



### Moving closer to 'holistic' security

by Mark Lillycrop

***'Holistic' is a very popular adjective in the IT industry at present, particularly in the security area, mirroring the fashion for consumer health products that treat the body as a whole, rather than focusing on individual ailments and symptoms. eTrust, Computer Associates' security management solution, takes this message very much to heart.***

---

In IT terms, the idea of holistic solutions responds to a growing concern that too many weapons in the existing IT armoury are designed to support a specific business function or group of functions, and are not well suited to providing a consistent approach to the enterprise as a whole. The thinking is that, however loosely individual devices, applications and databases interoperate beneath the covers, at a business level there is a real need for a complete, integrated view, incorporating not just internal processes but the entire workflow between suppliers, business partners and customers.

Nowhere is this concern more prevalent than in the area of security management, where CIOs are desperate to build a single profile for identity and access control requirements across the organization, while identifying the areas of vulnerability where the business is most open to threat from outside attack. Such profiles are no longer restricted to IT activity - security is increasingly an inter-disciplinary affair, with Chief Security Officers taking on responsibility for many aspects of physical security (such as facility management and building access), which are becoming inextricably linked with data center operations.

A further dimension of holistic management is the increasingly international nature of security policy, with commercial, government, and health organizations needing to comply with significantly different levels of privacy legislation in different geographies - particularly within the European region. For multinationals, this makes it essential for personal information to



## Arcati Research Bulletin

be managed with a fine degree of granularity, and for cross-border transfer of sensitive data to be tracked with great care.

One supplier that is responding particularly well to the need for 'holistic' security management is Computer Associates, whose eTrust product set draws on the combined strengths of the company's diverse software repertoire, and its long history in enterprise management. CA has faced much criticism over the years, some of it justified, for building up a software empire with little thought to long-term integration or support. But in recent years, the company has paid far more attention to leveraging the benefits of its vast product range as a whole, and to taking advantage of its experience in mainframe systems to extend enterprise-class management functions to distributed and Web-based platforms. Indeed, one of the big advantages of the eTrust security product-set is its platform independence, and its centralized handling of key identity-related information.

### Inside eTrust

eTrust is composed of three discrete but closely inter-related elements - Identity Management, Access Management, and Threat Management - all controlled via a unified Security Command Center.

At the heart of the *Identity Management* component is a dedicated Identity Directory, which stores data in account-based profiles created for each individual (see Figure 1). The Directory includes information on access to facilities and networks as well as to information resources, and incorporates single sign-on and self-management via a portal-based interface. Because of

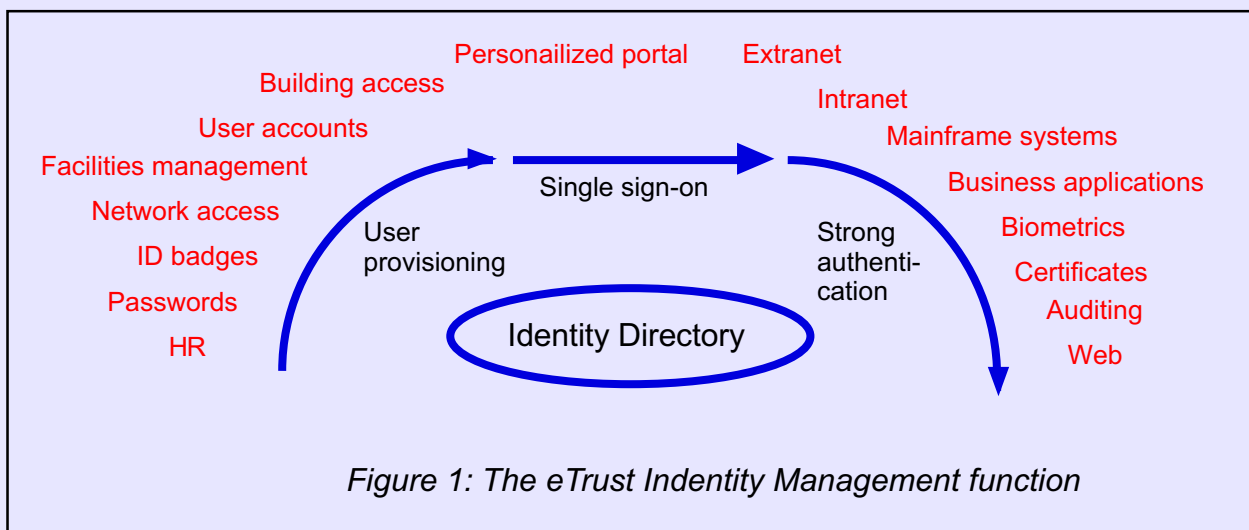


Figure 1: The eTrust Identity Management function



## Arcati Research Bulletin

the technology's centralized architecture, it lends itself to maintaining a single point of reference on every employee and business partner, which can evolve flexibly as personal and security details change. There is also a strong focus on process automation as a way of reducing security management costs.

*Access Management* as a function is in many ways complementary to Identity Management. eTrust focuses specifically on providing a consistent, enterprise-standard level of access control across all applications, irrespective of the underlying operation system. This ensures that, however secure the platform, data can be managed in compliance with privacy laws relevant to the type of application involved and the geographical location of the individual accessing it.

The third element of eTrust, *Threat Management*, provides a constant monitor for signs of attack or vulnerability. It combines the power of traditional virus detection and eradication technologies with a more granular approach to management, using Antivirus Virus Block and Intrusion Detection tools to isolate affected parts of the network, and responding according to pre-defined policies and information gathered on the nature of the threat. The flexibility of this approach allows security administrators to concentrate their efforts on the most significant intrusions, and on the most business-critical parts of the network, and this in turn could lead to significant cost savings.

As with so many system management and security solutions today, the real effectiveness of the product depends on the way that information is collected, filtered, and presented to the administrator, and on the simplicity of the management interface itself. eTrust pulls together information from its constituent parts and feeds them into the *Security Command Center*, offering a highly visual representation of security profiles and threats. The Command Center also controls the level of automation that is applied across the network, and this is an area where CA has a vast amount of expertise to offer.

### **Bottom line**

Inevitably, the long-term success of eTrust will depend on the level of integration between the tools themselves, not just at the Command Center level but in the direct sharing of security-related information and processes. We expect to see eTrust evolve in the months ahead, as CA further strengthens the interoperability of the component products.



## Arcati Research Bulletin

In view of the centralized nature of the eTrust architecture, and the power of the Identity Directory, we see this offering as a very promising solution for companies looking to achieve cost reductions and improve automation across the extended enterprise. We expect it to appeal particularly to businesses coping with the complexity of conflicting security and privacy legislation on opposite sides of the Atlantic, who will be attracted to the flexibility of its identity and access control functions.

---

*Mark Lillycrop is Chief Analyst of Arcati Ltd and an Associate of Valley View Ventures, Inc. For further information on this paper or Arcati services, visit [www.arcati.com](http://www.arcati.com) or e-mail [mark@arcati.com](mailto:mark@arcati.com).*