Why a *host-based intrusion defense system* -- with deep packet inspection — is the “last line of defense” for your mission-critical servers

Dear [NAME]:

What will happen to your business when a cyber-attack penetrates your firewall and other network defenses — and hits your mission-critical servers head-on?

It could result in costly and embarrassing service disruptions … down-time … lost productivity … stolen data … regulatory fines … angry users … and irate customers.

That’s where **Deep Security** — Third Brigade’s host-based intrusion defense system — can help.

Yes, firewalls intrusion detection/intrusion prevention (IDS/IPS) and other network defenses are important. But the ultimate protection … the last line of defense for mission-critical servers … is Deep Security, our host-based intrusion defense system.

Third Brigade Deep Security detects and prevents attacks. It resides on the server with the applications it protects. Dozens of enterprises — including Bell West, CitiStreet, and Workstream — already rely on Third Brigade to stop computer security breaches for thousands of mission-critical servers.

Reason: in today’s threat environment, hackers have more ways than ever to penetrate or bypass your network defenses. Mobile computers can be compromised when they leave the perimeter, and be used as launching points for sophisticated attacks the next time they connect to the network. SSL and other encryption techniques can blind network scanning devices, allowing attacks to tunnel all the way to the host.

Looks deep inside data packets for threats

Third Brigade’s high performance, deep packet inspection engine enforces security profiles that are configured for each host by monitoring all inbound and outbound traffic streams for malicious code, contents that might signal an attack, and policy violations. Deep Security insps everything from the packet header down to the payload.

Good data is permitted to pass. Bad data is blocked. And suspicious data is neutralized.

Blended approach reduces false positives

Third Brigade uses a unique, multi-tiered approach to security. It combines an ICSA-certified firewall, exploit filters, vulnerability filters, smart filters, and custom filters to dramatically reduce false positives — minimizing time spent chasing down alarms triggered in error, compared to other solutions.

An instant shield against zero-day attacks

Deep Security's IDS/IPS filters prevent known vulnerabilities from being compromised by new exploits for which signatures do not yet exist. A conventional signature-based intrusion prevention system can't recognize these threats — and lets the bad packet through.

Third Brigade's rapid response team of security experts continuously monitors the latest vulnerabilities. New filters are developed and delivered to protect your servers against these critical vulnerabilities within hours of their announcement. You can automatically or selectively apply these updates to thousands of servers — in minutes — without a system reboot.

Protects every server in your data centers

Deep Security protects Windows, Linux, and Unix operating systems … servers (database, e-mail, Web, FTP, and others) … enterprise applications, and custom Web applications — giving you a single source for all your host intrusion defense needs. Plus, our software is up to 10 times faster than Snort-based systems.

FREE IT security guide!

In our just-published IT security guide, "Web Application Security: The Overlooked Vulnerabilities," we'll show you how you can keep your critical systems — especially online applications (60% of which have an exploitable vulnerability, according to Gartner) — safe with host-based intrusion defense.

To get your FREE guide … and a FREE Information Kit on Third Brigade's host intrusion defense solution … just complete and mail the card enclosed. For faster service, call toll-free **866-684-7332.** Or download your free guide here: **www.thirdbrigade.com/was**

Sincerely,

Brian O'Higgins, Chief Technology Officer
Third Brigade, Inc.

P.S. To arrange a free, no-obligation "vulnerability assessment" revealing where your web applications are most susceptible to attack, call us toll-free at 866-684-7332 today.

THIRD BRIGADE®
deep security solutions

11710 Plaza America Drive
Suite 2000
Reston, Virginia 20190
USA