THE SECURE DIGITAL WORKSPACE

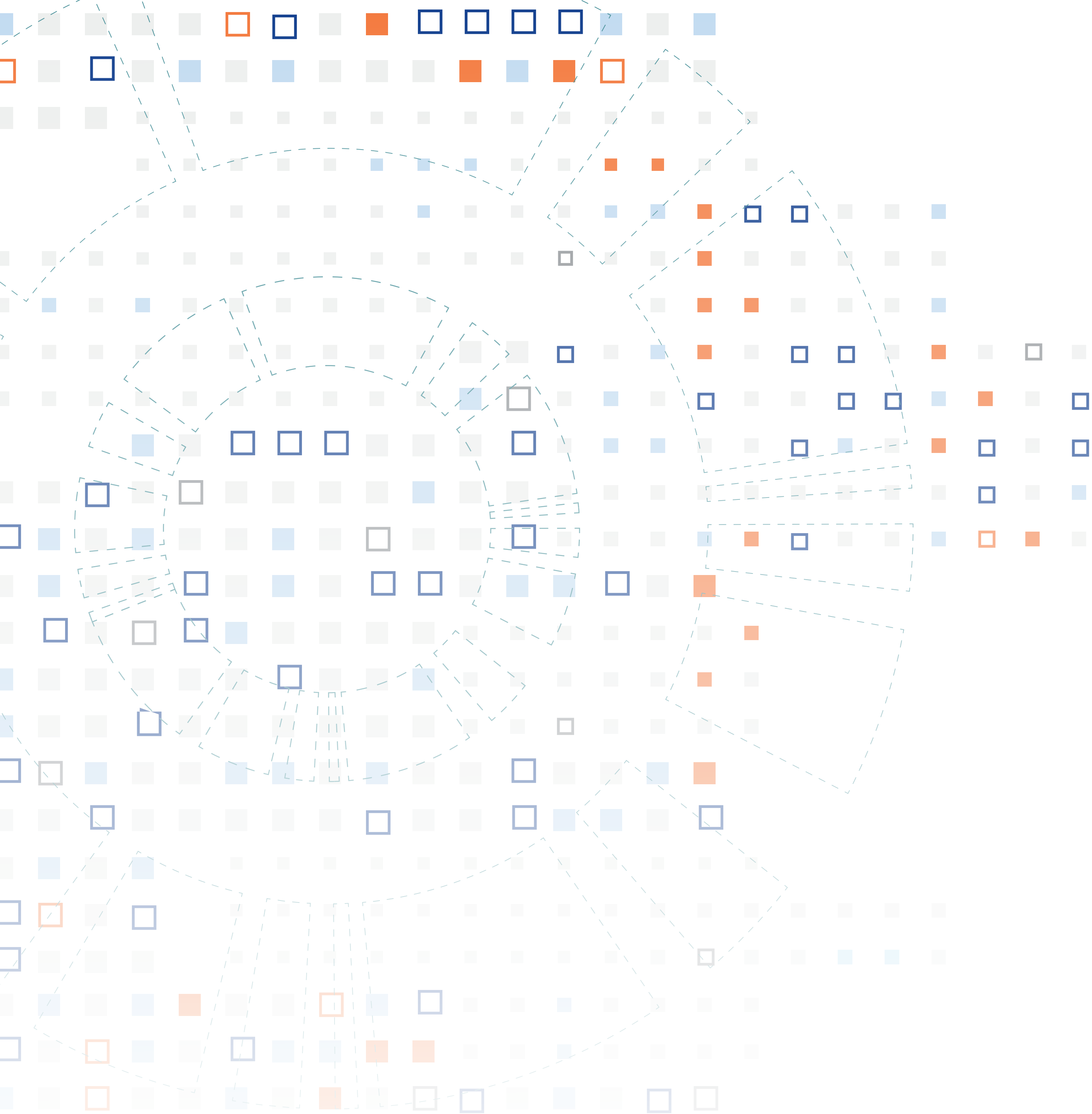
A MORE EFFECTIVE AND FLEXIBLE WAY OF WORKING

WHITEPAPER

SecureLink

SAFELY ENABLING BUSINESS

TABLE OF CONTENTS



WHY YOU NEED A SECURE DIGITAL WORKSPACE

There is no denying it. Technology has changed the way we work and the way companies manage their systems. Throughout the various industries, mobile working has become a standard. Employees want to work anywhere, anytime and on any device. This flexible way of working may not compromise their user experience nor their privacy. And there must be a safe distinction between their private and their corporate data.

An increased mobility implies higher security and data protection concerns. Therefore, the appropriate security controls must be implemented and there has to be a strong data loss prevention. Threats come both from outside and inside the organization. So, on top of protection against external threats, identity-defined workspaces are strongly advised as not all employees should have access to all applications.

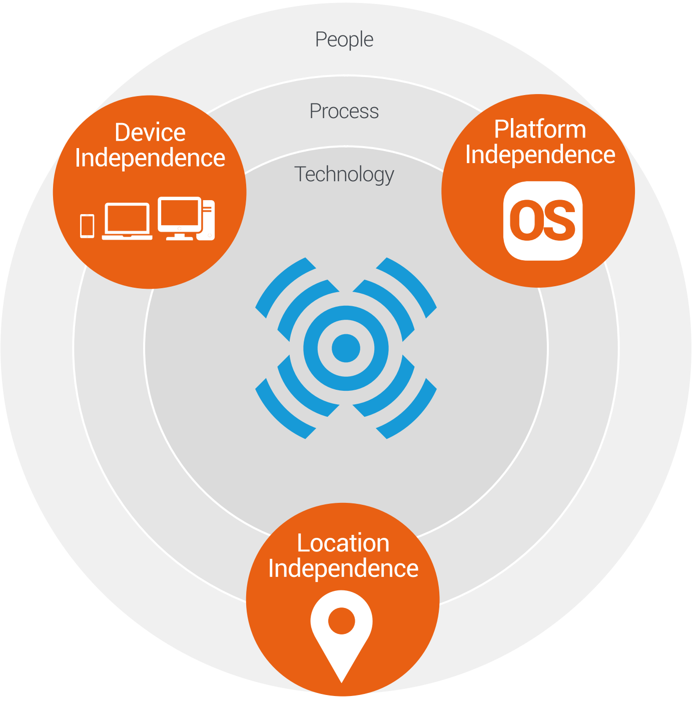
Cyber security has become of utmost importance these days and breaches can seriously harm your company. As a well-known security integrator, SecureLink has the right expertise to assist you in achieving a customized Secure Digital Workspace. A workspace that meets your needs and budget. We help you create a solution roadmap to support your employees as selecting the right technologies can be very complex and resource-intensive. The overall infrastructure must be planned and implemented in an organized manner. Throughout this whitepaper, we will elaborate on how SecureLink can assist you in developing a SecureWorkspace solution.

WHY YOUR DATA NEEDS TO BE CENTRALIZED

The **SecureWorkspace solution** combines workspace flexibility and security in your datacenter. We safely want to deliver access to applications anytime, anywhere and on any device while keeping your unstructured data in your datacenter. Why is it so important that the **data is centralized**?

First of all, we have to emphasize the importance of data. Data is the center of every business model. It creates value, intelligence, insights, but it also entails danger. **Data security** will definitely be the main focus in the coming years. European legislations such as the **GDPR** only accentuate this. When companies are attacked, and data is stolen, this will most certainly disrupt their daily functioning. Even whole economies can be brought down. **All data is valuable**, even the email address and phone number of a friend. If companies get access to a database containing millions of email addresses, names and phone numbers, the value is immense.

Moving and sharing data is essential to business success. You cannot hide your data because the value lies in its processing. So, how do you do this in a secure way? The most effective way to implement data security, is to **keep it in one central location**. The centralization will offer you more control on where your data resides, who accesses it and why. Users nowadays often work in a decentralized environment on their mobile device while processing data and copying it to the central location to share it. The SecureWorkspace solution enables organizations to provide a large number of clients or users with access to applications from any location, anytime and on any device **without leaving a trace of the data on the device or location**.
This means that there is Location Independence, Device Independence and Platform Independence.



STRONG SECURITY WITHOUT COMPROMISING USER EXPERIENCE

The data centralized in your datacenter must be strongly secured. **Implementing security controls, can have a negative effect on the user experience.** It might be complicated or slow things down and it often restricts the users' freedom removing or denying actions or control. Users are sometimes not allowed to personalize their workspace because of security reasons for example. The SecureWorkspace turns this strategy around by implementing security-by-design and upholding user experience avoiding shadow IT.

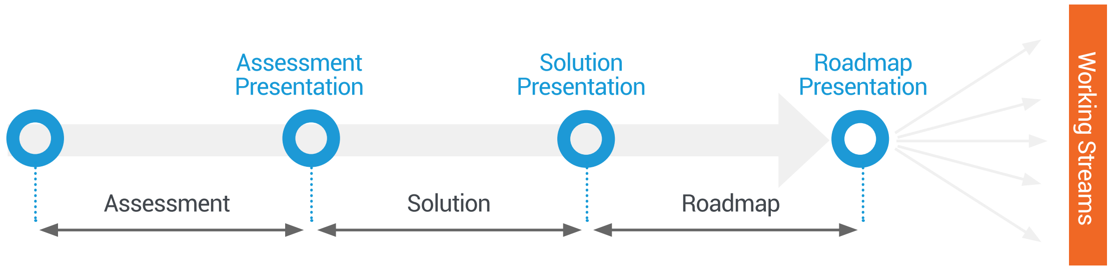
The SecureWorkspace addresses this problem by only sending out screen and keyboard strokes over the network and this ensures access to applications as if you were working locally.

DEVELOPING A CUSTOMIZED SECUREWORKSPACE SOLUTION

Building a coherent workspace strategy is a real challenge. It must improve the user experience and the efficiency of your employees. SecureLink developed a process that helps you gain insights into the ideal strategy for your organization. We take into account your budget, business model, data processing and IT culture.

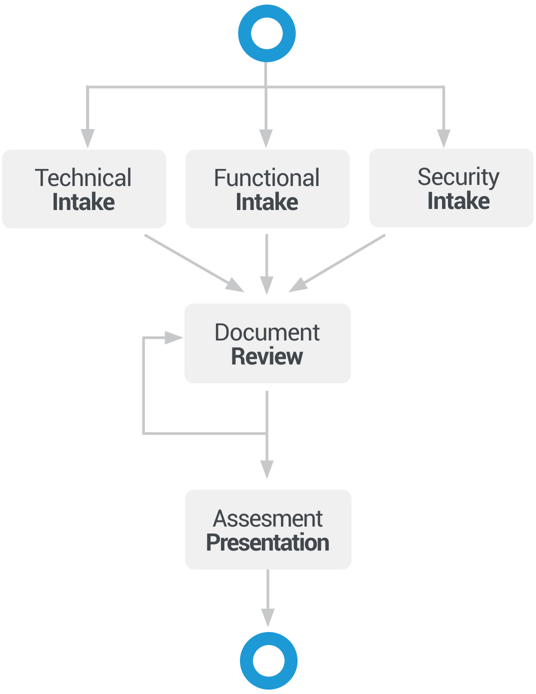
The Solution Process

The Solution Process is based on our best practices. It consists of three phases: The Assessment Phase, The Solution Phase and the Roadmap Phase, resulting in one or more working streams.



The Assessment Phase

The Solution Process starts off with The Assessment Phase. The Assessment Phase consists of a Technical, Functional and Security Intake.



During the **Technical Intake**, we interview technical engineers and take a look at the existing environments and technologies.

We will gather all relevant information and requirements needed for the future workspace solution. We focus on the following topics (if applicable):

- Server platform, storage and backup;
- Network infrastructure and layout;
- Server virtualization technologies;
- Applications and other resources offered to end users: Windows applications, web or SaaS applications;
- File sharing and document management environments;
- Active Directory or other identity services;
- Client devices such as PCs, thin clients, laptops, phones, tablets…;
- Peripherals and other devices connected to end user devices.

During the **Functional Intake**, we assess the customer's situation from a functional point of view. We get a thorough overview of the existing environment by interviewing employees with executive, operational and end user profiles on their current way of working with devices, applications and data. Their user experience and possible suggestions for improvement will be assessed.

Functional aspects might include the following:

- How do users connect to applications;
- Where do they connect from;
- Are there requirements regarding offline availability for certain applications or data;
- Which devices are used for connecting to the applications and data and which devices are preferred;
- Which applications are considered as business critical;
- How do users access and utilize data.

During the **Security Intake**, we take a look at the current environment from a security perspective. Interviews with the security officer as well as users will give insights into the current security regulations and requirements. On top of that, a risk assessment will be conducted regarding the current workspace environment.

The Security Intake includes:

- Data classification
- Application risk analysis
- Identity and Access Management
- Secure Connectivity

Based on this research, we will create a document in which this information is combined. Review sessions with the customer will be organized in order to verify the content and the conclusions so the document can be revised where necessary.

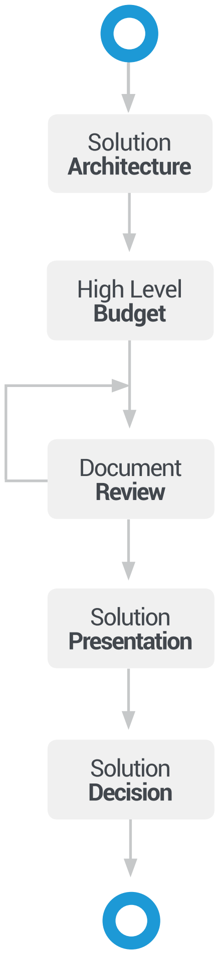
Once the assessment has reached its final state, the results will be presented to the customer and they will be used for the solution definition phase.

The Solution Phase

Based on the information gathered in the assessment, a solution architecture will be defined by our specialized architects.

This architecture will be described in a solution architecture document, containing the following items:

- A solution description;
- A high-level overview of the architecture;
- A diagram describing different components and their relationships;
- Key design decision points and justifications regarding technology choices.



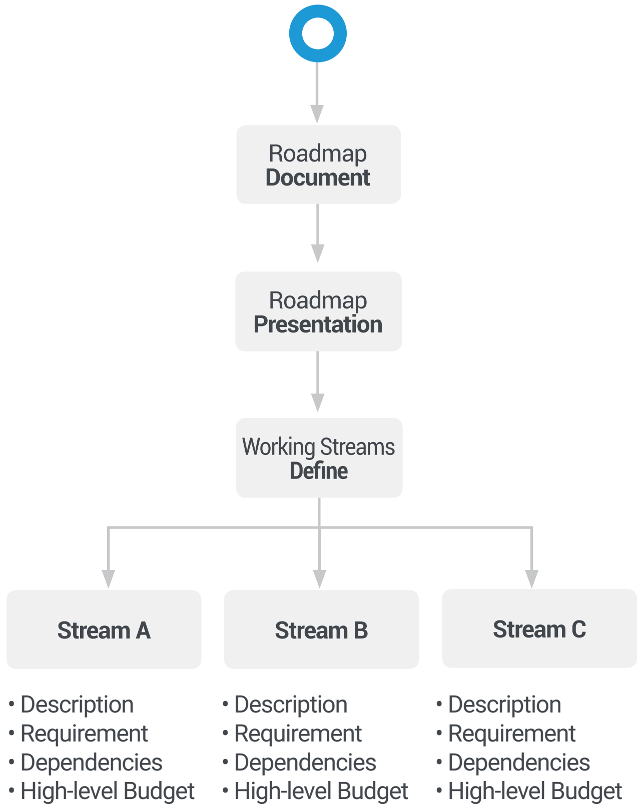
When an architecture is determined, we add an overview of the budget estimations to the solution document. The investment and operation costs related to infrastructure, licensing and services will be described.

The SecureWorkspace solution document which contains high-level targets and the overall budget will be discussed with the customer during the review process. During that process, adjustments can be made and additional customer input can be incorporated.

When this document is final, the results will be presented to the customer. They are also used as input for the roadmap definition phase.

The Roadmap Phase

To draw out the roadmap, we follow the steps below. The roadmap definition is the final part of The Solution Process. Once the high-level target architecture and overall budget have been defined and approved, a roadmap will be created and described in detail. This document will contain a timeline with a visual representation of each step required to evolve from the current situation to the target solution.



Several working streams will be identified in this roadmap, each with its own goals based on the current dependencies and requirements. Each stream is of course based on the available budget at that time. More concrete budget estimations will be made where possible and we will determine how many projects are needed in order to achieve the goals of the working stream. We really need an in-depth view of the budget so we know how many experts we can rely on for which amount of time. We also need to know which technologies we can deploy. It is perfectly possible to roll out the projects in different stages, depending on the customer's available resources.

Subsequently, this roadmap document will be presented to the customer. Therefrom, decisions can be made concerning the working stream, prioritization and execution, taking the defined dependencies into account.

CONCLUSION

Safe access to applications and data from anywhere, anytime and on any device without compromising the user experience resulting in higher flexibility and efficiency. That is what a SecureWorkspace will bring to your company. Building a coherent strategy to obtain this SecureWorkspace is a real challenge. That is why SecureLink developed a process that helps you build the ideal strategy for your organization taking into account your budget, business model, data processing and IT culture.

A SecureWorkspace infrastructure offers you access to applications and data as if you were working locally. Since only screen and keyboard strokes are sent over the network, all data can be kept in the datacenter or private cloud. This centralization will offer you more control on where your data resides, who accesses it and why.

If you want more information about the Secure Digital Workspace, please do not hesitate to contact us.

Do you have a question, comment or are you looking for more information about the **SecureWorkspace** ask our SecureLink Experts.

Author **Bob Deleeck** - Business Developer SecureWorkspace @ SecureLink
bob.deleeck@securelink.be

@SecureLinkBe SecureLink Belgium

SecureLink

SECURELINK

Safely Enabling Business

SecureLink specializes in the design, the implementation and the support of the most reliable and innovative networking, virtualization, security and data center infrastructure solutions. Over the years, we have become one of the largest Pan-European cyber security integrators.

We offer more than just advanced technology; we are also service providers who offer vendor-independent advice. Thanks to our extended security expertise, we are able to solve the most complex cyber security challenges.

Our experience in Managed Security Services offers you security and continuity. The SecureLink cybersecurity specialists are available 24/7 to assist you from the Cyber Defense Center. Our experts are known for their results-oriented, no-nonsense approach and strong expertise.

SecureLink's know-how, passion and personal customer approach result in an innovative service, high customer satisfaction and acknowledgement from the most renowned vendors in the industry. We safely enable your business.

Fields of expertise:

- SecureWorkspace
- Virtualization
- Next Generation Security Gateways
- Endpoint Security
- Proxy Security Gateways
- Managed Services
- Dynamic Network Access Control
- Core Network Services; Secure Infrastructure
- Visibility & Analytics
- Cloud Security

> We offer more than just advanced technology; we are also service providers who offer vendor-independent advice. Thanks to our extended security expertise, we are able to solve the most complex cyber security challenges.