steadfast

800 S Wells St, Suite 190
Chicago, IL 60607
312-602-2689

# INTRODUCING: The Steadfast Security Suite

Security is no longer an afterthought; every business must consider the security of their data and communications. Companies need to examine their risk factors and mitigate them as soon as possible. Data loss and compliance matters often top the list of concerns, but it's important to never lose sight of your most important asset: your business's reputation.

Security is an ever-shifting landscape of threats and responses, and Steadfast diligently remains current to help clients remain protected and secure. Our proactive approach to business ensures that our clients and their data are protected; we communicate regularly with our clients, updating them on our security measures.

The Steadfast Security Suite has many products to help businesses build their optimal security solution. Our solutions include: Managed Firewall, IDS/IPS, SSL VPN, Web Application Firewall (WAF), DDoS Protection, Data Security and Encryption, Vulnerability Scanning, Log Management, Email Security, and Security & Compliance Consulting.

## Managed Firewall

The basic building block of a sound security plan is a firewall. The firewall monitors and controls traffic between two separate networks; it acts as a barrier while utilizing specific rules to assure that only the network traffic you want reaches your systems. Rules can be used to restrict access by IP, port, protocol, or the like. A firewall is a static, basic level of security, but is a simple way to manage a large number of potential security threats by substantially reducing public access to certain systems or applications. It is a required component of most compliance standards. But having a firewall is not enough. Without proper rules, updates, and monitoring, your firewall is not very useful. Every firewall provided by Steadfast is a managed firewall, so we can help manage your solution.

Our Juniper SRX firewalls do more than provide basic firewall functionality; they also support IPsec tunnels, which allow setup of a secure, encrypted, point-to-point tunnel. The tunnel allows you to setup off-site systems, such as systems inside your office, to behave as if they are on the protected side of the firewall, improving ease of access for devices that are already authenticated or approved.

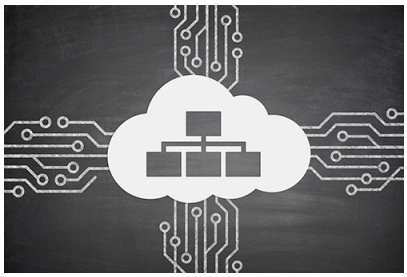
| Type of Firewall | About |
|---|---|
| Software Firewall | Available with all systems, built into the operating system. A software firewall can work in many cases, but may not protect against specific system-based vulnerabilities. It can also make the system more susceptible to denial of service attacks, and requires close policy management. |
| Shared Firewall | Steadfast's shared firewall product is a redundant F5 hardware firewall, offering a good level of protection with flexible capacity. This firewall provides scalable protection. |
| Dedicated Juniper SRX Firewall | Recommended for large environments, this option offers IPsec tunnels, added IDS/IPS features, and other routing and management capabilities. Redundancy is attainable with two firewall devices. |

## Intrusion Detection & Prevention System (IDS/IPS)

An Intrusion Detection System (IDS) detects and reports upon malicious activity or other policy violations based on identifying heuristics and patterns (also known as signatures) of common attacks or vulnerabilities. The system automatically acts upon these reports and blocks this activity, transitioning to an Intrusion Prevention System (IPS). All of our IDS/IPS options can serve in either capacity.

An IDS/IPS can warn or protect a system from attacks or vulnerabilities that are more complex than firewall capabilities, due to these complex signatures. The IDS/IPS utilizes substantially more resources than a firewall due to the added complexity, however, it is not a firewall replacement, as it will not detect all malicious traffic. Steadfast utilizes a Juniper SRX or Radware DefensePro IDS/IPS, allowing for customized solutions based on your needs.

## SSL VPN



Steadfast's SSL VPN product allows your users to connect from anywhere; you can enjoy the security of knowing all communications to the Steadfast network are secured via encryption.
An SSL Virtual Private Network (VPN) establishes a secured tunnel, encrypted via SSL, between your network and a hardware appliance. It is much more flexible and mobile than other tunneling methods, such as an IPsec tunnel; it is often used to grant specific users access to specific areas, instead of using broader site- or IP-based firewall rules.
Our SonicWall SRA SSL VPN appliances offer a wide array of client support including Windows, Mac OS, Linux, Android, and IOS clients, as well as a clientless option, to assure ease of use for everyone in your organization.

## Web Application Firewall (WAF)

A Web Application Firewall (WAF) can process much more complex rules than a standard firewall, specifically for HTTP (web application) traffic. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. A WAF is specifically designed for HTTP traffic, enabling extensive rule customization; attacks can be identified and blocked, protecting your traffic.
It's important to note that a WAF is not a replacement for a firewall or IDS/IPS, as it only protects HTTP traffic. It is a required component of most compliance standards if your data or systems can be accessed through a web-based application.
We proudly use Radware AppWall at Steadfast, and are happy to discuss how our solutions can meet your needs.

## DDoS Protection

Distributed Denial of Service (DDoS) attacks are on the rise. DDoS attacks utilize a large number of systems from around the Internet - often compromised systems - to launch a volumetric attack on a system. Attacks generally utilize throughput or number of requests attacks in order to prevent normal system operation.
DDoS attacks are not intended to breach security or compromise data, but to make it impossible for legitimate users to access a system. Often, a DDoS attack can be used to mask another security compromise.
As the number of systems online with substantial power and network capacity grows, DDoS attacks are becoming more common, and larger in scale. DDoS attacks attempt to act like a legitimate user of the site, making it difficult to separate legitimate and illegitimate traffic. A standard firewall, IDS/IPS, or WAF will only have limited effectiveness against DDoS attacks, and a dedicated appliance or resource is preferred.
Steadfast uses Staminus SecureNet and Radware DefensePro to keep our clients safe.

## Data Security and Encryption

There are many solutions to keep a system secure on the network side, but keeping your data secure on the system itself is vital. Keep your data secure via access control and encryption.
We provide both through Vormetric, assuring only select individuals and applications have access to specified data, even if they are able to get through the layers of network security. This encryption is transparent; it will not impact the general use of the encrypted data, such as replication or backup, while keeping it secure. Data security and encryption can be a requirement for some compliance standards, such as HIPAA.
Steadfast's solution includes centralized access control, a common method of encryption, and complete reporting.

## Vulnerability Scanning

Attackers have an unparalleled ability to uncover vulnerabilities in your network and applications. If you are to keep your infrastructure and data safe, you need to be aware of vulnerabilities even faster.

Our vulnerability scanning services are designed to spot vulnerabilities and let you know about them before they are exploited. In addition, with weekly scanning, you can discover vulnerabilities sooner than 30-day scan alternatives.

Vulnerability scanning is a required aspect of PCI DSS compliance and highly recommended to all enterprises. This scanning is included free with all of our fully managed dedicated servers and cloud services.

## Log Management

As part of PCI DSS compliance, you are required to store and monitor detailed audit logs. Every connection, every data transfer, and every user action must be accounted for, and checked for suspicious activity.

The problem is that few know how to consolidate logs and identify the signs of a security threat, and those that do rarely have the time.

Combining the latest automated tools, and our years of experience in network security, we can conduct daily log audits on your behalf. Without any impact on your workload, you can be confident that your data is protected and, most importantly, that you have met your compliance requirements.

## Email Security

Email has changed the way the world does business – in most ways, for the better. But email is also a point of exposure, both to email viruses and incoming spam that could potentially cripple your network.

With end-users in control of email, you need to be certain that viruses and spam will never reach your inbox. Our managed email security solution offers 99.9% spam blocking with less than one false positive in a million emails, on a fully redundant system that is always online. We'll keep your email secure.

## Security & Compliance Consulting

You may know the managed security services you are looking for. If so, you can select from any of our services and create an overall solution that works for you. But if you need more help, we want to hear from you.

We can consult on which services you need to meet the demands of compliance, including PCI DSS, HIPAA, SOX, FISMA, and GLBA. This will usually include a combination of our hosted services, and changes to your infrastructure and internal policies as required.

Through both of these methods, you can pass compliance audits and meet the standards that your investors, stakeholders, and customers deserve.

| Terminology | Definition |
|---|---|
| SSAE 16 | An auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SSAE16 provides guidance to service auditors when assessing the internal control of a service organization and issuing a service auditor's report. |
| SOX | Enhanced standards for all US public company boards, management, and public accounting firms. It requires management to assess the effectiveness of internal controls, obtain external validation of those controls, and provide assurances that financial/accounting processes are protected from unauthorized usage. |
| HIPAA | Requires the establishment of national standards for electronic health care transactions for providers, health insurance plans, and employers, and the security and privacy of health-related data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system. |
| PCI DSS | The PCI DSS standard was created to help payment card industry organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands. |