

I D C V E N D O R S P O T L I G H T

Continuous and Seamless Governance, Risk and Compliance Management in an Unpredictable Environment: The Need for Advanced Tools

Sponsored By: BeCrypt

January 2009

Eric Damage

Introduction

Remote connection, distant access to IT systems, and ubiquitous employees and managers are nowadays commonplace. Most PCs are mobile, internally or externally. Infrastructures and networks allow easy connection/reconnection to the IT system, from inside or outside the organization, and most applications are accessible from any configured laptop or desktop. With broadband penetration, users are ready for remote work, using laptops and desktops outside the office, or even anonymous machines, to connect and access resources.

These days, a wide range of solutions covers the need for organized ubiquity. Broadband wired and wireless connections, Web applications, VPN, endpoint security software, remote secure access, and identity management will help organizations to "project" their users in a given landscape, at a given moment, with a given security policy. "Cloud computing" is also generating a new relationship between the user and the resource — the IT resource is "somewhere" in the cloud, the user is "somewhere" on earth!

Still, ubiquity-enabling solutions can be considered cumbersome when not too user dependant (most VPNs must be user-activated). Many organizations have implemented remote secure access (RSA) policies, but the risk of disruption, data and file corruption, and data leakage and threat is still growing. Regulations and laws can also be an obstacle to real and total ubiquity based on a single machine.

The Need for Secure Ubiquity

Ubiquity is not a new notion to support any new technical revolution.

From its origins in late 60s, personal IT has always tried to achieve the golden promise. Machines would take on tiresome tasks (high-speed calculations, storage, archiving, indexing...), while the user would be supported in being clever and more productive.

In the business world, things have changed profoundly. In the late 80s, using a laptop was a sign of privilege; today, a laptop is a commodity.

Thanks to progress in general, IT users can work remotely and seamlessly regardless of the device or network. In addition to fixed and wireless broadband penetration, applications' Webization opened up IT resources to contributors. Employees, stakeholders, and partners can access any resource and contribute to the organization's goal, whether financial or not.

In such an "always-connected" world, the personal computer moved from a fixed and central device to a fully mobile and self-sustained friendly machine.

Social research on computer usage identified the phenomenon of IT "consumerization." The high level of personalization allows users to create a unique portfolio of applications and settings on a PC. Each user creates a unique machine and lines are blurring between personal life and professional life.

Whatever the level of integration between the user and his PC, the need for secure, reliable, and duplicable IT cannot be disputed. Consider, for example, that major European airports collect almost 3,500 lost or forgotten laptops per week, and 57 % are never reclaimed (Source: *Dell-Ponemon Institute, July 2008*).

What if the personal computer vanishes? Do we lose the user and its contribution to the organization's value proposition? What if the rules do not allow the use of the personal computer in a given environment?

In any situation, security and business continuity cannot rely on the fact that the user is always using a personal computer.

The Need for Secure Continuous Ubiquity

Secure remote access is one thing; secure continuous and seamless ubiquity another.

Whatever the secure remote access solutions are, the problem of a lost laptop will always be the same. No machine, no access. No user, no productivity. No value generation, no business

If the loss of a laptop is the main threat to productivity, other, non-accidental situations can generate the need for PC-less ubiquity. Due to regulations, moral constraints, or common practices, it is often impossible to use third-party infrastructure to connect remotely.

A government official cannot use a Web café to connect to the governmental IT system. An online banking user cannot use a machine other than his own, in a given secure ecosystem, to operate massive financial operations. Lawyers cannot connect from their clients' premises.

Executives from public companies must respect some financial regulations and keep many results confidential before officially publishing. During a period of non-disclosure, can they afford to travel with a PC full of private and confidential data?

Regulated and classified industries must follow some connection process that will prevent them from basic connection scenarios.

Some crisis or accidental situation can also generate a need for secure continuous ubiquity.

In 2007 and 2008, many organizations had to set-up and test "Asian flu emergency plans" that included recommendations for employees to stay home. Consigning workers to home was considered the best way to prevent massive contamination and virus spread in public transport. But freezing any public transportation use for a few hours was just the beginning of the process; in the case of a real outbreak of Asian flu, weeks of freeze were scheduled.

In such situations, which can be non-accidental, basic remote secure access based on a mobile personal computer is not enough to cover the need for a real secure and seamless ubiquity.

Considering BeCrypt

BeCrypt is a global company founded in the U.K. in 2001. The mission of this high-level player is to meet the demand for data protection and integrity in the personal computer and PDA area. The dissemination of laptops, PDAs, and personal devices turned niche demand into a wide market need within a decade. BeCrypt serves many different communities in the industry with some focus on

verticals. Government, defense, law enforcement, and customs and excise are users of BeCrypt technology all over Europe. Financial services, pharmaceuticals, and insurance and banking clients have also joined the user community.

The major need is to cover data integrity, confidentiality, and compliance during its life cycle, especially while on the personal device. BeCrypt solutions are agent-based in personal devices, and they are managed centrally from a single console at the client's HQ.

In terms of technology, the BeCrypt offering is encryption (engine and software). As for any secure solutions, BeCrypt follows international and local standards to deliver robust, safe, and accredited solutions, through a combination of FIPS and government approval¹. This allows BeCrypt to deliver data protection technology to a wide range of public, governmental, and private clients.

The BeCrypt range of products extends from basic local disk protection to device control and management. More recently, BeCrypt added a virtual secure PC for safe connection:

- **Disk Protect** secures data on laptop and desktop computers by enforcing strong user authentication and by encrypting all data on the hard disk(s) and secures data on removable media, such as USB memory devices, by removable media encryption.
- **Connect Protect** controls the use of peripheral devices, allowing an administrator to apply group policies via Microsoft Active Directory.
- **PDA Protect** secures data on personal digital assistants (PDAs) by enforcing strong user authentication, encrypting all data on removable memory cards, controlling high risk features, and controlling and auditing synchronization (connection to a desktop machine) and file transfers.
- **Enterprise Manager** provides a framework for managing a large security solution, with encryption key management (secure key storage and auditing) and a centralized device recovery facility.
- **Trusted Client** is a low-cost highly secure mobile access device that gives users the ability to access networks, data, and applications from any Internet-enabled PC. Trusted Client drastically reduces the risk of data loss and insecure access.

BeCrypt Trusted Client

In order to cover the need for continuous, seamless, secure ubiquity, BeCrypt recently unveiled BeCrypt Trusted Client. Trusted Client is a solution that allows off-the-shelf USB memory to be used as a secure access device.

This bootable, fully encrypted USB flash drive is combined with a set of software and a range of services. It allows centralized secure connection to resource from any connected PC without leaving any trace, and without using local resource such as operating system and fixed disk.

The main feature of Trusted Client is that it allows the user to set an independent secure session from any computer while being totally separated from the local context. The USB flash drive, once inserted in any unmanaged computer, launches a self-contained secure environment with a Web browser and a full set of personalized applications (email, and business applications such as booking and billing automation, CRM, SRM).

¹ The BeCrypt cryptographic library is certified FIPS 140-2 (U.S. Federal Standards International Standards)

BeCrypt Solutions (disk protect and connect protect) are certified CAPS (Certified Assisted Product Service) Baseline, CAPS enhanced, DIPCOG certified, and CCTM (U.K. — CESG)

After authentication, the remote user will face a familiar screen and desktop. While using data and resources, he will comply with security policy and compliance. All connections settings (including VPN) are embedded in the USB flash drive. For security needs, the USB drive is self-defending, and it will reformat in the case of failed authentication.

The solution creates either a protected local virtualized environment or a simple thin-client, the key and its data are totally encrypted by the central management tool and the user cannot change any settings.

Challenges

Virtual PC and the user environment are a very agile combination of portable solutions (under virtualized environments), hardware simplicity (encrypted USB flash drives have no value if lost and are very cheap to replace) and use simplified interaction (nothing is required except connection to an ordinary PC).

The main secure value in such a solution is centralized management. The organization will have full control of the virtualized environment, secure connection, and device life cycle. This allows full control of settings, use, and configuration by the organization. In terms of security policy, central management allows close and direct control of users and usage.

This must be considered a key advantage for enhanced secure and compliance needs.

However, this solution could appear to be rather complex.

Getting a USB stick to simulate a full desktop environment means a complex pile-up of technical layers under a strong virtualization process, making the thin-client configuration of the software preferable for many use-cases. In addition to this complexity, full encryption of any data contained in the drive is a challenge for security managers, as is the need for authentication. These challenges are greatly reduced where the encrypted device is dispensable and data stored centrally.

IDC understands that this complexity calls for a robust service layer to support fast implementation of this agile solution. The user must not be invited to any settings and configuration operations. So, the hidden back-office service must assume a high level of complex tasks. Applications and connection settings, data security, track records, continuity and user support, licensing, and provisioning management are still a major requirement in such a demanding context. The same is true for maintenance, upgrade, and solution life cycle.

IDC invites organizations to embrace a global overview of the impact of such solutions before adoption, though for organizations with existing support for thin-client or virtualization, there may be an opportunity to leverage the existing infrastructure.

Conclusion

Organizations in a complex and connected world have made significant steps in the past year toward better control of security and continuity. Major progress in the network and infrastructure field allow global connections from almost any point to almost any point.

At the same time, global IT maturation has brought about significant changes in the use of IT.

From a "positioned" posture (where the user was seated on a chair before a keyboard), IT maturation has supported a "projected" posture.

Supported by lighter IT and broader network coverage and bandwidth, users have slowly become ubiquitous. They can travel inside and outside the IT secure perimeter while keeping the same access to resources. Connection and productivity are possible from anywhere, with any device, at any time, and for any reason.

This ubiquity is a strong business enabler. Better productivity, better reactivity, better communications, and better knowledge transfer help any organization to achieve its mission optimally.

Nevertheless, serious threats and complex regulations must be considered when implementing global IT mechanisms and connections. Manned and automated IT attacks can severely weaken the reality of the Global Village.

Security policies and regulatory frameworks constrain many uses and IT postures in order to cover the risk and support business continuity.

Security editors and vendors are able to generate efficient layers of protection to support secured ubiquity in many situations.

Nevertheless, a new set of tools has been released on the market. These tools support secure continuous ubiquity, even in unpredictable situations. They also generate greater confidence in a safe, widespread dissemination of IT.

Based on self-bootable USB device, these solutions provide major progress in terms of security governance and compliance:

- Self-bootable virtualized environments on a USB stick take away from the user any security governance considerations. The tool is totally managed by the organization, and the user cannot update security settings. This is a major step forward compared to highly personalized PCs and laptops that give too much control to the end user.
- Centrally managed connections create better compliance governance by keeping a focus on all IT settings for an optimized alignment between IT use and governance.
- Enhanced security solutions managed virtually can support a better secure remote access policy and practice. By enabling unmanaged plain connected PCs to join complex networks and value chains, these new tools shorten and simplify the complex cost chain to a secure and compliant IT infrastructure for organizations. Return on investment and total cost of ownership considerations are applicable for massive implementation throughout widespread user communities.
- Faster agility to change provided by central management of tools must also be considered as an argument to convince organizations to consider these new solutions.

IDC strongly believes that secure continuous ubiquity solutions represent a unique opportunity for organizations to:

- Regain control of security and compliance governance.
- Smooth the impact of straight and tight security and compliance obligations on the user experience.
- Enhance a better ubiquity experience to the benefit of the user, the value proposition, and the cost of IT ownership.

A B O U T T H I S P U B L I C A T I O N

This publication was produced by IDC Go-to-Market Services. The opinion, analysis and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

C O P Y R I G H T A N D R E S T R I C T I O N S

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localisation of this document requires an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com