



1040 North Tustin Avenue  
Anaheim, CA 92807  
(800) 842-0221  
[www.maxxess-systems.com](http://www.maxxess-systems.com)

## EndPoint Solutions for Data Centers

### Background

Within modern organizations the role of Data Center Operations [DCO] has evolved from one of an important, but bounded functional service, to the central operational role for every facet of the organization. This trend has been driven by the functional leverage of IT solutions, the dramatic increase in the need to coordinate information and actions throughout the organization to meet competitive challenges and the economic advantages of shared digital infrastructure.

All of these trends will continue for the foreseeable future. Organizations that fail to respond to these dynamics will become economically and competitively irrelevant. At the same time, these changes create new risks and vulnerabilities that require significant organizational change to manage.

Over the past five years, much has been made of the technical convergence of the IT and the Security functions within organizations. In fact, this convergence has primarily been little more than the migration of Security away from dedicated networks and platforms to those that share the technology and structure of IT systems. These changes have been driven by the same three dynamics that have led to the changes in data centers themselves: functionality, coordination and economics. At the present time, the three major manifestations of this convergence are:

- The use of IP networks to replace all other network technologies and topologies;
- The use of general-purpose server platforms rather than dedicated controller hardware for high-level solution management; and
- The use of general-purpose network storage to replace special-purpose video storage.

These are all meaningful, but not organizationally significant, responses to the changing technical, economic and threat environment.

We are beginning to see the emergence of a new phase of convergence of the IT and the Security functions within organizations: one that is primarily an *operational* convergence rather than a technical convergence. Although IT Security has become a more significant element of DCO consuming roughly 10% of most data center budgets, and although modern Security IT systems look, in many aspects, like data center systems, the operational aspects of IT and Security remain largely disjoint. In many senses, IT Security is inward focused – concentrating on protecting IT and informational assets – while Security IT was outward focused – concentrating on extending the utility of the IT infrastructure to address organizations physical and personnel security requirements. While these two dynamics share some common elements, they will not align to meet the overall requirements of a modern, complex, organization unless they are effectively integrated at an operational level.

Within most organizations, the scale and maturity of DCO often suggests that extending the policies and procedures that have been proven within the IT functions to the Security functions will be the most effective approach to drive the required operational convergence between IT and Security. Security, however, has essential operational requirements that are very different from those of IT and modern Security systems address critical operational needs that cannot be compromised in the convergence process. As a practical matter, therefore, this operational convergence must be addressed as an integrated solution driven by the overarching organizational needs.

### **New Security Requirements**

Organizations today face security challenges that cannot be appropriately addressed via the traditional *stovepipes* of IT Security and Physical Security. Among some of the major security challenges that require a highly integrated response are:

- Coordination of personnel, asset and facility control among distributed facilities using high performance resilient networks;
- Communication, storage and management of large quantities of video data both with and without analytic support;
- Integration of internal event information with external resources on a local, regional and national basis;
- Maintenance of real-time knowledge of the status of human and material assets and maintenance of these assets in the presence of both natural and man-made disruptive events; and
- Assessment of the consequences of disasters and the options available to the organization for reconstituting operational activities.

Although, theoretically, a number of organizational elements could assume the responsibility for meeting these security requirements, DCO controls the vast majority of the organizational assets that are required; in particular the communications

infrastructure and the data storage resources. As a practical matter, therefore, DCO will need to extend its operational responsibilities to include these new security requirements.

### **Security Solution Framework**

The design and implementation of security solutions for even moderately complex enterprises is an extremely difficult undertaking. In realistic environments, the enterprise being protected, the value distribution within the enterprise and the security threats are continuously evolving and, therefore, traditional security designs can result in solutions that, over time, are protecting the wrong assets against the wrong threats. As a simple example, a security process that is highly effective at preventing employees leaving a site with a stack of one million sheets of confidential documents is useless for preventing losing this same information contained on a flash drive that has a volume of less than 0.3 cubic inches and weighs less than 0.5 ounces.

Practical security solution design, therefore, need to accommodate that the nature of the problem that they initially need to solve is imperfectly known and that the problem will continue to evolve over the life of the system. It is also critical that these solution designs be capable of integrating new technology on a continual basis; not only for the usual reason that new technology typically enhances the cost-effectiveness of the system, but also because this new technology is available to the threat community and systems that cannot respond to technology change will rapidly be rendered ineffective.

Effective security solutions that provide long-term utility in this complex and evolving environment, therefore, require a highly structured and disciplined design approach. At the same time, it is not practical to approach every security challenge with a solution that is developed from first principles. As a practical matter, these designs must be approached within an implementation context that is, on the one hand, open and flexible while, on the other hand, is known to be cost-effective and poses low implementation risk.

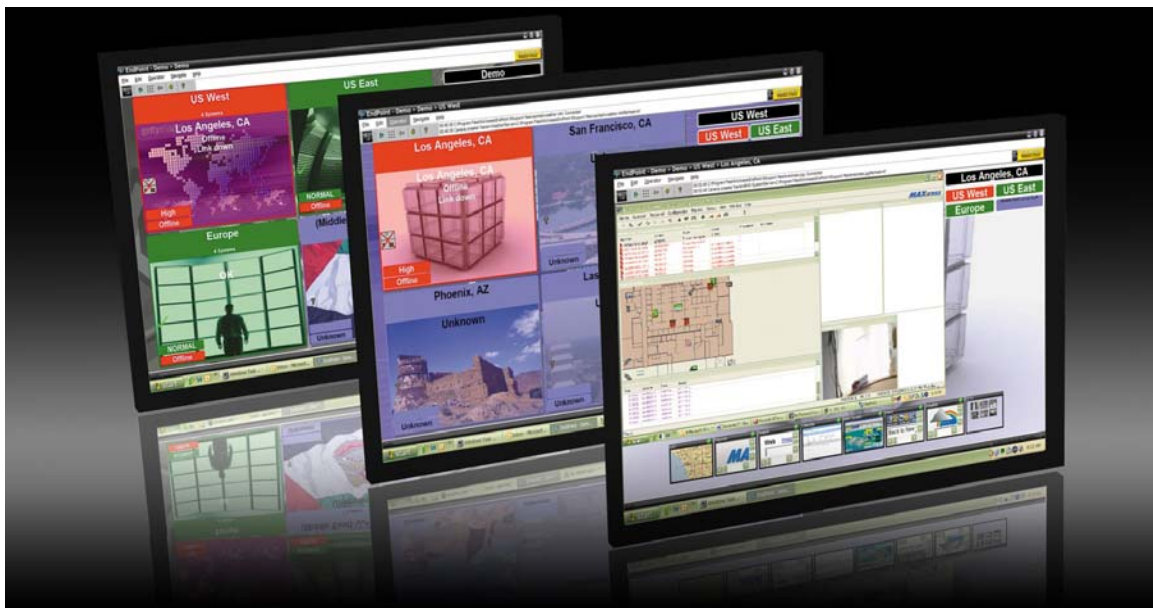
*EndPoint*, from MAXxess Systems, has been developed as a solution framework that enables the development of sophisticated security solutions in a stable technical context that enables rapid implementation of cost-effective structures that can be adapted in situ to meet specific requirements and which can continue to evolve as requirements and technology change. EndPoint has been built upon standard IT components and is designed to take maximal advantage of IT resources such as communication networks and storage resources.

### **Conclusion**

EndPoint can serve as the central framework to enable DCO to address new and evolving organizational security requirements. It can provide effective integration of IT Security into the context of overall organizational security and as a vehicle for managing

distributed resources across both the corporate WAN and the global Internet. Because EndPoint has been developed from an operational security context, it is structured to enable effective management of unplanned events and it presents and correlates information from disparate sources greatly facilitating real time decision making and response implementation.

Critically, EndPoint has been designed to accommodate ill-defined, complex and evolving requirements that are commonly encountered in operation security environments by providing a structured, but loosely-coupled architecture that can be extended and adapted as the operational environment, the available technology, the organizational requirements and the critical threats change.



***EndPoint Event Management Framework***