



▶ Delivering a Security Application for the Web



A manufacturer of security appliances was looking to branch out into the internet security space, and selected Emtec to develop critical components of their software for a new product line.

The Challenge

This security appliance manufacturer saw that traditional gateway defenses were proving to be inadequate against a variety of malware, leaving many corporate networks exposed. To combat this issue, they began development of a new product line of security appliances that would enable secure web traffic for companies of all sizes. They called upon the expertise of Emtec to help.

Emtec Solution

Emtec created a highly scalable, server-side software solution to crawl, analyze and pre-compute threat ratings for URLs. This critical piece of infrastructure is deployed at a client's data center and communicates with the threat database maintained by the manufacturer. The crawler takes URL feeds as input, crawls the actual web site, analyzes the content, and generates threat ratings. The crawler infrastructure is designed to be flexible and scalable, allowing for highly granular, policy-based configuration at both at the domain level as well as the individual URL level.

The URL analysis and threat computations are implemented in the form of plug-ins, each designed to analyze a specialized type of exploit. In addition, the plug-ins can be dynamically loaded into the crawler at run time. As a result, adding support for newer threats only requires development of an additional plug-in, with no changes to the core system. The crawler is also architected to allow for URL feeds in various formats, so adding support for additional URL feeds involves writing a simple program that converts the feed to a standardized intermediate format.

To support the sheer amount of URLs to be crawled, a distributed system including a distributed database as well as a distributed execution engine, was employed which enables near linear scalability with the client's hardware. Sophisticated monitoring and administration capabilities were also provided to help the data center administrator manage a production system. The solution was developed by the Emtec team utilizing Python and MySQL running on FreeBSD.

The full solution that our client brought to market is comprised of a security appliance deployed onsite at a client, and software infrastructure deployed at the manufacturer's datacenter maintaining a massive database of pre-computed threat ratings for URLs.

Outcome

Emtec successfully designed and developed a high performance security solution for integration into a line of security appliance products. With its flexible and scalable architecture, the software allows the addition of future features, giving the products a longer lifecycle as well as an ability to support countless devices. Our partnership with this security appliance manufacturer has produced a unique outbound threat monitoring system with comprehensive management and reporting capabilities that has extended web security beyond the traditional proxy and URL filtering preventing spyware from ever entering the network.

Established in 1964, Emtec, Inc. is a systems integrator that provides IT services and products to the federal, state, local, education and commercial markets. Our market leading value-based management methods, coupled with best-in-class IT technology, consulting and development services, address a wide range of specific client needs, as well as support broader IT transformation initiatives. Emtec's service capabilities span the United States, Canada and countries around the globe.