

Services Overview

Parapet Security's mission is to secure the e-infrastructure that is the foundation of your business. The goals of our service are to ensure that your communication networks, computing environment, and the applications, services and data contained therein maintain their confidentiality, integrity and availability at all times. In simple terms, our mission is to help your organization protect its secrets, have confidence that its systems are trusted and not breached, and keep its e-infrastructure functioning 7 x 24.

Full-Service

We offer a full suite of services that is comprehensive in scope and flexible in execution to fit a wide range of businesses, technological environments and requirements. Our services fall into four categories:

- **Assessment**—We comprehensively evaluate your e-infrastructure for security risks against your business strategy. We also compare it to processes and best practices established by international security standards organizations such as NIST, NSA, SANS, CISSP, CISA, ISO 17799, ISACA and the Common Criteria. We will document and recommend an action plan tailored to your business strategy, technology environment, budget and culture. We can also go beyond recommendations to help you implement those changes. Finally, we offer an Attack and Penetration Exercise in which we, with your full cooperation and knowledge, simulate different attack scenarios to test the defensive robustness of your current network, or the effectiveness of a new security project.
- **Intrusion Detection**—Our services range from recommending, sourcing and installing the most appropriate intrusion detection solution set for you, to customizing and integrating an enterprise-wide system. This service applies to clients who have an existing intrusion detection system (IDS) as well as to those who need to put one in place.
- **Intrusion Prevention**—Without secure computers, there is no e-security. We provide complete, secure host configuration and build architecture for both Microsoft Windows™ and Unix™ environments. Once platform systems are built to secure host standards, we will help you integrate specialized software to provide application-layer anomaly detection functions to supplement your intrusion detection systems. Operating further up the stack this way will curb the number of false positive alerts you receive and give you more confidence in your intrusion data.
- **Rapid Response**—In the event of an impending security event or after a breach, your security demands rapid response measures based on established triage policies and business priorities. Our foremost goal, of course, is to Contain and Continue, to minimize the severity and duration of the damage and enable the resumption of your normal business as soon as possible. Subject to your preferences, we can also implement Preserve and Prosecute mode and attempt to track down the attacker. Our security experts and engineers will work along with your system administrators and business line

managers, either remotely or on site, for as long as needed until the emergency is over. After that, we will help you analyze the problem, then recommend and implement corrective actions that will improve future detection and prevention efforts.

Hands-on Capability

Parapet's security experts, consultants and engineers have wide-ranging experience as security officers and auditors, system administrators, network architects, and consultants in both the government and private industry. Thus, we are able to offer not only consulting services but also implementation services, including design, installation and integration of hardware and software.

Multi-Layer E-Infrastructure

For each service, we deal with every layer of the infrastructure as necessary and appropriate. Some issues are layer-specific, while others affect all layers in your e-infrastructure. For example, Intrusion Detection focuses on the perimeter of the network, while guarding against internal threats involves all aspects of the infrastructure. In the Parapet Framework, there are four layers:

- External Network—the perimeter that borders the outside world, be it the Internet, VPN or extranet connected with your partners and remote employees.
- Internal Network—the multitude of networks within your enterprise and its many departments, divisions and locations.
- Hosts—the pervasive pieces of networked equipment such as computers of all classes, servers of all types, and peripherals (printers, fax machines, external modems).
- Services, Data and Applications—the services (e-mail, printer, databases, payroll, etc.), software and information residing in the hosts, the “crown jewels” of your enterprise, that are the prime targets of most attacks. It is damage in this layer that causes you the most financial loss and public embarrassment, and requires the longest time to repair and restore.