WHITE PAPER

Secured Desktop as a Service

Cyber Defense Product Team

EWD 215

HYBRID CLOUD SOLUTIONS

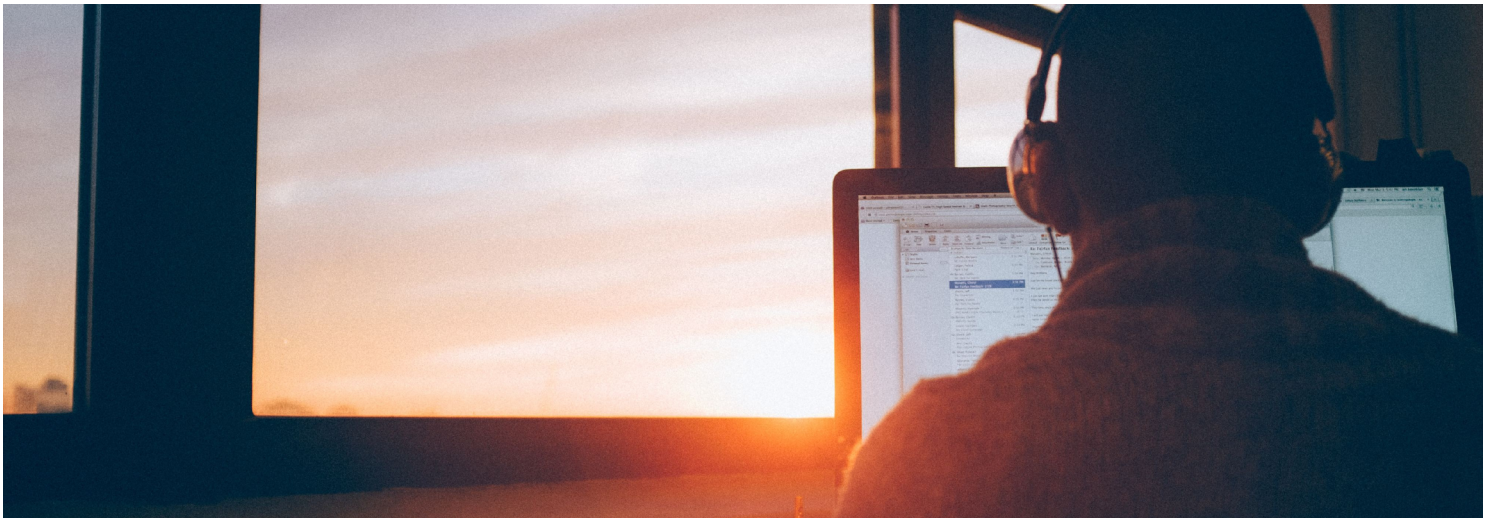
INTRODUCTION

An increasing number of struggling organizations and companies experience IT as a complex and baffling endeavor. Cyberthreats emerge frequently from the use of apps, the internet and the Cloud, rendering cybersecurity navigation progressively difficult. That is why implementing a good cyber defense strategy is essential.

The field of IT is a highly competitive one, and finding qualified IT staff is a time-consuming, challenging task. Due to the complexity of IT and cybersecurity, employers continue to spend financial resources on the maintenance, capacity and education of their staff. Furthermore, the field of IT struggles with a shortage of qualified workers. This complexity, competition, and scarcity renders IT a costly investment. Furthermore, Murphy's Law applies to IT implementation, which means that unpredictable difficulties will arise. Implementing IT technology is therefore a lengthy and expensive process. These challenges associated with on-premise IT are mounting, which makes it difficult to manage and reduce business expenses.

Lastly, we should also consider societal expectations when it comes to investing in new technology. Millennials now constitute a significant part of the job market, and tailoring to their professional skills, desires and expectations is key to corporate success. Being brought up in a quickly advancing and globalizing world, millennials expect, desire and utilize cutting-edge technology in the workplace.

"Millennials expect, desire and utilize cutting edge technology in the workplace."



CHALLENGES FOR CLOUD PROVIDERS

Cloud providers are increasingly facilitating specialized IT service, tailored to the user's needs. Companies and organizations profit from this approach, as these providers offer intelligent solutions that are aimed at fixing recurring IT issues.

The cloud market currently offers a wide range of service-orientated IT infrastructures and platforms, such as Azure, AWS and Google. The market's focus has thus shifted, now chiefly aiming at satisfying front-end needs. Recurring challenges in front-end development include creating individualized designs and satisfying user demands concerning end-point devices/equipment. These challenges also include establishing excellent performance and functionality, location-independent secure access to company data, and facilities that make such data available both online and offline.

During the past decades, companies and organizations have dealt with these challenges by creating individual IT departments, data centers, application platforms and end-user applications. They have also invested significantly in human resources.

Such costly investments, however, are no longer necessary. As a cloud provider, EWD215 has developed (and continues to develop) cutting-edge solutions and products for our customers and their IT needs. Our aim is to satisfy these needs by providing secure access to your desktop as a service.

DESKTOP AS A SERVICE I

Desktop as a service (DaaS) is a concept which includes endpoint devices, functionality and performance, and secure access to your company data. It combines public cloud functionality with on-premise stored data. Let us explain this concept with the following three scenarios:

I: Full Cloud Strategy

The public cloud's capacity can be strategically maximized. When we employ such a strategy, the endpoint device's requirements for computational performance are limited (zero or thin client when working in a Google environment, or with a Chromebook). All applications run in the cloud, and they are accessible via a browser. Additionally, all data is stored in the cloud. We will refer to this scenario as a Full Cloud Strategy.

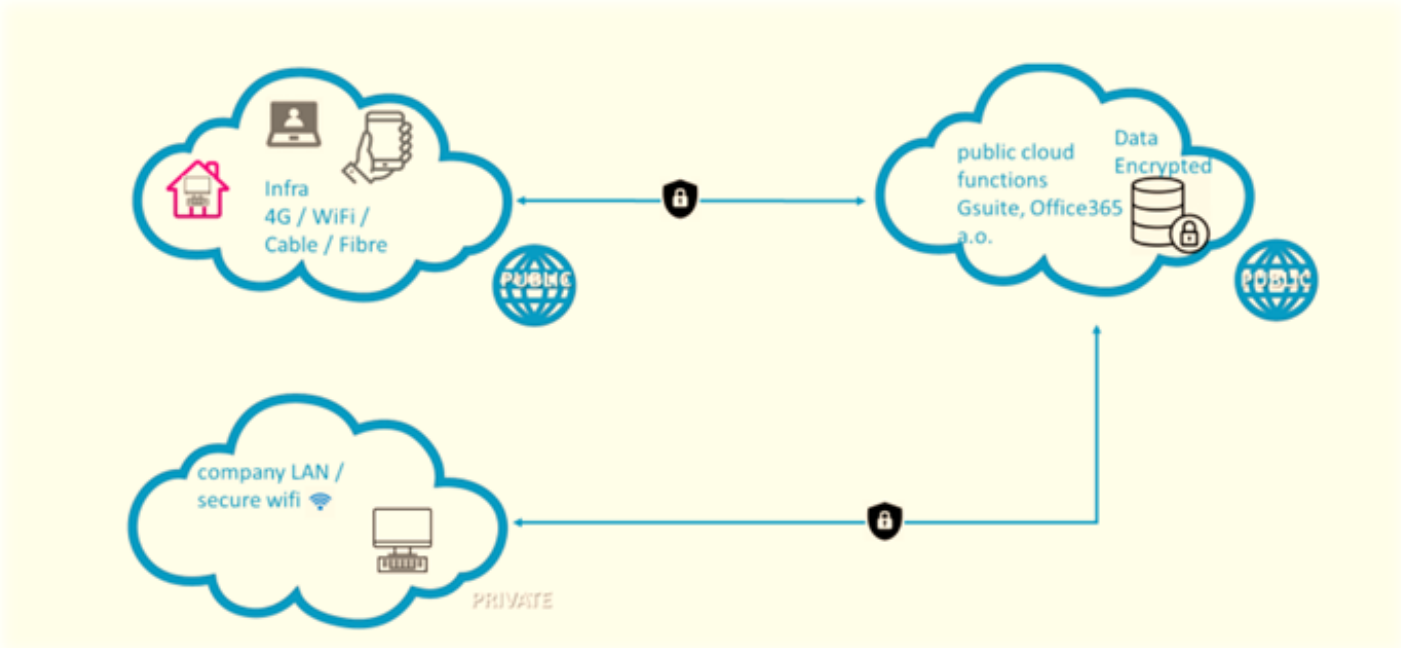


Figure 1 : Challenges emerging from a Full Cloud Strategy

DESKTOP AS A SERVICE II

II: Private Data Cloud Strategy

Accessing public functionality whilst storing your data in a private cloud environment presents a second scenario. Companies and organizations may opt for this strategy as a mode for threat analysis and data classification. Threat analysis and data classification may be part of a business strategy, but may also prove necessary precautions against invasive threats from competitors.

After all, it is essential that innovative and recently developed products are marketed efficiently, especially when working in a highly competitive, fast-growing field. Unethical competitors may be eager to gain insight into the company's progress and product development. Consequently, the threat of IP theft or an undetected data leak may motivate you to store your data securely in a private environment.

This second scenario presents another challenge, that is, a safe integration of the cloud's functionalities with secured private data.

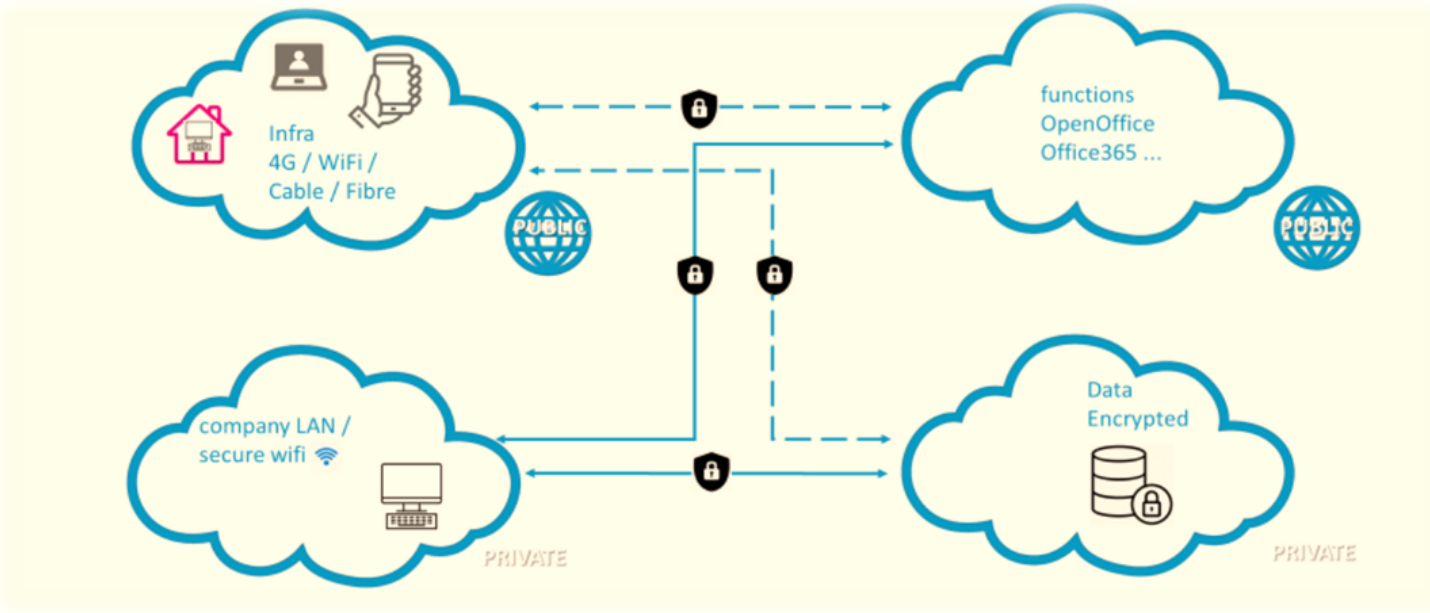


Figure 2 : Challenges emerging from a Private Cloud Strategy

DESKTOP AS A SERVICE III

III: Hybrid Cloud Strategy

The use of internally developed software/business functionality, which is not web based (due to legacy, or other reasons), presents a third scenario. In this scenario, we use limited public cloud functionality, integrating secure access with data, and functionality with a private cloud.

This may include an on-premise private cloud. An environment which is operated by existing IT systems necessitates complex integration. This situation differs from a Full Cloud Strategy. The use of a Hybrid Cloud Strategy is therefore appropriate in this situation for it enables a combination of decentralized and central functions/data.

The degree to which economic and/or reputation loss is likely to occur eventually determines whether data encryption is necessary. You can prevent being hacked or hijacked by ransomware through constantly monitoring your cloud environment. Detecting malicious applications in your cloud environment can prevent cyberattacks and limit damages significantly.

These three scenarios all present different challenges, which may seem daunting and complex at first sight. However, a competent, professional and reliable cloudprovider will easily solve these issues.

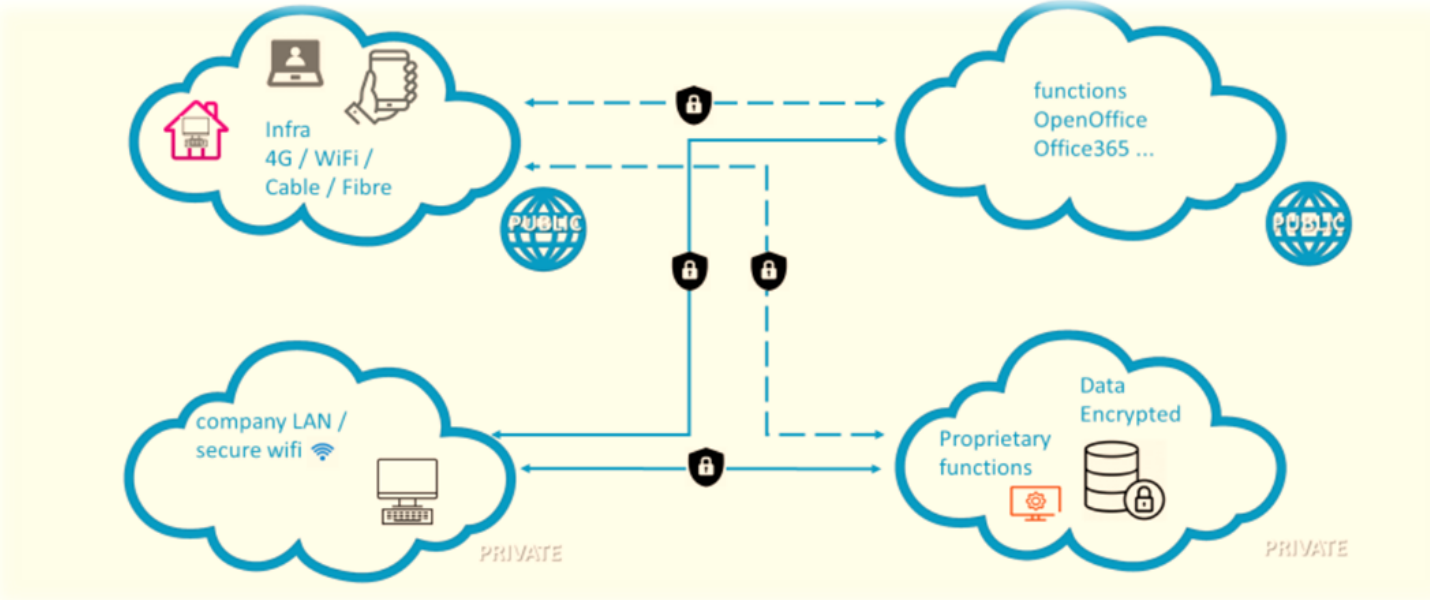


Figure 3 : Challenges emerging from a Hybrid Cloud Strategy, including legacy systems

RISKS ASSOCIATED WITH LACKING CYBERSECURITY

Data leaks and invasive ransomware inflict substantial damages upon companies and organizations each year. These damages can be assessed in both quantitative and qualitative terms.

"2/3 of Dutch companies have suffered from at least one invasive cyberattack in 2019."

Based on a 2019 international research by Hiscox, we now know that 2/3 of Dutch companies have suffered from at least one invasive cyberattack in 2019. In 2018, however, only 1/3 of Dutch companies were attacked.

In other words, the number of cyberattacks is increasing at a shocking rate. The financial losses associated with these attacks have increased as well. In 2018, the financial losses amounted to an average of 184.000 euros per company. In 2019, this number had increased to an average of 300.000 euros.

Reputation loss after a successful cyberattack can also have a major impact on businesses. While large companies may be able to compensate for the loss of customers that results, for small to medium businesses, reputation damage and loss of customers can prove devastating, sometimes fatal.

In a study conducted by Radware, 43 percent of the participating companies reported that they experienced negative customer reviews and reputation loss after a successful cyberattack. Other studies suggest that a company will lose 1/3 of its customers after a data breach. In another study by Gemalto, 70 percent of the 10.000 participating individuals claimed that they would stop doing business with a company after a data breach.

Sources:

Hiscox. "Hiscox Readiness Report." Web.

Gemalto. "Majority of consumers would stop doing with companies after a data breach, finds Gemalto." Web.

Radware. "Radware reports shows that respondents claim average cost of cyberattack now exceeds 1 million dollars." Web.

BENEFITS OF INVESTING IN LEASED IT

Investing in leased IT is financially benificial to your company. After all, purchasing servers and client hardware is expensive. The total costs for owning leased IT are significantly lower. In other words, you gain financial advantages, not by wasting financial resources on internally-developed IT, but by investing in your core business. EWD215 approaches IT as a form of innovative technology that allows you to conduct your daily business operations efficiently and smoothly. This efficiency allows you a competitive advantage. We provide the backoffice software and hardware required for safely operating your desktop computer in the office, on the road or at home.

"Spend your financial resources productively. Invest in leased IT."

In addition, EWD215 provides customized and user-friendly IT. Consider, for example, an administrative environment, in which office applications such spreadsheet, word processing and presentation tools are frequently used. In this situation, web-based access to CRM and other applications is provided. Data on user's request can be safely stored on-premise, or in a private cloud environment. Functionality can be accessed via the public cloud. However, integration in a monolithic or hybrid environment is complex. This complexity is minimized, and rendered compatible with the work environment and application architecture.

Lastly, investing in leased IT and cybersecurity constitutes an adequate and cost-effective mode for risk management. As we have outlined in previous section, inadequate cybersecurity may result into significant

"Investing in leased IT and cybersecurity constitutes an adequate and cost-effective mode for risk management."

reputation loss and financial damages. Cybersecurity that is provided by a reliable, skilled cloud provider reduces such risks significantly. EWD215 secures your desktop as a service with high-quality European security products. These products are highly innovative, and respond to cyberthreats and risks aptly and swiftly. The cloud environment is continuously monitored in a Security Operations Center, and invasive cyber attacks are warded off beforehand, or quarantined after the user's input.

"Quit spending money on IT development. Invest in your core business instead."