



CUSTOMER SUCCESS STORY: WORKSTREAM, INC.

PROTECTING MISSION CRITICAL HR APPLICATIONS

“Our unwavering commitment to delivering a superior, consistent, secure end-user experience is integral to our growth and success. Third Brigade® Deep Security helps ensure the 24/7 availability of our mission-critical web applications, protect sensitive customer data, and allow us to more quickly deliver best-of-breed products and services to our customers, while maintaining the highest security standards.”

Mike Gioja, CIO, Workstream

CUSTOMER PROFILE

Workstream helps companies cost-effectively manage their entire employee lifecycle, from recruitment to retirement. Workstream has over 400 clients including Visa, Dell and Nike. Workstream’s Enterprise Workforce Management applications are delivered on-demand, allowing organizations to better manage their high-performing workforces, while controlling costs. At the center of the solutions is a web-based portal that aggregates and integrates all of the resources relevant to workforce management. A state-of-the-art data center hosts these applications and ensures security for client data and 24/7 application availability.

BUSINESS CHALLENGE

Over the past five years, Workstream has acquired 15 companies and more than 20 applications, creating a heterogeneous IT environment, with a wide range of operating systems, clustered databases, virtualized web servers, and custom-built web applications provided via Software as a Service (SaaS). Although these systems are protected by firewalls, anti-virus, and other layers of network security, the company recognized it needed to complement these approaches, and move to the next level.

“Security threats are constantly changing,” noted Mike Gioja, CIO of Workstream. “We need to stay

ahead of the threat, and further enhance our security posture to ensure we are protected from new types of attacks and exploits.”

For compliance reasons, Workstream needed to demonstrate to its customers that their applications and data are proactively protected, and that the company is using security best-practices to minimize the risks of an attack. And like most companies, it needed to do this quickly, without imposing significant management overhead, or impacting application availability and performance.

THIRD BRIGADE SOLUTION

Third Brigade Deep Security is an advanced, host-based intrusion defense system that brings proven network security approaches, including firewall and intrusion detection and prevention, down to individual networked computers and devices. It protects operating systems, infrastructure software and applications from attacks that exploit software vulnerabilities.

Recognizing the demanding nature of the business and technical environment, Workstream and Third Brigade professional services together developed and implemented a staged deployment plan. Security profiles, which specify the protection to be configured and enforced automatically for one or more hosts, were successively tested and tuned in a development



Host Intrusion Defense Systems

Third Brigade Deep Security was architected to support the demanding, operational requirements of companies like Workstream that have high standards and expectations with respect to the performance and availability of their custom-built applications.



CUSTOMER SUCCESS STORY: WORKSTREAM, INC.

and pre-production environment, for each application, before being applied to the production system. At each of these three stages, the team first ran the system in detect-only mode, before switching it to prevent mode, with the firewall. Through this approach, the security profiles were further tuned at the application and sub-module level to maximize their effectiveness. This also allowed the team to demonstrate to key stakeholders that the addition of this important layer of security had no noticeable impact on performance or availability.

“Our approach to intrusion defense is fundamentally more robust and practical for enterprises that need to protect high value, high risk servers and applications,” said Brian O’Higgins, CTO of Third Brigade. “It provides rapid, multi-platform protection, while minimizing the total cost of ownership and impact on hosts and administrators.”

Third Brigade’s high performance deep packet inspection engine examines all traffic streams for malicious code and other anomalies. This allows it to detect and prevent a broad range of attacks—including SQL Injection, Buffer Overflow, and Cross-Site Scripting. The centralized management system is used to create and manage security profiles, and track threats and preventive actions taken in response to them.

With Deep Security, detailed, information-rich reports can be automatically generated and delivered to key stakeholders, to highlight relevant security metrics. For example, executive-level reports can be delivered monthly, to provide summary information that can be used with end customers. Also, application owners can receive reports that address their specific interests, on a weekly basis. Detailed reports can be generated on a daily basis for system administrators.

“We’ve been very impressed with the Third Brigade solution,” explained Tony Mukomah, Director of Operations at Workstream. “The centralized management console gives us the flexibility to customize, deploy and manage appropriate host-based intrusion protection across the multiple tiers of our functionally diverse suite of applications—a definite edge over other solutions.”

RESULTS

“Third Brigade Deep Security has improved the security of our systems, and stopped attacks that would have negatively impacted our business, without having a noticeable impact on host performance,” said Gioja.

In addition, the solution has allowed Workstream to manage its patching process more effectively. With new filters developed and delivered to customers within hours of the latest vulnerability announcements from operating system, database, web and email server vendors, Third Brigade Deep Security also shields commercial applications until patches are deployed. This effectively extends the patching window by weeks or months in some cases. Now, they can test and deploy patches on a scheduled basis, rather than reactively, knowing that their hosts are automatically protected from new vulnerabilities.

“Customers are impressed with our world-class approach to protecting their data and applications,” concludes Gioja. “The value of Third Brigade’s security solution is easy to demonstrate to new and existing customers.”

For more information on how Third Brigade can help you take greater control of your business, please contact us:
1-866-373-6977
information@thirdbrigade.com
www.thirdbrigade.com

ABOUT THIRD BRIGADE

Third Brigade specializes in providing host intrusion defense systems to organizations that need to detect and prevent attacks that exploit vulnerabilities in mission critical systems. Third Brigade Deep Security allows businesses to apply comprehensive security profiles to hosts that protect against known and zero-day attacks using deep packet inspection. It helps ensure compliance and the 24/7 availability of critical systems, provides a virtual patch for software vulnerabilities, and allows organizations to deliver Internet-based services with greater security and confidence. Unlike other host intrusion detection and prevention systems, Third Brigade Deep Security provides broader, faster and simpler protection. **Third Brigade. That’s control.**



“Third Brigade”, “Deep Security Solutions”, and the Third Brigade logo are trademarks of Third Brigade, Inc. and may be registered in certain jurisdictions. All other company and product names are trademarks or registered trademarks of their respective owners. © 2007 Third Brigade. All rights reserved.