link22

SECURE ACCESS

link22 Secure Access is a simple and secure toolbox for the modern digital workplace.

SIMPLE
AND SECURE
TOOLBOX

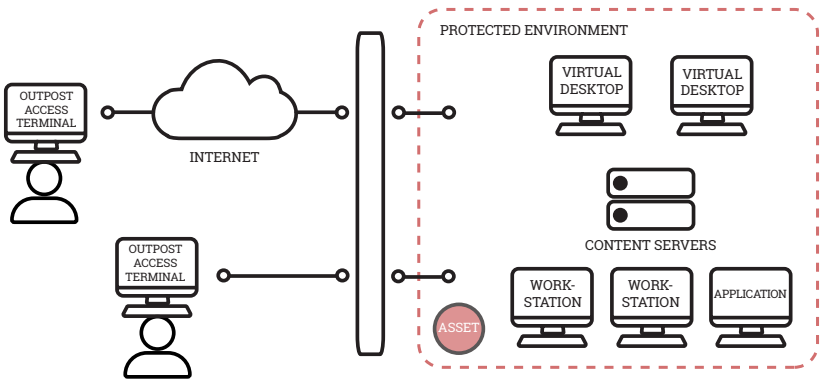
ADOPTABLE TO YOUR SPECIFIC SECURITY NEEDS

Secure Access

link22 Secure Access is a simple and secure solution for the modern digital workplace. It allows you to control all access to your IT environment whether you are working within your controlled premises or are mobile with the need for remote access over Internet.

Secure Access is built on the principle to move the desktops, applications, and services into the data center and build a secure perimeter to maintain the protection of your sensitive applications and data. Unwanted exposure of your data is greatly reduced by a sound IT-security architecture building on read-only end point devices, network segmentation, and virtual desktop separation. The sensitive resources can be accessed locally within your office environment or remotely only after the user has been authenticated and authorized. No data is stored on the end point devices and all communication with the data centre is encrypted.

Secure Access means an extra layer of security, without compromising the maintainability and flexibility to appeal to everybody from small corporations to large enterprise organizations. With an agnostic view on security, link22 Secure Access can be adapted to your specific security needs. Perhaps you are working in a highly secure and regulative environment where nationally approved security solutions must be used. No problem; with our Secure Access toolbox we will find a solution that can be approved yet fulfills needs for usability and functionality.



SOLUTIONS FOR DIFFERENT NEEDS

With link22 Secure Access we can provide:

- **Role-based Access Control**
  We provide an overall approach for access to your IT environment by requiring authentication and authorization of everyone and possibly everything, prior to trying to access the resource that needs a thorough protection. You can look at Secure Access as an additional layer of security protecting your IT environment.
- **Hardened Clients**
  All clients are hardened according to established security baselines. The hardening covers the hardware, BIOS and operating system. Different access clients exist for different needs. Some workplaces are stationary, others are mobile.
- **Centralized Management**
  Users and access clients are all centrally managed. This enables us to manage large installations and continuously adapt to changing needs of usability as well as security.
- **Security Auditing**
  We make sure that every security relevant event will be forwarded to your organization's SIEM for continuous supervision and analysis. This gives you peace of mind knowing that you are in control.
- **Smart Card**
  We all know that smartcards are better than passwords. With Secure Access we can integrate your PKI solutions for increased security.
- **VPN/TLS**
  Remote access over Internet requires encryption. Different organisations have different requirements. We will find a solution where we will integrate the encryption solution of your choice.
- **USB Management**
  Some organisations allow the use of USB memories, some don't. Within the toolbox we have the tools to implement and control the usage of USB devices. Or completely disable USB devices, if that is what your policy says. If the usage of USB memories are disabled, we suggest instead using our Secure Transfer solution where you can gain full control of what's imported and exported.
- **Network Access Control**
  By using additional security on the network layer we can reduce the exposure even more and thereby increase security. By adding Network Access Control, we can control the possibilities to communicate within the network.
- **Adaptable to your specific needs**
  We always start by analysing your specific requirements and suggesting a solution that fulfils your IT security policy while it is still easy-to-use and effectively supports your business needs.

TAILORED MANAGEMENT

Outpost Manager

Outpost Manager is the central server handling all the system's access clients along with all users and groups in the system. Outpost Manager is built on Microsoft Server with Active Directory activated, hardened and tailored to manage a Secure Access solution.

The main security features of Outpost Manager are:

- **Centralized user management**
  Outpost Manager handles all the users in the system, including authentication with either password, smartcard or any other token compatible with Windows.
- **Centralized management of access clients**
  Outpost Manager controls all access clients in the system, such as configuration, updates, GPOs etc.
- **Time Server**
  Outpost Manger provides a common time to all access clients and other equipment in your secure access solution.
- **Centralized management of USB Devices**
  The usage of USB devices can be centrally managed from Outpost Manager by installing a management software onto Outpost Manager and agents on every access client.
- **Centralized management of network access**
  Access to the network layer can be centrally managed from Outpost Manager by selecting network equipment that support Network Access Control (NAC) in combination with management software on Outpost Manager and agents on every access client.

SUITABLE FOR REMOTE ACCESS

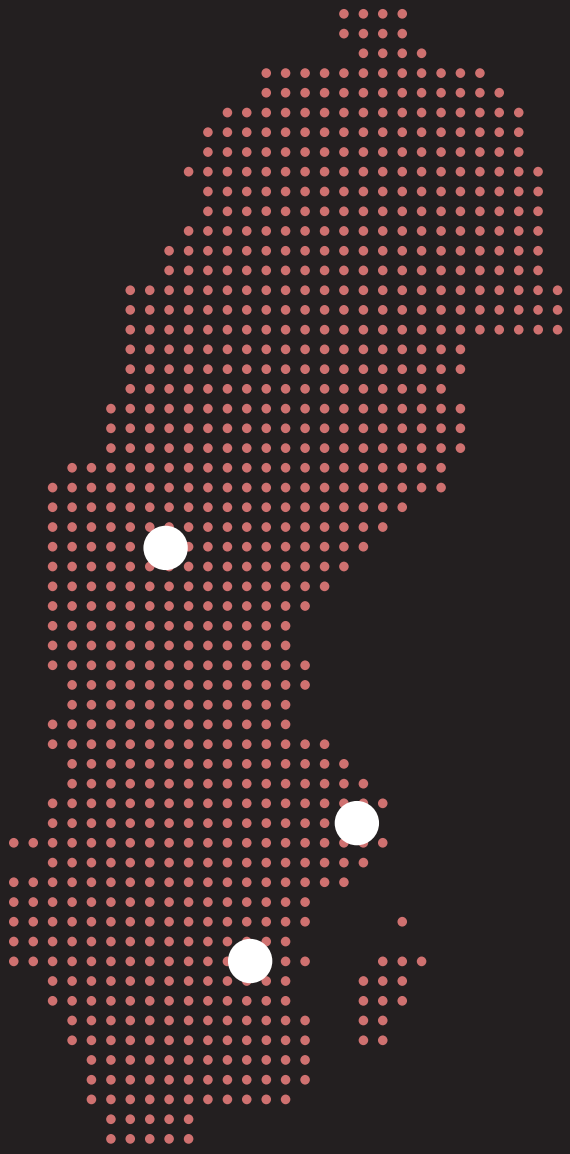
ADAPTED FOR STATIONARY PLACEMENT

Outpost Access Terminal

Outpost Access Terminal is our answer to the need for thin clients, adapted for stationary placement within your office environment. Outpost Access Terminal implements a role-based access control. The standard Windows Desktop is replaced with a simplified interface where you will be presented with a selection of applications you are authorized to use. Typically, this means a set of links to virtual desktop environments. If you need an environment for remote access, we can adapt an Outpost Access Terminal with a VPN-solution.

The main security features of Outpost Terminal are:

- **Kiosk Mode**
  From Outpost Access Terminal you are only allowed to initiate a limited set of sessions to central IT services, like a remote session to one or several VDI environments.
- **No local persistent storage**
  Outpost Access Terminal does not persistently store any information locally. This is achieved by leveraging on Microsoft Windows solution for thin clients.
- **Centrally managed**
  Outpost Access Terminal is centrally managed from Outpost Manager
- **Smart Card**
  Outpost Client is equipped with a built-in smart card reader.



Head office Linköping

link22 AB
Teknikringen 8
583 30 Linköping

+ 46 13-13 24 00
info@link22.eu

Östersund

link22 AB
Kyrkgatan 53
831 34 Östersund

Stockholm

link22 AB
Tellusvägen 43
186 36 Vallentuna