

New Technology and Services to Enhance the Business Value of Your IT Network

Progent's IT Connection Newsletter

Progent

Highlights

- Progent's *E-mail Guard* blocks spam, viruses and Directory Harvest Attacks via Postini's managed services
- Have equipment at an Internet Data Center? Progent offers on-site and remote support
- Windows XP Service Pack 2 includes new security technologies to defend against *malware*
- If you need help with Cisco technology, ask Progent to provide a certified expert
- For recommendations about great sources for hardware and software, give a call to Progent's Vendor Network
- Progent's Technical Response Center now offers desktop support

E-Mail Guard Managed Services NEW PRODUCT Block Spam, Viruses, Directory Harvesting

Spam now accounts for four out of five email messages. The spam epidemic seriously degrades the business value of your IT network by lowering productivity, slowing system performance, distracting IT management, and adding stress to the work environment. To solve this problem, Progent has partnered with Postini to offer small businesses *E-Mail Guard*, a

(Continued on page 4)



Progent's Expert Support Now IT SOLUTIONS Available at Major California Data Centers



Internet Data Centers offer companies of any size an economical way to achieve a secure, fault-tolerance environment for mission-critical equipment. Data centers house web and email servers, switches, routers, modem racks, mass storage and other equipment. Progent's **Data Center Support Services** provide expert on-site and remote support for businesses who use data centers in Northern California.

(Continued on page 2)

Windows XP Service Pack 2: WINDOWS NEWS Security Takes a Quantum Leap

Windows XP Service Pack 2 (SP2) incorporates a massive revamping of the core security architecture of Windows XP. The security technologies built into SP2 represent a quantum leap in Windows XP's ability to resist malicious attacks.

Windows XP SP2 addresses areas that have been the main targets of malicious software — what Microsoft calls

(Continued on page 3)



Progent Support Available at Major California Data Centers

(Continued from page 1)

Data Center Support Services

Progent's data center support services are designed for companies with equipment located at Internet Data Centers (IDCs) and in need of on-demand on-site and remote support from Microsoft and Cisco certified experts.

Progent offers a full range of data center and collocation support services, including system architecture evaluation, Windows and Linux server installation and setup, troubleshooting for server and communications infrastructure, developing and deploying fault tolerant configurations, architecting and implementing layered security structures, firewall implementation and troubleshooting, configuring load balancing environments, and deployment of fault tolerant cluster configurations.

24x7 Monitoring

Data center customers can leverage Progent's Microsoft Operations Manager subscription service to get 24x7 server and application monitoring that goes far beyond simple connectivity monitoring. The Technical Response Center can respond proactively to

detected failures before they progress to serious system problems. Progent offers expert remote troubleshooting for fast and cost-effective problem resolution, or if necessary Progent can dispatch certified engineers to the data center for on-site service.

Progent's expert support resources are an economical alternative to the managed services packages provided by many data centers because you pay only for the support you need when you need it. No minimum retainers or monthly support contracts are required.

Experts in Data Center Support

Because Progent's consultants have many years of experience working with dozens of data centers in Northern California, Progent can communicate efficiently with their engineering, network administration and facilities management teams in order to expedite service requests and escalate problems for speedy resolution.

If you are looking to move to collocation for the first time, Progent can design, architect and spec out a complete solution that will meet the your business, technical and budgetary requirements, while adhering to the best practices

for data center deployed solutions. Critical elements such as fault tolerance, remote management, data protection and backup, and hardware support can all be managed by experts with years of field-proven hands-on experience that allows them to know which solutions work and which don't. Progent can manage your entire migration into the data center, including comprehensive project management services to ensure a seamless move with minimal disruption of business.

You can use Progent's data center experts as a backup to your in-house IT support resources or as a second-level escalation resource for complex infrastructure or server problems. Progent's philosophy of encouraging knowledge transfer from our certified experts to our customers IT personal ensures that our clients get the best value for their IT support investment.

Progent can help you select a data center for hosting and collocation that meets your specific technical requirements, connectivity options, desired service response levels, corporate security standards, application-specific redundancy and fault tolerance goals, budgetary restrictions, and geographic proximity needs.

Collocation facilities features and pricing can vary dramatically. To help you make the best decisions for your business, Progent's experts can educate you on the options and choices with more than 100 data center options available in Northern California.

Contact Progent for Data Center Support

For support for equipment located at a data center or for help planning a data center strategy, call **800-993-9400** or send email to **information@progent.com**



Windows XP Security Pack 2 Beefs Up Security

(Continued from page 1)

“malware.” These critical security areas improved by SP2 include Remote Procedure Calls (RPCs), DCOM, Windows Firewall (previously called Internet Connection Firewall or ICF), and preventing the execution of any malicious, unauthorized programs.



Microsoft groups security enhancements of SP2 into five categories. Although these technologies do not eliminate the need for promptly downloading periodic security updates from Microsoft, they do bolster the core ability of Windows XP to defend against malicious attacks.

1. Network Protection

These security technologies help provide better protection against network-based attacks, like MSBlaster, through enhancements to Windows Firewall and a reduced RPC attack surface. SP2 innovations include:

- Turning on Windows Firewall in default installations
- Closing ports except when they are in use
- Improved user interface for configuration
- Improved application compatibility when Windows Firewall is activated
- Enhanced Windows Firewall enterprise administration through Group Policy
- Reduced RPC attack surface
- Added restrictions on access control of DCOM infrastructure to reduce exposure to network attack



2. Memory Protection

Some attacks try to cause excessive data to be copied into computer memory, causing what are called buffer overruns or overflows. SP2 reduces the vulnerability of Windows to buffer overflows by protecting memory using tags that either allow or deny executables to launch. This No Execute (NX) scheme is currently supported by AMD Athlon and Opteron chips. The newest Intel Prescott-based Pentium 4 chips will also support NX.

Hardware-enforced Data Execution Prevention (DEP) uses the CPU to mark all memory locations in an application as non-executable, unless the location explicitly contains executable code. This way, when an attacking worm or virus inserts program code into a portion of memory that is marked for data only, an application or Windows component will not run it.

3. Safer Email Handling

New SP2 security technologies help stop viruses such as SoBig.F that spread through email and instant messaging. More defensive default settings and better attachment control isolates potentially unsafe attachments before they harm other parts of the system.

When Internet Explorer analyzes the content of a Web page or downloaded file, it decides how to handle the



file based on the MIME type assignments and an analysis of the content itself. SP2 automatically renames a file to match its true content before placing the file in the Internet cache. It also prevents promoting one MIME type to another (text to HTML, for example) if the second MIME type has additional functionality.

4. Enhanced Browsing Security

Windows XP SP2 includes security enhancements to Internet Explorer which provide improved protection against malicious web content. For example, the Local Machine zone is locked down to guard against running hostile scripts and block harmful web downloads. Better user controls and interfaces help prevent malicious ActiveX controls and spyware from running without the user's knowledge.

5. Improved Computer Maintenance

SP2 introduces the Security Center to provide a central location for information about your computer's security. SP2 also includes the new Windows Installer, which provides more security options for software installation.

How Progent Can Help

Windows XP Service Pack 2 is available for free downloading from Microsoft's web site. Progent's Microsoft-certified consultants can assist you in planning a pilot evaluation of SP2 or a company-wide deployment. Progent can also help you understand how this important new software can benefit your business. For more information, call Progent at **800-993-9400**

**Subscribe to the
IT Connection Online**

SUBSCRIBE

To receive the *IT Connection* newsletter online, send your email address to **subscribe@progent.com**

Progent's *Email Guard* Uses Postini's Managed Services to

(Continued from page 1)

managed service that stops spam and email-borne viruses before they can penetrate your corporate firewall.

E-Mail Guard handles the security and management of corporate email by providing continually updated spam and virus filtering, content filtering, and protection from email-based directory harvesting and denial of service (DoS) attacks. *E-Mail Guard* also includes monitoring, reporting and content management tools plus outbound filtering to help you troubleshoot your email system and define and enforce corporate email policy.

E-Mail Guard is based on Postini's Perimeter Manager, a pass-through service which routes all your email to secure, fault-tolerant data centers — the same ones used by Google, eBay and Yahoo — where messages and attachments are screened using heuristic rules analysis. Clean email is forwarded to your email server, and suspicious email is tagged and delivered or quarantined to a web-accessible storage area for you to review. *E-Mail*

Guard can be set up quickly and works with any email system by redirecting your mail exchange (MX) record.

The *E-Mail Guard* service suite includes:

- **Spam Filtering** using heuristic-rules that analyze sender's IP address and message content
- **Real-Time Virus Protection** with customizable filters and quarantine areas for safe review
- **Attachment Filtering** for policy-based blocking, re-routing or trusted partner pass-through
- **Connection Manager** to block invalid SMTP connection attempts and Directory Harvest Attacks
- **Delivery Manager** for load balancing and for storing messages in case your email server fails
- **Event-Based Alerts** to notify your administrator instantly during attacks and system outages
- **Real-Time Monitoring and Graphic Reports** for web-based views of system status and usage

Advantages of *E-Mail Guard*

Filtering email at the desktop, server or gateway wastes network bandwidth, disk storage and IT management time. *E-Mail Guard* uses Postini's Perimeter Manager to stand between the Internet and your corporate network, preserving both your system and personnel resources. Because Postini's full-time security experts continually update filtering policies and virus databases, your email system always has the most current security technology without the intervention of your IT staff.

Perimeter Manager can also improve your email reliability. Postini's data center uptime averages 99.999 per-

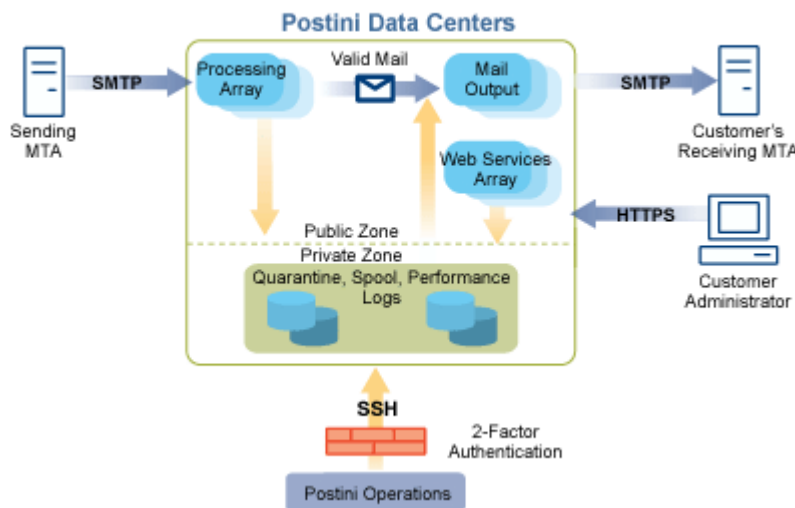
cent, far higher than small business email servers can expect to achieve. If your email server fails, messages are temporarily stored in a secure database at a Postini data center for delivery once you're back on line. Perimeter Manager's load balancing technology restores recovered email by sending it at a measured pace in order to prevent your email server from being overwhelmed.

Perimeter Manager is also a powerful defense against Directory Harvest Attacks (DHAs). This is an aggressive technique used by spammers to gather employee email addresses by running scripts against email servers. DHA propagation is the primary driver behind the dramatic growth in spam targeted to corporate email users.

Benefits of *E-Mail Guard*

- Accurately filters email to eliminate spam and viruses
- Secures your email system from Directory Harvesting Attacks and Denial of Service Attacks
- The Managed Service strategy keeps spam and viruses outside your firewall, increasing network performance and reducing stress in the work environment
- Compatible with any email system — no hardware or software to purchase, install, manage or upgrade
- Automatic updating of managed services frees up your IT management staff

Postini Data Center System Architecture



Block Spam, Viruses and Directory Harvest Attacks

(Continued from page 4)

Key Features of E-Mail Guard

- Secure external buffer stops unwanted or malicious email before it reaches your corporate firewall
- Monitoring, management tools and graphic reports give you detailed visibility of all your corporate email traffic
- Email policy, content and attachment management, plus outbound email filtering help you define and enforce your company's email policies
- Easily customizable by end users
- Fail-safe architecture ensures no message is lost if your email server fails
- Continual development, implementation and review of security policies and standards by Postini's full-time staff of information security experts
- Information security policies and programs are built around the ISO 17799 specification, the standard for enterprise computing
- Good email is delivered instantly because filtering is done in memory, not on disk

How Progent Adds Value to Postini's Services

Progent is a Postini aggregator and support specialist. If your business is too small to qualify for a standard Postini license, you can still have access to Postini's Perimeter Manager services via Progent's *E-Mail Guard* service program. Progent's email security experts can help you develop a comprehensive email security strategy that addresses spam and viruses. Progent can also help you plan and implement a phased rollout of Postini's services, select spam filters specific to department needs to reduce the risk of false positives, develop auditing and reporting practices, train your management, educate your end users on how to avoid spam and prevent virus propagation, and define an enforceable corporate email policy aligned with your business goals. Progent can upgrade, troubleshoot, and monitor your entire email and network infrastructure based on industry best practices plus Progent's experience as certified Microsoft and Cisco experts.

Progent's Microsoft-certified consultants offer on-site computer help and IT consulting services for Exchange Server 2003, Windows Server 2003, and for the entire family of Microsoft Servers. Progent's migration, integration, update, and support services include planning and system design, installation and deployment, project management and documentation, onsite and remote technical support and troubleshooting, help desk services, security consulting, and outsourcing.

Why Does Progent Recommend Postini?

Gartner Research has recognized Postini as the number one spam filtering Managed Service Provider (MSP) with respect to the ability to execute. Postini's administrative tools were recently cited by PC Magazine as the most advanced of any of the corporate anti-spam solutions they have reviewed, and in Network World's test of 16 anti-spam products Perimeter Manager scored the highest in accuracy for catching spam and delivered the lowest false-positive rate.

Postini processes over 1 billion messages weekly for over 2,700 customers and serves over 5 million end-users. The high volume of email processed makes Postini's heuristic filtering engine continually more refined and efficient, and the company's large customer base gives the Postini staying power that protects your investment in managed services.

Preserving Email Privacy

E-Mail Guard does not require users to provide personal contact or demographic information. Customers can deactivate services at any time by turning application settings off. Progent and Postini never sell or make available individual names, lists of users, or aggregate data to any third parties for gain. User configuration information provided to Postini is used explicitly to deliver services that match the client's requirements and not for any other purpose. All user-specific information and email message information, including content, addresses, categorizations and IP addresses, are kept strictly confidential.

Impact on Email performance

Unlike store-and-forward solutions that use standard email server technology, Postini's patented email processing method allows messages to be processed in real-time as the packets flow through the Postini servers. This also ensures that Postini does not expose customer data to hackers or potential loss of data. Postini's filters process all email with no direct human contact with mail flow or individual messages. Mail messages are processed within milliseconds and immediately passed through to your email server. This eliminates any perceptible latency.

Contact Progent for Email Solutions

If you are interested in using Progent's *E-Mail Guard* managed services or if you need Progent's consulting services to fix or enhance your email system or help you develop a complete security strategy, call Progent at **800-993-9400** or contact **information@progent.com**

Postini's Spam Filtering Technology

TECHNOLOGY FOCUS

Progent's *E-Mail Guard* is based on Postini's managed services, which utilize patented pass-through technology versus store-and-forward methods for blocking spam, email-borne viruses, Directory Harvesting and Denial of Service Attacks.

Under Postini's approach, email bound for your email server is processed in real-time through Postini's secure Email Processing Center. Postini's Connection Manager uses heuristic rules analysis to identify patterns of behavior associated with Directory Harvest Attacks (DHA) and immediately rejects DHA messages. Postini's Content Filter then separates spam and viruses from legitimate messages using an in-memory process that takes only milliseconds. Valid email is instantly passed on to the destination mail server. Email suspected of containing spam or viruses can either be quarantined in a web-based, password-protected message center for review by an administrator or end-user, or tagged and delivered.

The entire process is fully automated. Valid email passes through and cannot be physically accessed by any persons other than the recipient.

Postini's system architecture is divided into public and private security zones. The Public Zone processes the flow of email and handles customer web access. Access to the web-based administrative console, for company administrators, or to the message center for end-users, is handled through Secure Socket Layer (SSL) sessions, an industry-standard public key cryptography methodology for authentication and encryption. Both passwords and data are encrypted before transmission.

The Private Zone is reserved for storing quarantined messages and customer profile and preference information. All user information and user configurations are processed automatically by software. Postini employees do not review this data. Only authorized services are allowed to traverse the two networks, and only authorized personnel are allowed access to the private network.

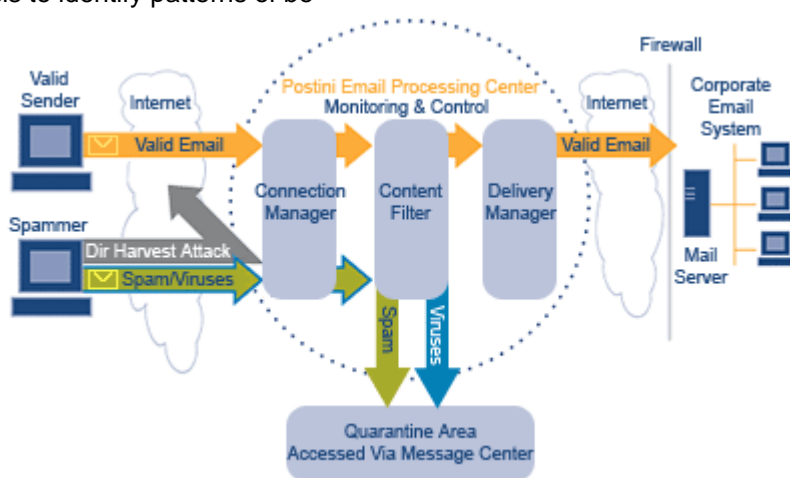
Some Spam Filtering Terms

Denial of Service Attacks (DoS)

An attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

Directory Harvesting Attacks (DHAs)

Scripted attempts to steal directory. Spammers send messages with various names to SMTP mail servers until the server accepts a name, then sell the name.



Email Perimeter

The point where control of email passes from the enterprise to the Internet.

False Positive

A valid email falsely identified as spam.

Firewall

System designed to prevent unauthorized users from accessing private networks connected to the Internet.

Heuristic Rules Analysis

A branch of artificial intelligence whereby self-learning programs improve with experience. With spam filtering, the more messages processed the better the results.

Load Balancing

In the context of spam filtering, the measured release of messages from a filtering service to an enterprise email server so as not to overload the server. This is an important feature of email business continuity service.

Managed Services

Outsourced IT infrastructure services such as spam and virus filtering.

MX Record

Mail exchange record, an entry in a domain name database identifying the mail server responsible for handling emails for that domain name. The MX record must be redirected to the outsourcer for external spam filtering.

Pass-through Filtering

Remote email filtering performed in memory before being passed on to its intended destination. A faster and more secure technique than store-and-forward filtering.

Call Progent for Cisco Technology Expertise

NEWS BRIEFS

As a Registered Partner for Cisco Systems, Progent can provide clients in Northern California with the services of Progent's on-staff Certified Professionals and Special-



ists who have training and field experience in designing, deploying, configuring, maintaining and troubleshooting networking solutions based on Cisco's industry-leading technology.

Progent's experts can deploy Cisco technology to offer small businesses access solutions that incorporate basic, high-speed, integrated, and remote networking. Progent has experience with Cisco's dialup, cable, DSL, telephony, and remote access

products. Progent's staff experts can also design and deploy Cisco Aironet wireless networking infrastructure including 802.11-based solutions to serve the needs of small workgroups or entire enterprises with office-to-office and building-to-building connections.

Cisco's industry-leading selection of networking hardware supported by Progent includes switches, hubs, firewalls, VPN devices, wired and wireless interfaces and modules, and storage networking product families. Because Progent is a Registered Partner for Cisco, Progent has access to the latest learning tools and training programs to stay at the leading edge of Cisco's network technology.

Contact Progent for Cisco Expertise

If you need help with Cisco technology, call Progent at **800-993-9400** or contact information@progent.com

Technical Response Center Offers Desktop Support

Progent's Technical Response Center was originally established to offer 24x7 phone support plus remote troubleshooting and network administration to businesses with Windows-based networks anywhere in the United States. Now individuals in need of emergency desktop assistance can call Progent's team of Microsoft-certified experts.

Progent's phone support services are available on an hourly basis, so you pay only for the services you use.

There is no minimum commitment and no retainer required. Easy payment options include VISA, MasterCard, American Express, and Discover.



To get started or to find out more about Progent's Technical Response Center, just call Progent at **888-412-5546** or visit the TRC web at www.progent.com/nationwide_remote_support.htm

Progent's Vendor Network Knows Where to Buy IT Products

Progent is well known in Northern California for helping small businesses determine the most appropriate IT products to buy and for integrating software and hardware into business networks. Now Progent can also help you select the most appropriate vendor.

With more than 15 years experience providing IT consulting services, Progent has developed a team of vendors of key software, hardware and services. Progent's **Vendor Network** is a group of manufacturers, software publishers and product resellers who consistently offer good prices, on-time delivery and effective support.

Because Progent has established excellent relationships with companies in the Vendor Network and has in many cases received formal training, Progent can offer expert integration and configuration services and, when necessary, can facilitate warranty repair. Progent can also advise you about product quality and support issues and can recommend reliable second sources for business-critical products.

Find Out More About Progent's Vendor Network

If you need help with Cisco technology, call Progent at **800-993-9400** or contact information@progent.com

PROGENT

560 S Winchester Blvd, 5th Floor
San Jose, CA 95128

Phone: 800-993-9400

Fax: 408-240-9450

Email: information@progent.com

Progent

*Helping small businesses build
and maintain IT networks based on
Microsoft and Cisco technology*

**This newsletter is available online at:
www.progent.com**

*The IT Connection from Progent is an online newsletter that updates you about important new budget-friendly products and services for improving the business value of your network. Visit Progent's web site at **www.progent.com** and find out how these new developments can help make your small business IT network more secure, more manageable and more productive.*