Business teams focus on managing the programme of implementation and delivering results from the SAP/ERP system. The need for an effective information security solution to support and protect the SAP/ERP system is not a primary consideration.

Standard practice for SAP/ERP implementation does not look at information security for the SAP/ERP system as a whole. Instead, existing network defences may be considered sufficient, or additional security measures are added on as each software module is implemented.

The result is that gaps in security are overlooked, or additional network security products add unnecessary costs to the business and create an inflexible environment that restricts the way users can access SAP/ERP applications.

### 2.1. The threat from inside the organisation

SAP/ERP servers are typically installed inside the corporate firewall. Existing network security against external attacks is often considered to be sufficient protection. However, this traditional approach of treating everything on the outside of the network as malicious and everything on the inside as benign is no longer valid. Trusted users may need access from outside the network (eg. employees working from home), while users on the inside are not necessarily trusted (eg. external consultants employed to deliver the SAP/ERP solution).

According to a Computer Security Institute / FBI survey 1) computer crime threats to large corporations and government agencies come from both inside and outside their electronic perimeters. Internal attacks are both commonplace and expensive.

With a standard deployment of SAP/ERP, there is little protection from internal threats. Any machine on the network can connect to the system servers, access control relies only on user authentication into the system, and all users have access to all SAP/ERP application servers regardless of their actual needs.

1) Source CSI/FBI Security Study 2003: [http://www.gocsi.com/press/20030528.jhtml;jsessionid=Y5IKKCR2WE1D0QSNLPSKH0CJUNN2JVN?\\_requestid=12743](http://www.gocsi.com/press/20030528.jhtml;jsessionid=Y5IKKCR2WE1D0QSNLPSKH0CJUNN2JVN?_requestid=12743)

## 2.2. Traditional security measures restrict productivity

Where internal security measures are deployed, point products add protection but at the cost of flexibility for the user. For example, a typical solution to prevent unauthorised access to the SAP/ERP server is to use a firewall that only allows specific corporate-owned machines with fixed IP addresses to connect. Users can only work from those machines, which is inefficient and inflexible as settings are not easy or quick to modify when circumstances change or a different IP address is assigned to the internal machine via DHCP (Dynamic Host Configuration Protocol).

## 2.3. Security of login details

SAP solutions do not encrypt communications traffic as standard. Network traffic between the user's machine and the SAP system, such as user-names and passwords, are transmitted in the open and are therefore not protected.

## 2.4. The threat from outside

External specialists are frequently employed to deploy ERP/SAP solutions and need access to the network whether they are working on-site or remotely. Exemptions to standard security policies may be required for the project. For example, to facilitate remote support, a direct access route – a hole in the network perimeter – is often created to facilitate quick and easy access, but this 'backdoor' bypasses any network perimeter security and creates a potential route for attackers to gain access to the SAP/ERP database. In addition, procedures are rarely put in place to ensure that these loopholes are closed once the system has been delivered.

## 2.5. Added costs for the business

Where information security for the SAP system is specifically implemented, security measures tend to be added on as each SAP/ERP module is deployed. The result is multiple access control products that overlap in functionality and which all require time and money to license, support and maintain.

# 3. Unified Access provides the solution for SAP/ERP security

Unified access control systems have been designed to protect data and applications and to provision secure access for authorised users regardless of whether they are located inside or outside the organisation.

Unified Access uses a model for security that aligns closely with the SAP/ERP model, allowing security and user access policies to be managed through a centralised access control platform.

The unified access solution from AppGate Network Security provides a platform that brings together all the functions necessary for secure access control, addressing all the requirements for SAP/ERP security, including:

- Encryption as standard: built-in encryption ensures that data such as username and password are automatically protected.
- Access control for internal and external security: all users, regardless of their location, are authenticated before access is granted, including external suppliers using 'backdoor' access routes.
- Access to resources on an 'as-needed' basis: for each user, access is blocked to all data and applications except to those resources they are specifically authorised to use. If a malicious user gains access to the system, the risk to online assets is minimised.

- Secure remote access providing a user-friendly working environment: users are able to work securely from any location using any device. End point security automatically sets dynamic rules to ensure compliance with usage policies.
- Strong user authentication: 2-factor authentication such as one-time passwords, which are delivered automatically to the user via SMS or email, strengthens security and cuts IT costs.
- Central control for better security, easy administration and regulatory compliance: centralised control of access policies means user administration is much easier and quicker to manage, and mistakes are reduced. Access rights can be quickly updated when users change jobs or leave the company. Full monitoring and logging of all access to system resources reduces overheads in reporting for regulatory compliance.

#### **4. Summary**

The potential risks to corporate assets and resources are significantly increased when an organisation deploys SAP/ERP. Standard industry practice for SAP deployment does not address information security needs, and actually introduces a number of processes that leave information unprotected. Existing network security should not be assumed to provide sufficient protection. SAP project teams are specialists in ERP and not necessarily well-positioned to identify the organisation's information security requirements or specify appropriate solutions.

Information security and user access should be recognised as a central element in any SAP/ERP deployment and managed holistically to provide the secure working environment needed to let users fully leverage SAP/ERP resources whilst also fully protecting corporate assets.

Unified Access is an information security model that closely aligns to the SAP/ERP model and delivers high levels of security, with policies controlling security and user access managed through a central user access platform.

The Unified Access solution from AppGate Network Security provides a comprehensive solution that addresses the security problems associated with SAP/ERP solutions and also delivers additional benefits including lower overheads, reduced IT costs, increased user productivity and higher system availability. With AppGate, system administrators are able to protect the organisation's data and applications while also enabling users to access the resources they need to leverage the full benefits of the SAP/ERP system.

## **Appendix A: Unified Access - the AppGate solution**

AppGate Network Security provides a platform that brings together all the functions necessary for secure access control. AppGate's solution contains four basic security functions:

- Application layer firewalls that protect the AppGate server and application servers connected to it.
- End-point security through an integrated device firewall and client inspection
- Encryption with built-in roaming for mobile and fixed network usage
- Granular role based access control.

Key features of the AppGate solution make it an ideal platform for addressing the information security requirements for any SAP/ERP solution. These include:

### **Comprehensive functionality in one solution:**

- ♣ The AppGate solution replaces many of the point products traditionally used for network security and access control. For example with the AppGate solution, the use of internal firewalls to protect SAP/ERP systems is no longer required. The AppGate system is itself the next generation dynamic firewall and is certified for Common Criteria and FIPS-140-2 for encryption protocols. As a result, network configuration is simpler and therefore easier to manage, and the cost of administration and on-going vendor support for these redundant products is removed saving the organisation rolling costs.
- ♣ Business requirements will change over time, and AppGate's comprehensive functionality will support the company's security and authentication roadmap without the need for further investment. For example, a company that requires a fast implementation of a solution based on Active Directory authentication may, later on, want to move to 2-factor authentication via one-time password to increase security. With the AppGate solution these changes can be deployed in a matter of minutes.

### **Encryption as standard:**

- ♣ AppGate provides one encrypted channel for each individual SAP/ERP user, regardless of their location or the amount of applications accessed. AppGate ensures confidentiality, integrity and proof of origin of the communication between users and the back-end SAP/ERP servers.

### **Access control for internal and external security:**

- ♣ AppGate provides the business with precise control over who should have access to different modules, at what time, from which location, from which devices, what authentication method is required and so on. For example: to access the finance system the user should be using a corporate-domain machine, between the hours of 8am-6pm, using 2 factor authentication, and anti-virus software must be running and up to date. The access rules and client inspections that can be put in place around an individual application are almost limitless and can meet any corporate security policy.
- ♣ The AppGate system safe-guards corporate assets not only from external threats but also from internal threats by blocking access requests from users except those who are authorised to access specific assets. Where access has not been granted, services are invisible, thus making it impossible to see or attack corporate assets.

### **User authentication:**

- ♣ Instead of relying on network perimeter security, the AppGate solution focuses on protecting the corporate assets. Therefore, all users, regardless of their location, are authenticated before any access is granted.
- ♣ The AppGate system can integrate with multiple authentication systems at the same time. AppGate supports a wide range of authentication methods including SMS 2-factor authentication, and certificate authentication for PKI deployments. A backup method of authentication can be offered to users in an instant if issues occur with the primary authentication method.

### **Protection of core systems:**

- ♣ Many organisations with mission critical systems run two networks, keeping the business network away from the mission critical systems. AppGate, with its high security role based architecture, simplifies the task of managing access between these two networks without complication or high administration.

### **Flexibility for a user-friendly environment**

- ♣ The AppGate solution allows users to access assets through a secure connection over any type of network connection, whether it is from a local corporate network, from home or over a wireless/3G connection. Additionally, with the AppGate solution, users may initiate their secure connection from virtually any type of device: a desktop PC, laptop, Smartphone or PDA, if the policy permits it.
- ♣ Availability of servers: AppGate blocks all unauthorised unencrypted network traffic from reaching the SAP/ERP servers, preventing flooding of the servers enabling a proper execution of business processes and helping to improve the availability of the SAP/ERP environment for users.

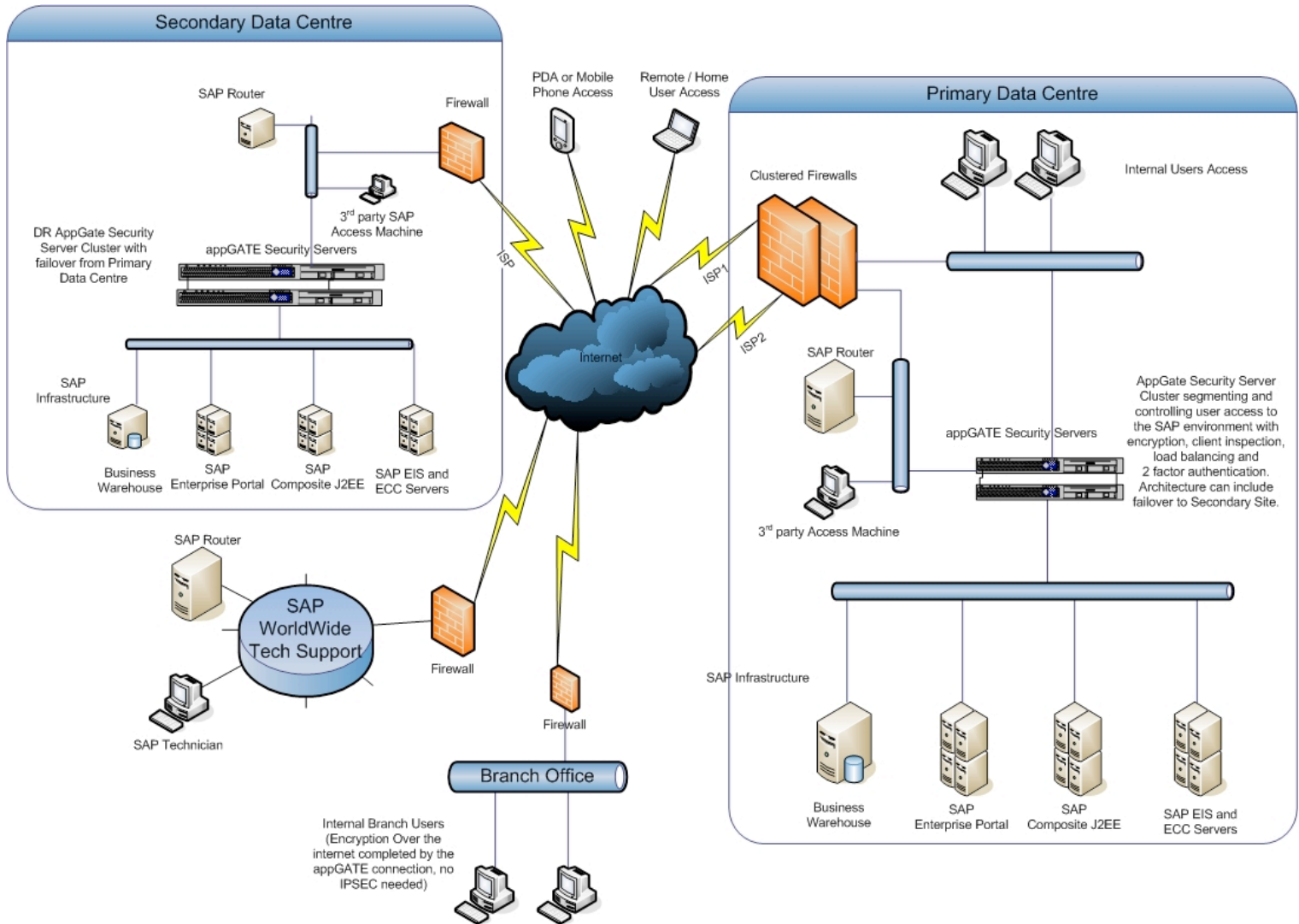
### **Business continuity / disaster recovery**

- ♣ AppGate servers can be clustered to ensure high availability, even across different locations. If one server becomes unavailable, users are automatically routed to remaining good servers as they connect.
- ♣ AppGate's ICE (In Case of Emergency) license enables the company to upgrade the AppGate server in an instant to handle unlimited concurrent connections for a limited period of time so that people can continue to work even if they can't access their normal work environment.

### **Central control for quick and easy administration**

- ♣ The AppGate solution provides a single, central point of control over security policies making it easy for access rights to be modified and enforced. For example, granting access to the security system for new users or removing access for employees who have left the company can be done from one central location like Active Directory. Once the SAP/ERP services have been configured within the AppGate system, it is just a matter of the Helpdesk team adding new users to Active Directory groups or deleting the user who has left the company.

# Typical AppGate Secure Infrastructure



**appGATE™**  
NETWORK SECURITY

AppGate Network Security AB

info@appgate.com

Tel: +46 31 774 43 50

Fax: +46 31 774 04 42