2009 North American Product Innovation Award

Cyber Security Technologies Corporation

The 2009 Frost & Sullivan North American Product Innovation Award in the field of computer forensics goes to Cyber Security Technology Corporation in recognition of the development of the Online Digital Forensic Suite™ (OnLineDFS™), an intelligent software solution for next generation live computer investigations. Computer forensics helps solve cyber crimes, resolve IT security incidents and support e-discovery by investigating the electronic data stored on live computers. The information retrieved can be used to help prosecute these crimes. This tool, based on a patented technology, is cost effective, easy to deploy and manage, while also offering quick investigative capabilities for live networked computer systems. OnLineDFS™ requires no pre-installed software to perform a live computer investigation and these investigations can be conducted discretely without disrupting other operations.

Company Background

Headquartered in Eden Prairie, Minnesota, Cyber Security Technologies is an affiliate of Architecture Technology Corporation which develops affordable next generation software solutions for live investigations of computer systems connected in a network. The company's products are widely used in IT applications for governments, corporations, law enforcement, military, and intelligence investigators. The company targets three markets, namely, investigation of live computer systems in a network, automating the detection and analysis of peer-to-peer (P2P) client programs and files, and automating investigations of Mac OS X systems.

Product Description

Computer forensics involves searching, preserving, and analyzing information on a computer system which can later serve as evidence in a court of law. A number of key cases have been won on account of the electronic evidence that has been recovered and as both software and computers continue to evolve, the computer forensics field is becoming a critically important domain.

OnLineDFS™, the company's flagship product, is a tool that is employed for rapid and cost-effective incident response and forensic investigations of live computers in networked environments. This tool captures and records volatile data that could be lost if a system is shut down. It can automatically examine selected systems on a scheduled basis and acquire information on running programs, network connections, data transmissions, memory, and registry. OnLineDFS™ is structured on a patented two tier architecture where the OnLineDFS™ server that provides functionality through a web based server constitutes the first tier, and the second tier is the investigator's module. The OnLineDFS™ server is installed in a secure environment within the

network and also manages the investigations. The investigator's module is available in two configurations: a Single-User Version and a Multi-User Version. As the name suggests in the Single-User Version, the investigator works directly at the server machine with only one investigator having access to OnLineDFS™ at a time. In the Multi-User Version, the investigator can work from a remote location and access OnLineDFS™ via a web interface. This configuration allows for up to 6 investigators to perform investigations simultaneously. Upon completion of the investigation, the data that has been collected from the target computer is displayed in the form of tables in a web browser for the investigator so as to make it easy to view and interpret.

OnLineDFS™ is designed for IT security professionals and investigators in government agencies, law enforcement, and in corporations for incident response, e-discovery, compliance, and criminal investigations in both live and networked environments.

Competitive Advantages

Most existing computer forensics solutions are invasive in nature, wherein the target computer device is investigated by physically connecting a forensic analysis device to it. Such a solution would require physical seizure of the target computer, which in some cases can prove to be troublesome to other users on the network depending on the criticality of the system being investigated.

Contrary to this, the OnLineDFS™ architecture has the ability to conduct live investigations without the need for pre-installed software on the computer being scrutinized. This tool is capable of conducting live investigations discretely without disrupting operations and can examine mission-critical systems without causing downtime. The system under investigation can be in active use or may also be unattended at the time of investigation and can be located anywhere in the network with distances ranging from a system in the next room to one connected thousands of miles away.

The company's patented two-tier architecture is easy to deploy and manage thus making it a very cost effective solution. As a plug-and-play tool, OnLineDFS™ gives security professionals and law enforcement officials enterprise-wide reach for any computer in a specific network. It can be accessed by investigators either remotely or using a secure (SSL) connection capable browser such as Microsoft Internet Explorer 4.0 or higher, Mozilla Suite, or Netscape Navigator 4.0 or higher. An additional feature seen with the OnLineDFS™ is that the data collected is stored in non-proprietary formats thereby facilitating the use of third party tools to analyze the data.

IP & Business Strategies

Cyber Security Technology Corporation has a highly experienced management team that comprises of executives with backgrounds in both the security and enterprise software fields. In March 2009 the US Patent and Trademark Office issued a patent for the core technology that the OnLineDFS™ is based on (US Patent No. 7,496,959). The company distributes its products directly and through a worldwide reseller network.

The company offers two other innovative software products, P2P Marshal™ and Mac Marshal™ that offer automatic investigation and analysis of challenging situations. P2P Marshal™ is an automated computer forensics tool that can significantly reduce the time taken to conduct a P2P investigation. This tool automatically detects and identifies P2P clients, files that have been downloaded and shared, and peer servers that were contacted in order to do so. It analyzes P2P usage on file system images and can perform a complete analysis for LimeWire, BitTorrent, uTorrent, and Azereus. One of the advantages of using P2P Marshal™ is the reduction in time required to carry out an investigation by automating the analysis process.

Mac Marshal™ is a newly launched product that performs investigation of hard drive images of computers running the Mac OS X operating system and other Mac specific applications such as Mail, Safari, iChat, Quick Time player, and so on. This product, like the P2P Marshal™ is equipped with a high degree of analytical intelligence and automation capabilities that helps in considerable time savings as well as cost to ferret out the needed forensic evidence.

Conclusion

In recognition of the company's contribution to the field of computer forensics with the OnLineDFS™ tool for the investigation of live computer systems connected in a network, Frost & Sullivan is pleased to present the 2009 North American Product Innovation Award in the field of computer forensics to Cyber Security Technologies Corporation.

Award Description

The Frost & Sullivan Award for Product Innovation is presented each year to the company that has demonstrated excellence in new products and technologies within its industry. The recipient company has shown innovation by launching a broad line of emerging products and technologies.

Research Methodology

To choose a recipient of this Award, the analyst team tracks all new product launches, research and development spending, products in development, and new product features and modifications. This is accomplished through interviews with the market participants and extensive secondary and technology research. All new product launches and new products in development in each company are compared and evaluated based on degree of innovation and customer satisfaction. Companies are then ranked by number of new product launches and new products in development.

Measurement Criteria

In addition to the methodology described above, there are specific criteria used to determine final competitor rankings in this industry. The recipient of this Award has excelled based on one or more of the following criteria:

- Significance of new product(s) in its industry
- Competitive advantage of new product(s) in its industry
- Product innovation in terms of unique or revolutionary technology
- Product acceptance in the marketplace
- New product value-added services provided to customers
- Number of competitors with similar product(s).

About Best Practices

Frost & Sullivan Best Practices Awards recognize companies in a variety of regional and global markets for demonstrating outstanding achievement and superior performance in areas such as leadership, technological innovation, customer service, and strategic product development. Industry analysts compare market participants and measure performance through in-depth interviews, analysis, and extensive secondary research in order to identify best practices in the industry.

About Frost & Sullivan

Frost & Sullivan, the Growth Consulting Company, partners with clients to accelerate their growth. The company's Growth Partnership Services, Growth Consulting and Career Best Practices empower clients to create a growth focused culture that generates, evaluates and implements effective growth strategies. Frost & Sullivan employs over 45 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from more than 30 offices on six continents. For more information about Frost & Sullivan's Growth Partnerships, visit **http://www.frost.com.**

www.awards.frost.com