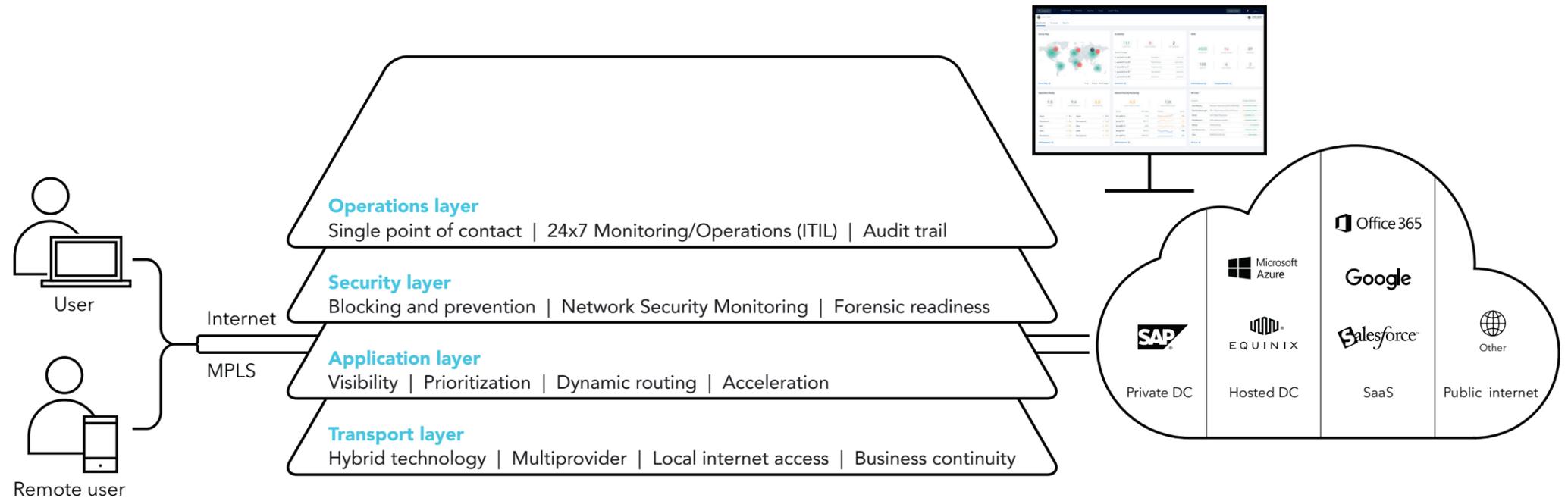# Secure SD-WAN – the next level of software-defined networking



## Transport layer

SD-WAN solutions standardize and simplify the usage and maintenance of hybrid WANs, in which diverse technologies are combined with each other (MPLS, VPN, internet, GSM).

As a result, non-critical data traffic can be redirected to cheaper internet connections. Then the cost-intensive MPLS connections can be adjusted to your intrinsic business needs, and hence costs can be reduced. Additionally, your speed and flexibility of connecting new locations increases, as well as your business continuity.

Internet connections facilitate the integration of different ISPs in various regions depending on the needs of diverse locations. In this way, the total network costs are reduced by 20 to 30 percent.

You can also achieve internet proximity at your business locations by making local internet breakouts available to them. Besides a massive load reduction on the WAN, latency is also reduced, which affects the efficiency of the users in a positive way.

## Application layer

Increase the transparency of the applications and services used by your organization, no matter whether they are hosted on your premises or in the cloud. Protect, prioritize and control your applications and services according to their importance for the enterprise.

Automatically control the path that your application data takes in the network by using application-aware routing. It guarantees high availability and smooth operations, because business-critical applications and services, such as SAP, MS Lync or Office 365, always have enough bandwidth at their disposal.

## Security layer

Existing blocking and prevention capabilities are insufficient to protect against motivated, advanced attackers. In today's world, a breach is inevitable and will eventually happen to every company or organization. Therefore, enterprises and organizations can no longer rely on prevention alone, but also need to shift their mind-set towards rapid detection and effective response.

Network Security Monitoring detects compromised systems quickly and enables you to respond in an efficient way. Contrary to conventional detection systems, the Network Security Monitoring service is built around and focuses on the security of end users rather than on individual events.

The service uses a combination of protocol and signature inspection methods to analyze network traffic and detect network threats, making it possible to respond to suspected intrusions quickly. Due to multilayer event processing by a central correlation unit, the generated alerts have maximum relevance in the security context.

## Operations layer

Automate the protection, operations and monitoring of your business-critical applications and your IT infrastructure by working together with a 24x7 organization that focuses on security and availability.

That way you guarantee a rigorous implementation of your security and operations guidelines, including proactive monitoring, as well as an audit trail that covers several years of transactions.

Meanwhile, a single point of contact reduces complexity by efficiently managing all your ISPs and ensuring network performance.

**open systems**

**Security enabled networks**

If you have any questions about this service, please contact
**sales@open.ch**

Open Systems AG
Räffelstrasse 29
8045 Zurich

t +41 58 100 10 10
f +41 58 100 10 11
www.open.ch