

User-centric Security and The Dynamic Enterprise

By F. Cosquer

Managing enterprise security risk has always been a challenge. Today, as end-user realities evolve and the pace of change in enterprises accelerates, the challenge of managing risk to enterprise assets is also growing. An increasingly mobile workforce is bringing new demands for anytime, anywhere, converged communications. Innovative new technologies have led to a flurry of new end-user devices and applications, enabling new capabilities that are further driving end-user demand. And more stringent regulatory requirements are increasing potential liabilities.

The Dynamic Enterprise is a term that describes an organization that is constantly evolving to quickly adapt to its market environment and differentiate itself from its competitors – must simplify communications, strengthen relationships and increase productivity in a continuous transformation process.

A dynamic enterprise has four key assets which it must efficiently and securely interconnect:

- The network, which is the foundation for the enterprise communications infrastructure
- People, which includes employees, contractors, partners and suppliers
- Processes, which are critical for compliance
- The knowledge in their organization, which is typically in people's heads or scattered across multiple databases

By securely interconnecting these four assets, a dynamic enterprise can quickly adapt to new market environments and differentiate itself from competitors. And it can benefit from simplified communications, stronger relationships and increased productivity to enable continuous and transformative growth.

One recent and promising approach that allows dynamic enterprises to securely share the knowledge in their organizations and reduce the risk associated with fast-evolving end-user realities is to bring security closer to people. In practice, that means reinforcing security at the points where end users connect to the corporate networks and reinforcing security for mobile user communications.

To fully understand how this user-centric approach to security can help dynamic enterprises evolve their risk management strategies, it is helpful to first take a closer look at the security impact of today's new end-user realities.

New End-user Realities and Security Impact

To be successful and profitable, dynamic enterprises must securely accommodate the new end-user realities. For instance:

- Enterprises must allow end users to connect to their networks from anywhere – from the more obvious need to support connections from remote offices, hotels and airports to the less obvious need to support new, blended lifestyles that allow end users to connect from home or from a café. Additionally, end users expect to be able to connect anytime and from a wide range of devices.
- In addition to accommodating new connection patterns, enterprises are also pushed toward allowing users to benefit from any available connectivity. This means supporting both wired and

wireless technology. With increasing penetration of 3G networks, enterprises must also support connection through service provider networks for extended coverage.

- Enterprises must allow end users to access corporate resources from anywhere and at all times. This capability increases the risk that sensitive information will fall into the wrong hands and, as a result, increases potential liabilities and business impacts for the enterprise.

Managing Risk with User-centric Security

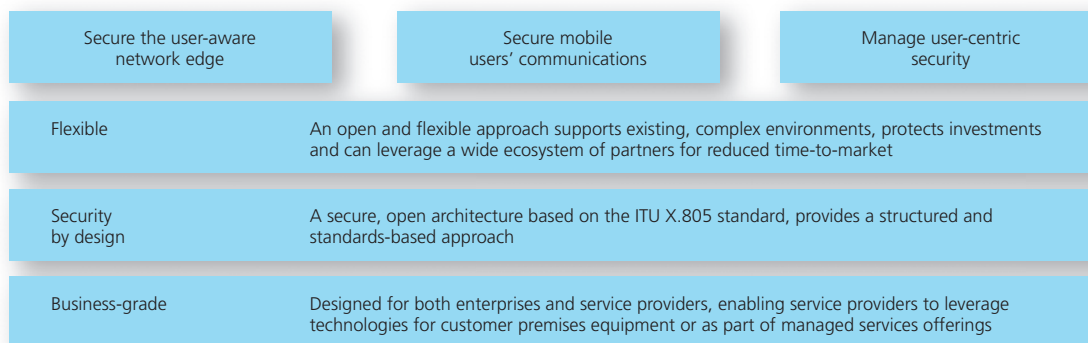
Most approaches to security in the enterprise have focused on protecting the network infrastructure with no or little attention to end users. As a result, traditional security functions and associated devices, such as firewalls and intrusion detection and prevention devices, deal mainly with network-level protection. Although still part of the overall security story, such an approach has limitations in light of the new security challenges described in the previous section.

User-centric security helps enterprises reduce the risk associated with fast-evolving end-user realities by reinforcing security closer to end users. User-centric security is not the same as user security.

User-centric security is about answering peoples' needs in ways that preserve the integrity of the enterprise network and its assets. User security can almost seem like a matter of protecting the network from the user – securing it against vulnerabilities that user needs introduce. User-centric security has the greater value for enterprises.

For user-centric security to be realized, enterprises must create secure environments within which end users can go about their business. They must be surrounded by security solutions that are integrated as a fundamental condition of their working environment, as opposed to intrusive, reactive security measures that can reduce end-user productivity and limit mobility. This approach requires reinforcing security at the corporate network connection points and for mobile users' communications as well as management of user-centric security (Figure 1).

Figure 1: User-centric security reinforces security closer to end users



Managing User-centric Security

Management is a key component of any user-centric approach – from identity, to audit, to in-country-specific policies and regulations. There are two key objectives that enterprises need to keep in mind at all times:

- Simplicity is security's best friend. Although this fact has been stated often, it remains a challenge.

- Reuse offers a clear path to protect capital expenditures and contain operating expenditures. Deployment of a security layer should maximize the existing architecture and ensure seamless integration with existing operational tasks and procedures. The latter will also increase simplicity by reducing training time and leveraging existing skill sets.

One approach to achieve simplicity and maximize reuse of the existing environment is to centralize functions and converge security management and network management under a single framework whenever possible. The following describes three areas where this type of centralized approach can be applied.

Centralized AAA services

It is a good practice to use existing Authentication, Authorization and Accounting (AAA) standards and extend their use for all devices in a unique repository (for example, desktops, laptops, IP phones, mobile handsets). With this approach, Remote Authentication Dial-In User Service (RADIUS) can be used for all new devices. This allows for easy overlay deployment within the existing secure architecture. It also helps ensure seamless deployment of Layer 2 authentication methods, such as IEEE 802.1X for IP phones.

Centralized policy management for all users

All user policies must be integrated and federated with the directories and systems already being used to manage user identities in the enterprise. A user-based profiles approach allows for security management and network management under a common framework and enables a set of attributes and user roles to be mapped with optimal abstraction. Users are defined in reference to roles (for example, employee/engineering, contractor/finance, visitor/briefing center) as well as network criteria (such as subnets, MAC range, VLAN).

Enterprises also need to custom-define their quarantine rules and ensure they can be applied in a multi-vendor environment. The advantage goes beyond provisioning to include operational procedures, such as central isolation and remediation of policy violators down to port, device and user, anywhere on the network – wired, wireless or remote. Interaction of network devices with a centralized policy management system facilitates the deployment of quarantine mechanisms against faulty users and contains attacks that may occur both at the edge as well as in the network.

Centralized monitoring and logs for audit and compliance

Full visibility is fundamental to detect suspicious traffic or activities and provide actionable information for better control. To avoid managing an overwhelming volume of raw data, monitoring and logging systems should support a per-user/role traffic classification with both real-time and historical data, including applications usage. In addition, for efficiency in operational procedures, the solutions should provide a dashboard that summarizes all collected security statuses and provides the ability to view and audit key user data drilling down to low-level events as necessary. Finally, two properties will protect the evolution of the monitoring and logging platform:

- Open interfaces for event collection and correlation with support for a complex ecosystem (third parties) as audit and compliance requirements evolve
- Hierarchical-based implementation for scaling, to support growth of the network and its user base

The benefits will be fully realized with a user-friendly interface that allows IT staff to understand the overall security status at a glance and make it easy to generate customizable reports for auditing purposes.

Conclusion

This user-centric security approach allows dynamic enterprises to support the evolution of everyday end-user realities and quickly adapt to the changing competitive landscape by implementing:

- Reinforced security at the edges of the extended corporate network where mobile end users are likely to connect
- Enhanced mobile user security with dedicated security functions embedded in the communications devices on which they rely
- Simplified and user-centric management of security with a unified interface, converged security management and network management under a unique framework whenever possible

There are several advantages to this structured and straightforward approach to user-centric security. They include:

- Improved productivity as a result of automated security functions and reduced end-user involvement
- Regulatory compliance facilitated by bringing key security functions closer to end users and the devices they carry
- Lower total cost of ownership by unifying of security functions and operational procedures

With a full portfolio of solutions and multi-vendor professional services, Alcatel-Lucent is committed to supporting dynamic enterprises as they evolve their risk management strategies.¹ By leveraging innovative technologies from Bell Labs and services teams with a global presence, Alcatel-Lucent delivers always-on security.

Francois Cosquer is Chief Technology Officer, Security, Alcatel-Lucent, Enterprise Products Group, Colombes, France.

To contact the author or request additional information, please send e-mail to enrich.editor@alcatel-lucent.com.

¹ <http://www1.alcatel-lucent.com/enterprise/en/solutions/security/index.html>; http://www1.alcatel-lucent.com/enterprise/en/solutions/security/security_portfolio.htm