A BUSINESS WHITEPAPER FROM NSFOCUS

NSFOCUS

MANAGED SECURITY SERVICES PLAYBOOK

Table of Contents

Building a Case for Managed Security Services

Today, Internet service providers recognize the fact that bandwidth has become commoditized. Connectivity prices are at an all-time low while competition is at an all-time high. In addition, hosting providers understand that differentiation plays a key role in their long-term sustainability, as new entrants continue to erode their revenue streams. Both are interested in understanding how additional service offerings can help generate new revenue, retain customers, create competitive differentiation, and provide sustainable growth for their businesses.

In the past, both types of providers (Internet service providers and hosting providers) have attempted to expand their service offerings. Some have been mildly successful, while others have been a complete failure. The challenge providers face is to create new, profitable service offerings that customers are willing to pay for. Just because a provider creates a new service offering, does not mean it will become highly sought after by customers, or generate substantial profits for the business.

The question then becomes, "What services do customers want, what are they willing to pay for, and what services will be profitable for the provider?" The answer to these questions are actually quite simple. Create service offerings that your customers "need". Everyone knows the Internet is plagued with malicious traffic. As a result, enterprises and small/medium businesses spend an exorbitant amount of money every day trying to do one thing - block the malicious traffic attempting to penetrate their defenses. Is there an opportunity for providers to help?

Those who understand the OSI Model, can use that model to create different solutions (offerings) to meet the different customer needs. For example, the most basic service offering all providers deliver is "connectivity". Organizations buy bandwidth from some providers and may purchase hosting from others. But at the end of the day, what customers are really paying for is connectivity to the Internet. Taking connectivity out of the picture would obviously effect every other potential service offering. Therefore, protecting connectivity "first", is critical to delivering any other offering.

Connectivity can be affected by a host of different things. Cable cuts, power outages, software bugs, and equipment failures obviously can cause outages. However, cyber-attackers (hackers) can also cause an outage, and can launch a large number of different types of attacks as well. In general, we can classify the problems hackers cause as follows:

- Outages caused by DDoS attacks are growing in popularity, size, and frequency
- Computers are becoming compromised by malware, including ransomware, daily
- Data is being stolen, made unusable, or made inaccessible, every day

There is a tremendous need to help solve the problems caused by hackers, and this is precisely where providers can step in with new service offerings. Providers are in the perfect position to help solve these problems since they provide the basic connectivity for all traffic in and out of their customer's locations that is used by hackers in the first place.

Therefore, let's begin with the first problem above – DDoS attacks are growing in popularity, size, and frequency. The motivations behind DDoS attacks are plentiful, and DDoS attacks are extremely effective at eroding defenses, consuming resources, and breaking connectivity. Not only do DDoS attacks cause those effects, DDoS attacks also cost money to defeat and can cause additional collateral damage for those with no defenses. Protecting against DDoS attacks is a great place to begin with new service offerings. Diagram 1 will help explain this further.

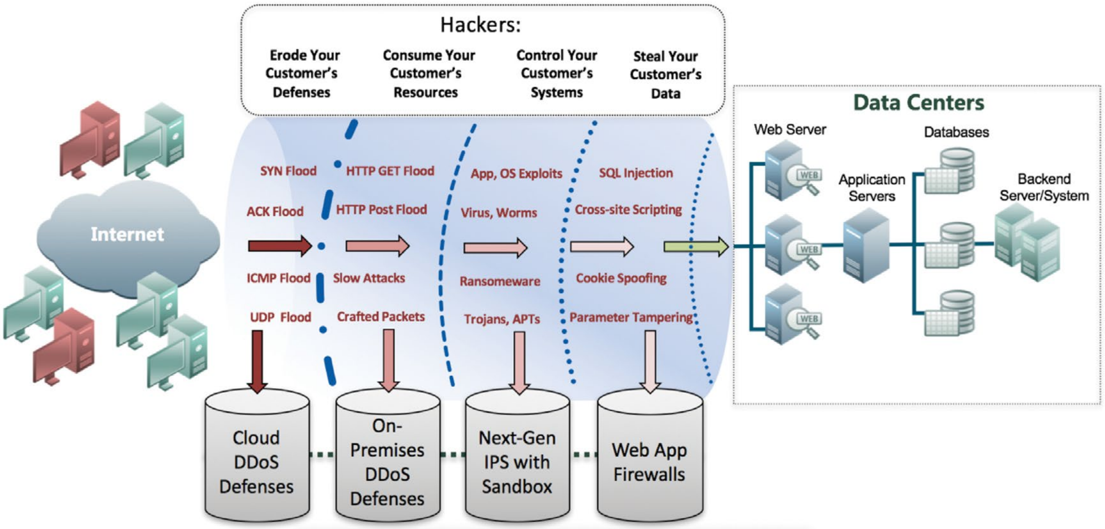

Diagram 1: Risk, Attack, and Defense Landscape

As shown in diagram 1, statistics prove that hackers:

- Erode Your Customer's Defenses
- Consume Your Customer's Resources
- Control Your Customer's Systems
- Steal Your Customer's Data

Hackers perform these actions for any number of reasons. Hackers typically want to:

- Take your customer's Internet access down
- Infect and control your customer's computers for other criminal purposes
- Steal your customer's data for monetary gain

DDoS Defenses as a Service Offering – Cloud-Based

Beginning from left to right in diagram 1, the first thing to eliminate are attacks that *erode your customer's defenses*. As shown, attacks like SYN Floods, ACK Floods, ICMP Floods, and UDP Floods are known as volumetric DDoS attacks. These types of network attacks are designed to not only consume all available bandwidth; they're also designed to completely erode your customer's other defenses. Firewalls, IPS, IDS, Sandboxes, Load Balancers, WAFs, etc. are all potentially impacted by these DDoS attacks. Their effectiveness can be completely compromised by a sizeable DDoS attack – even if the attack does not consume all available bandwidth.

The DDoS attacks mentioned above are best defeated by Cloud DDoS Defenses. Since DDoS attack volume can consume all available bandwidth in many cases, these attacks must be defeated upstream from the customer's location. From an enterprise perspective, these attacks are most often defeated by a network cloud, so to speak. However, what exactly does upstream mean with regard to providers? There are two schools of thought, while remaining in the context of delivering services that can defeat these types of attacks.

Tier 1 service providers with vast infrastructures can obviously defeat these attacks in "their cloud" by deploying DDoS defenses within their own infrastructures. But can smaller service providers (Tier 2, 3) do the same? The answer is yes. Not only can smaller providers deploy their own DDoS defenses to be offered as a service, they can also partner with someone who already has Cloud DDoS Defenses. If smaller providers feel they are not ready to deploy defenses of their own due to a host of different reasons, they can easily "resell" services they obtain from others who do have Cloud DDoS Defenses.

Although the potential service margins may be smaller when providers resell someone else's service, there's no reason they can't private label the service, or even add additional value by acting as a trusted intermediary between the cloud DDoS provider and the end-customer. Service providers already have a usage and billing infrastructure in place, and are closer to the customer than the cloud DDoS provider. The possibility of offering a one-stop-shop for Cloud DDoS Defenses is a reality for smaller providers, even without owning their own DDoS defense infrastructure.

Hosting providers can also offer DDoS defensive services on their own. Since each hosting provider's infrastructure can be viewed as a mini cloud, they are perfectly positioned to offer revenue-generating, volumetric DDoS defenses to their hosting customer base. Hosting providers often have a sizeable number of 10G pipes and can easily defeat attacks targeting their own customers, as well as attacks against their own infrastructures.

In the case of the hosting provider, if they or their customers come under a full pipe saturation attack, the attack must be mitigated upstream. The recommendation for hosting providers and smaller service providers is to ensure they have an agreement in place with a cloud DDoS provider to eliminate volumetric attacks upstream, and a method of transferring the costs back to the customer who was the target of the DDoS attack in the first place.

All providers must fully understand they are generally not under DDoS attack — in most cases, their customers are the target. If providers can defeat these attacks for their customers, they should be able to realize revenue for doing so. Not only can providers recognize new revenue streams by defeating volumetric attacks, they can also ensure attacks do not impact their own infrastructures and result in collateral damage.

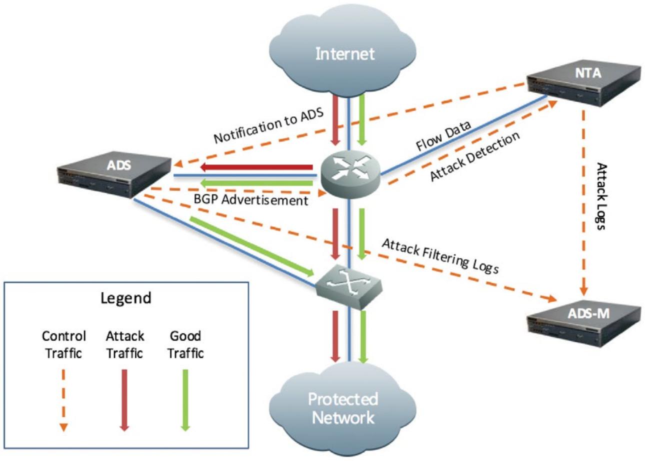

Diagram 2: The required technology to defeat volumetric DDoS attacks in the network

The solution shown in diagram 2 is capable of defeating 20 Gbps of DDoS attack traffic, and can be expanded well beyond this capacity to defeat any DDoS attack size on record.

- NTA – Network Traffic Analyzer - detects DDoS attacks by monitoring traffic flow data
- ADS – Anti-DDoS System - eliminates DDoS attacks within traffic streams
- ADS-M – ADS Manager - provides single pane of glass management and reporting with multi-tenant customer portal

DDoS Defenses as a Service Offering – Premises and Hybrid-Based

In the context of diagram 1, hackers also use DDoS attacks to *consume your customer's resources*. Today, industry statistics demonstrate that a large portion of the DDoS attacks observed do not consume all available bandwidth of their victims Internet connections. In addition, many attacks are very short in duration. Hackers understand that launching smaller/shorter DDoS attacks are a great way to consume server and network resources. They also consume time, attention, human resources, and log storage.

HTTP GET floods, HTTP POST floods, low-and-slow attacks, and specially crafted packet attacks are known to the industry as Layer 7 DDoS attacks. These attacks are designed to cause a significant strain on available resources. However, can these types of attacks also be an indicator of something more insidious?

Most people do not realize that Layer 7 DDoS attacks go right through firewalls. Firewalls that are placed in front of servers that are accessible from the Internet, have configured holes in them. Called Port Forwarding or Static NAT, operators must open inbound holes on firewalls in order for incoming traffic to be able to pass through them. This is done in every case where firewalls protect servers.

When holes or ports are opened on firewalls, not only do Layer 7 DDoS attacks pass through them, but a host of other attacks do so as well. Most industry analysts agree that a significant portion of DDoS attacks are being used as a \ distraction while hackers are compromising computer systems and stealing their victim's data. Known as Dark DDoS, these attacks hide other attack activity quite effectively.

Most industry analysts also recognize the fact that defeating the broad spectrum of DDoS attacks requires more than just cloud DDoS defenses. From volumetric DDoS attacks to low-and-slow DDoS attacks, the best approach to defeating these attacks requires a combination of cloud defenses and on-premises defenses – called the hybrid approach. This approach defeats all DDoS attacks regardless of their size or duration.

In diagram 2, the technology shown can be deployed in the providers' cloud to defeat volumetric attacks. That same technology can be deployed on-premises, not only to defeat volumetric attacks, but also Layer 7 attacks. Defeating Layer 7 attacks is done more effectively the closer the technology is deployed to the victim's network because more granular defense policies can be applied.

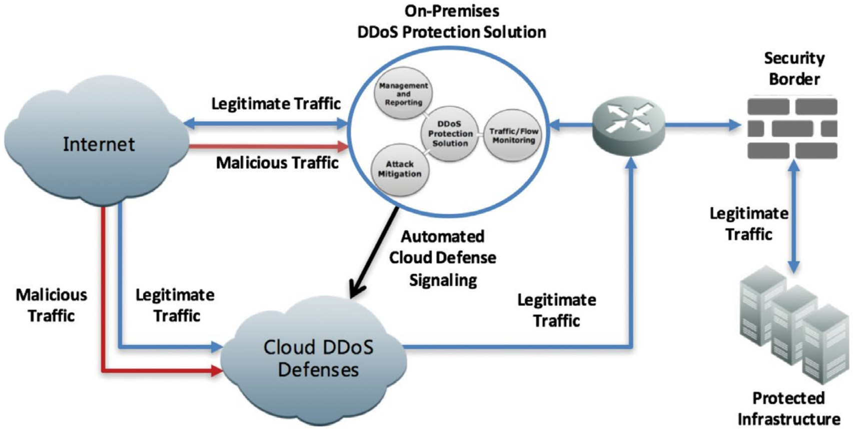

Diagram 3: The hybrid approach to defeating all DDoS attacks

As shown in diagram 3, in the hybrid approach to defeating DDoS attacks, the on-premises technology is completely capable of defeating all attacks up to the point of complete bandwidth saturation. However, when Internet bandwidth begins to be fully consumed, Cloud DDoS Defenses must be engaged. Notification to the cloud to divert traffic though Cloud DDoS Defenses is performed by the on-premises defenses, via Automated Cloud Defense Signaling, as shown by the black arrow in diagram 3.

The other role of the on-premises defenses is to be the eyes and ears for the cloud-based service provider. Providers who desire to offer cloud DDoS defenses are often completely blind to their customer's traffic, until traffic is diverted through their cloud. Without on-premises visibility into the customers traffic, cloud DDoS defenses would not be able to detect when a customer was under DDoS attack. Many providers who do not offer a hybrid approach, must rely on the customer to notify them of a DDoS attack. By the time a call is made, and traffic is diverted to the cloud, outages are sure to be incurred.

Any provider who desires to offer managed DDoS defenses as a service must recognize that a combination of defenses is required. Both cloud-based and on-premises defenses work in concert and are completely aware of each other. In addition, having both defenses in place reduces the need to engage the cloud for sub-saturation attacks. In other words, if the attacks are smaller in size, they can easily be defeated by the on-premises defenses.

Next Generation IPS (NGIPS) as a Service Offering – Cloud-Based

In the context of diagram 1, the next opportunity for providers is to defeat hackers who desire to *control your customer's systems*. Computers are becoming compromised by malware, including ransomware, almost daily. All organizations connected to the Internet recognize that much of the traffic they receive is nothing more than malware. Application and operating system exploits, virus, worms, Trojans, ransomware, advanced persistent threats, etc. make up a great deal of the traffic traversing the Internet – globally. This traffic has nothing more than malicious intent, and providers today can help solve this problem for their enterprise and small/medium business customers.

Both service providers and hosting providers are in a unique position to reduce the amount of malicious traffic their customers receive from the Internet. Since all traffic traverses the providers' networks, they can help eliminate the vast majority of the malicious traffic they are transporting. Known malware can easily be eliminated by the providers, and even unknown malware can be identified and filtered as well.

Providers who strategically deploy high-capacity Next Generation Intrusion Prevention Systems (NGIPS) and sandbox technologies in their networks, can use those systems to defeat the vast majority of known malware their customers receive from the Internet. Forwarding their customer's traffic through NGIPS and inspecting suspicious files with sandbox technologies will significantly reduce the amount of malicious traffic customers receive. Although not a complete replacement for on-premises NGIPS, cloud-based NGIPS can act as a pre-filter. Eliminating the vast majority of known malware in the provider's networks would allow on-premises NGIPS and sandboxes to focus more on "unknown malware".

Delivering cloud-based NGIPS services does require SLAs that not only protect the customer, but also protect the provider. The problem of false positives and false negatives can become an issue and must be addressed in SLAs. Therefore, providers who desire to offer NGIPS as a service must spend time building SLAs that protect both parties.

Most industry veterans who have worked with IPS systems in general, realize that false positives are a problem for all IPS systems. Although NGIPS technologies are getting better at reducing false positives, they can still end up blocking good traffic. As a result, there often is a tradeoff that must be considered. In order to reduce the amount of false positives (blocking good traffic), NGIPS systems must be tuned more loosely to avoid that situation. As a result of tuning, more false negatives will be incurred. False negatives in this case indicate that malicious traffic was not blocked.

Providers who desire to offer NGIPS as a service must accept that they will never be capable of eliminating ALL malicious traffic. Instead, their service needs to be marketed as a way of reducing malicious traffic for their customers. In this way, customers would feel confident that the vast majority of malware is being eliminated by their provider, while they will focus on the remaining malware.

NGIPS as a Service Offering – Premises and Hybrid-Based

Is there a case where the hybrid approach makes sense concerning NGIPS? It all depends on the technology deployed. If the cloud and on-premises systems work together, they can provide a very effective defense against malware.

NGIPS that is deployed in the cloud obviously would have to be configured with less stringent policies to eliminate the possibility of false positives. However, NGIPS deployed on premises could be tuned with much tighter policies. In this case, if malware is detected by on-premises NGIPS, that system must be capable of signaling to the cloud NGIPS to begin defeating that malware upstream. Hybrid NGIPS as a service can be a complete reality for providers today. Diagram 4 highlights that deployment scenario.

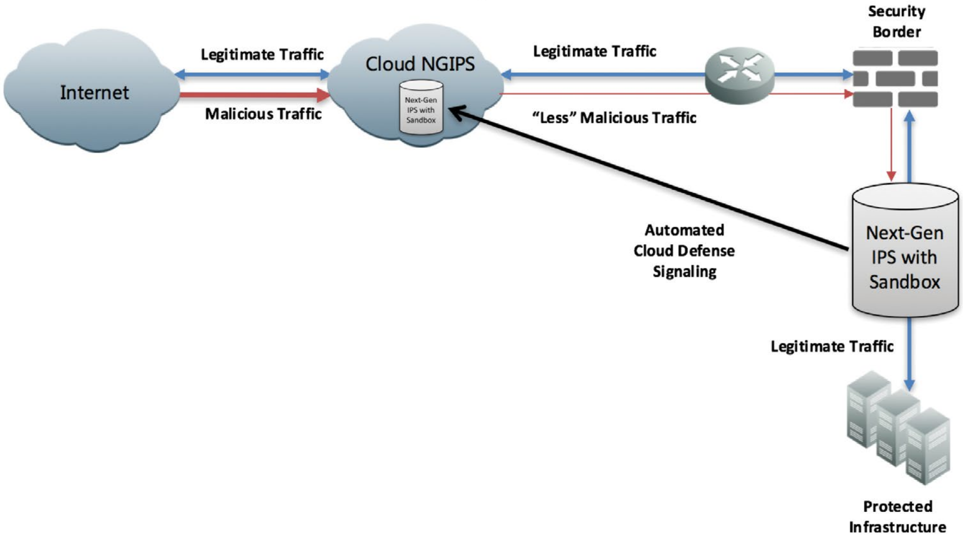

Diagram 4: Hybrid Next Gen IPS

Web Application Firewall (WAF) as a Service Offering – Cloud-Based

Again, in the context of diagram 1, hackers also desire to *steal your customer's data*. The frequency of network breaches that result in the loss or theft of data have been continuously on the rise for nearly a decade. Data is being stolen, made unusable, or made inaccessible every day. Hackers focus much of their efforts on data, since stolen data can be sold on underground markets in many cases. Since data is often stored in databases, these databases are a prime target for hackers. SQL Injection, Cross-site Scripting, Cookie Spoofing, Parameter Tampering, and a host of other targeted attacks are designed to allow hackers access to critical data.

The industry recognizes that the best way to protect databases, and the critical data they store is by using Web Application Firewalls (WAF). Many government and industry regulations either recommend WAF, or demand its usage to protect critical data from hackers. Service providers and hosting providers can utilize WAF technologies in their clouds to protect their customer's databases from a host of targeted attacks.

WAF technology is much different than the technology previously discussed. Cloud DDoS Defenses and on-premises DDoS Defenses most often operate at lower layers in the OSI model, for example Layer 3 and 4. They also have capabilities of defeating DDoS attacks at Layer 7, but only in clear-text. They have no ability to defeat low-and-slow DDoS attacks across encrypted traffic.

NGIPS with sandboxing capabilities also has the ability to defeat DDoS attacks. However, NGIPS and sandboxes are more focused on defeating malware and advanced persistent threats (APTs). Using their deep packet inspection capabilities, known and unknown malware, and APTs are detected and eliminated from traffic streams.

WAF however, does have the ability of defeating low-and-slow DDoS attacks across encrypted traffic streams. Not only do they have the ability of defeating encrypted attacks, they also look much deeper into the traffic then the aforementioned defenses. WAF technologies have the ability to defeat database attacks since they understand the context of data queries and protect against the OWASP Top 10 vulnerabilities.

Service providers can offer managed, cloud-based WAF services to their customers in multiple forms. WAF technologies can monitor traffic streams in provider's networks, and take action when they see exploits or hackers attempting to take advantage of OWASP Top 10 vulnerabilities targeting their customer's databases. WAF technologies can also be deployed in hosting providers' networks to protect against attacks targeting their hosted customer's databases. All providers are in an excellent position to offer managed WAF services.

WAF as a Service Offering – Premises and Hybrid-Based

Today, many enterprises and small/medium businesses are not moving their critical data and their databases to cloud providers like Akamai, Amazon, and others. Instead, enterprises often use these public services for non-critical data like websites, while keeping their critical data and databases on-premises in their own data centers. This hybrid-cloud approach presents an opportunity for service providers to offer on-premises WAF services to their existing customer bases. Offering managed WAF services and deploying WAF technologies on-premises can be a reality for service providers today.

Conclusion

Network connectivity has become a commodity business. Business internet access once priced at $500 per month for 1.5 Mbps is now available for half of the cost at almost 70x the capacity. While this is great for consumers, pure play service providers often struggle to maintain profitability and grow revenue in the face of increased competition. As the prices for hosting services continue to decrease, while new competitors continue to erode hosting providers market share, the need to generate long-term revenue streams is critical for both types of providers.

As a result, many providers have turned to managed services as a means of increasing revenue, improving margins, building customer loyalty, and creating competitive differentiation. Managed security service providers, in particular, have experienced tremendous growth fueled by both the complexity of modern cyber-attacks, and the increased acceptance of cloud delivered services by organizations of all sizes. In working with these managed security services partners, some key success factors have emerged that enable them to profitably deliver Managed Security Services:

Choose an accurate and reliable security solution. There are many anti-DDoS, WAF and NGIPS solutions available, but their effectiveness can vary dramatically. The best solutions are both fast and accurate. Accuracy is critical because users will not tolerate legitimate traffic being blocked, and speed is important because most attacks are over within minutes, or they are executed through the undetected installation of malware.

Deploy a multi-tenant management solution. Successful providers have many customers and the managed security solution in use by the provider should support multi-tenancy so that security policies and reporting can be customized on a per customer basis. Further, the solution should offer a personalized web GUI so that the customer can access network status and reporting themselves without having to involve the service provider's operations staff.

Incur expenses only in the presence of revenue. Many providers have already deployed security technologies in their own network. In most cases, these solutions are being used to protect the service provider's infrastructure and can be re-purposed for new, revenue generating security services. Ideally, this equipment uses a scalable architecture that supports clustering to increase mitigation capacity as new customers are added.

The hybrid approach to defeating many attacks is the best approach. Industry analysts agree that the hybrid approach of combining both cloud defenses and on-premises defenses offers the most comprehensive and economical strategy. Providers who do not offer the hybrid approach suffer due to redirecting traffic to their cloud that could be defeated by on-premises technology. Also, providers who do not offer hybrid defenses are blind to their customer's traffic from the customer's perspective. Deploying hybrid defenses solves both of those problems.

Cloud-based and on-premises managed NGIPS with sandbox will be in high demand. As the Internet becomes more-and-more cluttered with malicious traffic, cloud-based NGIPS with sandbox services will be more in demand. In addition, small/medium enterprises often do not have staff that can manage and operate NGIPS and sandbox technologies. The opportunity for providers to offer managed NGIPS with sandbox to that customer segment will likely produce new revenue streams that will be quite significant.

Cloud based and on-premises managed WAF is a reality. As network breaches that cause the loss of data or theft of data continue to increase globally, WAF technologies will become more widely deployed. Providers are in the perfect position to offer managed WAF services to their customers.

The move to SDN and NFV is around the corner. As providers begin to realize that a managed security services model can generate long-term revenue, they will also desire to move away from physical appliances that provide security services. Vendors who build anti-DDoS, NGIPS, sandbox, and WAF technologies all must begin to move in the direction of supplying their technologies as software-based, virtual appliances. Choose suppliers who offer their technologies in both physical and virtual appliances.

About NSFOCUS

Mission

Today's cyber-attacks are more frequent, complex, and destructive than ever, and they often result in loss of revenue and theft of vital data. NSFOCUS is committed to helping our customers mitigate risk, protect their valued assets, and maintain continuity of their business services. Our strategy is to provide the most competitive security solutions and services for customers, and to be the world's most reliable network and application security company.

Profile

NSFOCUS IB, headquartered in Santa Clara, California USA, is a global network security vendor providing comprehensive, multi-layered protection from today's advanced threats. Our solutions protect the world's largest banks, telecommunications, gaming, technology and social media companies, and are continuously updated by the NSFOCUS Security Labs, one of the world's largest security research labs. NSFOCUS is a member of the Microsoft Active Protections Program (MAPP), StopBadware.org and the Cloud Security Alliance (CSA).

Customers

NSFOCUS customers include 4 of the world's top 5 banks, the largest telco's and mobile operators, and numerous financial services, government and enterprise organizations. Our products and services have helped more than 27,000 customers mitigate risk, protect their valued assets and maintain high levels of business operations. The company's business spans the United States, Japan, Europe, China, Southeast Asia and the Middle East. Our advanced products and support responsiveness have impressed partners and customers alike, and have sparked explosive growth and success.

NSFOCUS

NSFOCUSGLOBAL.COM