



1040 North Tustin Avenue
Anaheim, CA 92807
(800) 842-0221
www.maxxess-systems.com

EndPoint Solutions

Background

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.

Structured Security Design

Structured security design segments the solution design into four hierarchical areas:

- Policy
- Process
- Procedures
- Protocols

Policy is the top level of the design hierarchy. Policy requirements are typically the most stable of the requirements and guide the design tradeoffs at all of the lower levels of the design hierarchy. Ideally, the complete Policy that drives the solution design is known a priori but, as a practical matter, this is often not the case. The reason for this is that it is often extremely difficult for organizations to establish Policy outside of the context of a solution structure: to some extent, what *should* be done is influenced by what *can be* done. EndPoint breaks this vicious cycle by providing a flexible solution framework that is driven by a software policy engine. To the extent that Policy is defined at the beginning of the design process, that policy can be built into the EndPoint solution. As Policy matures or evolves, however, the EndPoint policy engine can be modified to address any necessary changes. These changes can be accomplished without any impact on the lower levels of the solution design hierarchy which represent significant investments in hardware, software, training and experience.

Process is the means of implementing Policy. If Policy is the definition of *what* to do, Process is the definition of *how* to do it. The core of EndPoint is a mature software framework that is built around three key components: a TCP/IP network-based communication structure that can be augmented, as necessary, with software or hardware gateways for interconnection with external systems; an event manager implemented as an SQL database application; and a visualization and presentation manager that provides a structured means of monitoring and controlling disparate systems and is optimized for effective response to both planned and unplanned events.

EndPoint implements these processes to the greatest extent possible utilizing Windows-based software and TCP/IP networking. This permits EndPoint to be implemented within the technology environment existing in most companies today and encourages the use of shared technical resources, particularly in the area of networking. These design choices permit highly cost-effective implementation of EndPoint and permit EndPoint to benefit from the rapid price and performance improvements that we anticipate these technologies to continue to deliver.

Procedures include both actions that can be automated and those which must be left to human response. EndPoint provides the ability to automate well-defined procedures in order to minimize the burden placed on human element of the solution. In many cases, however, it is not possible to define them appropriately or, at least, not to define them completely. The nature of the security challenge is that it is often important to respond quickly and efficiently to events that are complex, unanticipated and incompletely characterized. In these cases it is not possible to assume that pre-defined procedures will provide an appropriate response. EndPoint addresses this class of challenges by providing the human element of the solution a rich set of information that can help to provide context for human decision-making. This information may consist of event information from within the enterprise being protected, but it may also include appropriate web-based information external to the enterprise, as well as news, weather and other activity feeds from external sources. EndPoint can change the range, scope and locality of this information to best meet the specific requirements of the solution.

Protocols represent the *how* of communication, both human and automated. EndPoint is designed around standard networking protocols, so that it can operate within any well-structured TCP/IP network including Ethernet LANs, WANs, MANs and VPNs. EndPoint also utilizes a set of software and hardware gateways to accommodate the unique protocols of legacy systems and/or systems that need to be brought with the solution framework. To the extent that third-party systems utilize standard digital interchange protocols [XML, HTTP, SMTP, etc.], the effort required to incorporate these systems into the EndPoint framework will be minimized. MAXxess's extensive background in open security systems, however, has provided it broad experience in developing gateways for a wide range of systems that have unique and/or proprietary communication protocols.

It is much more difficult to provide a complete solution to the human protocol challenge. EndPoint, however, provides a set of tools [e.g. event classification, e-mail notification and structured messaging] that can assist the user to communicate effectively within the constraints of policy and process.

Conclusion

EndPoint, therefore, is a critical element in the design process for the complex solutions required to meet the security challenges of today – and tomorrow. It is also, however, the core backbone of the implemented solution itself. Because EndPoint bridges these two essential phases of the implementation of security solutions it is uniquely able to provide effective, durable solutions to the most significant security challenges facing enterprises today.