unify Harmonize your enterprise

Mobility: is your business protected?

Real-time conversations are happening right now: on the move, and on virtually any device. And it's not just voice. We're chatting on instant messaging, sending documents over email, and accessing corporate data in the cloud. But as your world goes mobile, how secure are your conversations?

It’s not just the virtual threats you need to worry about – unsecured WiFi hotspots and virus attacks on poorly protected mobile devices. There’s a huge physical problem too.

Mobility is changing security

We're now working everywhere. Fixed workplaces are giving way to hot-desking and home offices. Desktop PCs are being replaced by notebooks, tablets and smartphones. Some are owned and supported by the business. Many are not.

While today's anywhere workers are more connected, more mobile and more productive than ever before, they're also more at risk. And so is your business.

It's not just the virtual threats you need to worry about – unsecured WiFi hotspots and virus attacks on poorly protected mobile devices. There's a huge physical problem too.

A notebook or smartphone left on a train or in a conference room is a tempting prospect for thieves. They may just want the device. Or they may want the confidential data that's on it. And we've all seen or read about the brand and business consequences of this kind of security breach.

A lack of adequate mobile security – in the communications channel, the network or on the device – is a very real issue for enterprises today, begging the questions:

- Should employees have confidential documents on their mobile devices?
- What happens if these devices are lost?
- Should user-owned devices be allowed in the corporate environments (Bring Your Own Device)?
- What measures are needed to enforce security on mobile devices against, for example, malware?
- What corporate applications can be used on which devices?

Entering the app world

Historically, both program and user data were stored on the device – often a desktop PC. That's changed. We're now in the world of the mobile app.

Traditional programs have been adapted for use on mobile devices – with user data typically being stored centrally in the cloud. Everything is now in sync and available from any location or device. And it's all highly secure. Or at least it should be.

Using the same app on all devices is particularly useful in a communications environment, for:

- Web conferencing: collaboration in
- a virtual space – sharing displays
- and documents
- Social networks: posting messages and blogs to colleagues and customers
- E-mail: rapid delivery and access to all e-mails from different devices
- Telephony and teleconferences: real-time conversations to one or many
- Video conferencing: getting face to face thousands of miles apart.

But make no mistake, without the appropriate security measures in place – to prevent call eavesdropping or data interception – your business conversations are at risk.

And even the most security conscious of organizations can become victims. On January 17, 2012, the hacker group 'Anonymous' listened in on a conference between the FBI and Scotland Yard, then subsequently published it on YouTube.

Security in the cloud

The move to cloud, for all its benefits, also increases risk. The challenge here is data storage – because it's no longer in your hands. You need to pay special attention to data protection as it's often stored outside of national boundaries – and therefore not covered by local data protection laws.

And don't be fooled. Social media platforms – Xing, LinkedIn, Facebook, Twitter, Yammer, YouTube, Wikipedia – constitute a special domain of cloud services. You need to think about security and security policy here too as your people engage with colleagues and customers in public forums.

Networks galore

Your mobile users are now connecting to their confidential information directly through Virtual Private Networks (VPN), or indirectly via the Internet. And they're doing so across a multitude of networks:

Mobile networks

By 2015 more than 60 percent of the world's population will be able to access 4G (LTE) mobile broadband technology. And, as lightening fast connectivity arrives, mobile data traffic is predicted to increase exponentially.

WLAN

Wireless Local Area Network (WLAN) design needs to cater for every user, and all devices. Laptops, for example, differ significantly from smartphones in terms of their features. The network has to allow simple inclusion of all mobile devices – and be able to manage the increasing number as they proliferate across the business.

LAN

Because users are now more connected to the corporate network over WLAN or a mobile network, the Local Area Network (LAN) has diminished in importance. But protection here remains critical. Don't forget, mobile devices connecting to your LAN may already be infected with malware as a result of their activities 'on the outside'.

So what to protect? The answer is everything:

- Your apps: typically these are not designed for the levels of security required by enterprise
- Your communication channels: confidentiality and privacy are acutely at risk as professional and private boundaries become blurred
- The cloud: mobile data, and Big Data, is adding a new dimension to data protection and security
- Social media: everyone can speak to everyone – an enhanced sense of awareness is required
- Devices: more options for everyone – and more doors for hackers to open
- Networks: a secure network (VPN) and many non-secure networks (WLAN, 3G/4G, UMTS) means your people must use the 'right' path

The value of thinking differently

So how do you securely integrate all these mobile devices into your existing corporate infrastructure? And how do you do it while keeping costs and management requirements down?

The answer is to think differently. Protection in your mobile environment is no longer a question of whether a particular security measure should be implemented, but rather which security measures are relevant along the entire path.

In the 'old' world, data security focused on measures that kept unwanted intruders out of the network. Powerful defense systems in the form of firewalls, antispam and anti-virus solutions, content filtering and reputation verification were implemented. In addition, appropriate authentication solutions were often set up to regulate access to the company's most sensitive information and zones.

But the increasing use of mobile devices means that applications and identities are being used inside and outside the perimeter – and its blurring professional and private boundaries.

Today, with so many ways of connecting to, using and sharing data, conventional security architectures simply won't deliver the levels of assurance you need.

New approaches trending today

There is a definite trend toward an interaction and information-based protection model. Although traditional security solutions, such as firewalls, will always remain in demand, additional components are needed.

Here are some promising elements of this extended security architecture:

Network Access Control
An already familiar concept to security professionals, Network Access Control (NAC) identifies devices and users – allowing them to access network sections and services based on defined rules. This is a must-have extension to the existing infrastructure for companies with mobile devices.

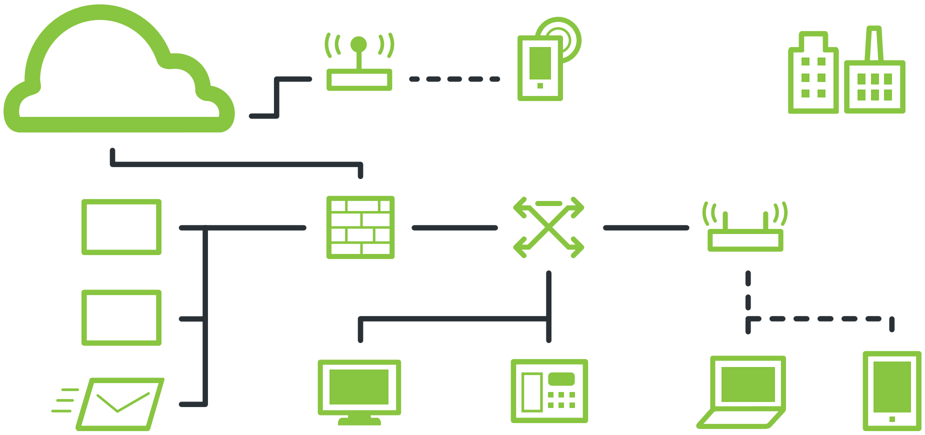
Identity & Access Management (IAM)
Without effective rights management for every user, chaos is inevitable. But in determining who has rights to what, both users and devices have to be identified. That's exactly what IAM does – precisely regulating which users can access which company applications and data, and on what devices.

Mobile Device Management (MDM)
MDM efficiently implements and enforces security guidelines on the mobile device. All devices can be centrally managed and updated, non-trusted apps can be blocked and data can be deleted remotely if a device is lost or stolen. MDM deployment becomes all the more crucial when confidential company data is stored on mobile devices. The trouble is, many MDM platforms still lack adequate support for todays wide range of operating systems and devices that are in daily operation across your business.

The key point is that no single solution will solve your mobile security challenges.

You need to take a harmonized approach – bringing your networks, devices, use cases and users together. Only then will you have an integrated solution that addresses both specific security issues, and supports your overall business objectives.

Today, with so many ways of connecting to, using and sharing data, conventional security architectures simply won't deliver the levels of assurance you need.



Action all areas

There's no doubt that CIOs and IT managers see an acute need for action in almost all mobility areas. But whether planning and deployment is strategic in nature is an open question.

And that's a problem. Not only does a piece-meal approach to security open up a host of potential risks, it can also mean companies fail to take full advantage of the transformational opportunities of that enterprise mobility can deliver.

A viable mobility strategy is needed across the board – with security at its very heart. Without this, you'll run the risk of your devices, platforms and applications proliferating to such an extent that they become impossible to control and manage. And they won't integrate efficiently with your existing infrastructure.

> "Only when users come to realize that security measures are meaningful and necessary are they prepared to accept them more readily, even when they entail some restrictions in terms of use."

So how to do it?

The first step to consider is how to control the adoption of mobile devices within your business. You need to make decisions about the types of devices that are to be supported, and the feasibility and impact of a Bring Your Own Device strategy.

You should also have a good idea of the services to be used and how these fit in with the corporate strategy. External aspects, such as customers, must also not be ignored.

Developing your mobile strategy
When it comes to restructuring, first look at your existing strategy:

- Can any existing components of this strategy be retained and savings made by doing so?
- Is the existing strategy actually compatible with planned business development?

Answering these two key questions involves examining the existing security paradigm, determining the new risks, and reviewing the possible solutions from an economic perspective.

With these factors examined and defined, other critical aspects come into play:

- Mobility management
- Organizational security
- Risk management.

Begin by establishing internal guidelines for the use of these devices – and modify existing guidelines to take account of any new aspects. Then clarify these changes with any relevant company regulatory bodies.

It's also important to ensure there is a clear assignment of tasks and responsibilities for any connected implementation or administration tasks.

Another critical aspect is employee awareness. You can never protect your systems against your own users. The technology implementation is important, but user awareness and understating is critical. They must be made aware of the need for greater personal responsibility and a more conscientious approach.

Addressing the technology

Today's security requirements demand extensive measures on both the personnel and technical levels. A basic level of protection for the traditional IT infrastructure can largely be ensured through purely technical measures – a firewall or proxy systems with the appropriate policies, for example.

But as we've seen, that's not enough. Switching from endpoint to access-based security solutions is absolutely essential. Endpoint security is based on the principle that a device is responsible for its own protection. Should a device actually be compromised, this means the attacker has direct access to your company's data.

Access-based solutions stop the attacker from directly accessing company data in the event of a device being compromised. This approach is based on multi-stage protection. On the one hand, your devices are protected against unauthorized access by third parties using a PIN or a similar mechanism. On the other, access to your company data is controlled by means of user authentication.

A positive side effect of such a portal or proxy system is that external devices have no direct data connections to the company's internal network.

The proxy system 'brokers' the data and presents an additional hurdle for potential attackers. Appropriate authorization policies ensure that your users are only granted access to the data that is relevant for them.

And finally, implementing a mobile solution also requires a modern NAC11 and IAM12 solution that takes account of the specific mobile security risks.

Building your business with mobile

Mobility is great. It creates a more productive, responsive and more agile workforce. But there's no doubt it also represents a serious risk to information security.

The key to addressing this dilemma lies in bringing together devices, networks and data security. Here IT departments must take a different approach – extending perimeter security to encompass protection in the world outside the walls of their organization. And it must be done as part of a strategic plan – addressing technology, user and business needs.

If this happens, your anywhere workers will get the kind of flexibility, choice and ease of use they desire. And you'll have the confidence of knowing that whatever the device or application is used, wherever the data is being stored, and whatever network is being used to access and share it, your information – and your business – is safe.

And, of course, you need the right partner. At Unify, we don't see mobile as something to "add"; we see it as an integral part of the new way to work. And as such, we can provide comprehensive support at all levels. To ensure the benefits of mobility never come at the price of security.

Best Practices in Mobile Security
When building out a comprehensive mobile security strategy, check you have:

- A flexible IT infrastructure able to adapt to mobile challenges – taking account both the existing infrastructure and the planned future direction of your business
- Measures that go beyond basic data protection – including user authentication, access control and policy enforcement
- A mature cross-platform Mobile Device Management solution to manage your portfolio of differing devices and operating systems (from smartphones to tablets)
- An understanding of any known weaknesses or security risks – such as unregulated app downloads on devices
- Clearly defined roles and responsibilities for all the technology, business and user elements of your strategy
- Guidelines for using and handling mobile devices and company data – and that employees understand these
- The support tools able to enforce compliance with your guidelines.

About Unify

Unify is one of the world's leading communications software and services firms, providing integrated communications solutions for approximately 75 percent of the Fortune Global 500. Our solutions unify multiple networks, devices and applications into one easy-to-use platform that allows teams to engage in rich and meaningful conversations. The result is a transformation of how the enterprise communicates and collaborates that amplifies collective effort, energizes the business, and enhances business performance. Unify has a strong heritage of product reliability, innovation, open standards and security.

unify.com

Mies-van-der-Rohe-Strasse 6, 80807 Munich, Germany

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

UNIFY Harmonize your enterprise