IBM Security

A firewall is just the beginning when securing your network

Significantly improve your network security by co-deploying IBM Security Network Protection (XGS) with your next-generation firewall

IBM Security White Paper

Minimum protection won't stop today's sophisticated attacks

When are your network defenses enough to protect your valuable data and business applications? More importantly, when are they *not* enough? Even after you've deployed a next-generation firewall (NGFW), there's a strong chance you need to do more.

That's because cybercriminals have found new ways to breach your perimeter defenses using zero-day, mutated and obfuscated exploits. Because attacks can be launched *behind* the firewall through the malicious or inadvertent actions of employees. And because trusted users connect to your infrastructure from untrusted technologies and locations every day.

Obviously, you're not going to scrap your firewall, as it is a key component in your organization's cybersecurity defense. But even an NGFW with its intrusion prevention system (IPS) option active does not provide the full network protection you need to counter the evolving threats attacking your network. You can do more to protect both the perimeter and internal segments of your network.

Insiders already behind the firewall were responsible for

60%

of all attacks in 2015.[1]

Learn more about stopping unknown threats in the IBM video.

[1] "Reviewing a year of serious data breaches, major attacks and new vulnerabilities," *IBM X-Force Research: 2016 Cyber Security Intelligence Index*, April 2016.

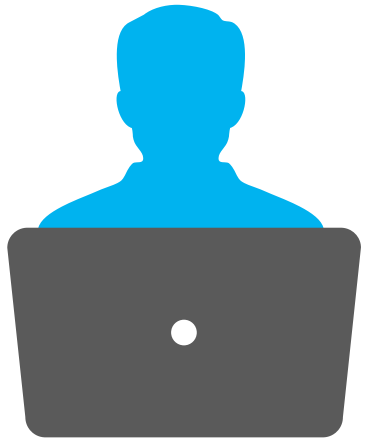
In today's threat landscape, a "both/and" approach is the answer

Taking steps to stop attacks at your infrastructure's perimeter is a critical best practice. But what happens when malware gets through the perimeter—or simply bypasses the perimeter by infecting a mobile device while it was off your network—and then begins traversing it? What happens when an attacker gathers and exfiltrates sensitive data? In cases like these, you can incur the cost of investigating the breach and remediating the vulnerabilities. You can suffer a loss of customers. You may also face legal expenses and regulatory fines.

Many times, an organization doesn't take notice right away—and that's the problem. Once inside, an attack takes an average of 256 days to identify.[1] And by that point, it can be too late to prevent damage. The cost of such hidden dirty work now averages 3.79USD million per breach.[1]

Often the problem lies in security products that were created to defend against yesterday's threats, such as worms that indiscriminately spread across the Internet by attacking known vulnerabilities using well-known exploit techniques. Though attacks have become more directed and more complex, security solutions often still utilize pattern matching to protect against specific exploits—an approach that fails in today's world.

To protect themselves from today's attacks, organizations must deploy solutions designed to protect against unknown and mutated threats, including attacks that hide themselves in encrypted traffic. Further, this protection needs to be enforced at more points than simply the perimeter firewall. It must inspect traffic on the interior of the network as well. In addition, deploying this protection must not require major re-architecture of the network.



55%
of IT security professionals agree that a standalone IPS provides superior intrusion prevention compared to an NGFW.[2]

▸ Learn what IT security professionals think about next-generation IPS in this Forrester survey report.

[1] "2016 Cost of Data Breach Study: Global Analysis," *Ponemon Institute*, June 2016.

[2] Next-Generation IPS In The Era Of Targeted Attacks: Security Solution Decision-Makers Prioritize Forward-Looking Solutions With Adaptive Intelligence," A Custom Technology Adoption Profile Commissioned by IBM, *Forrester Research*, January 2016.

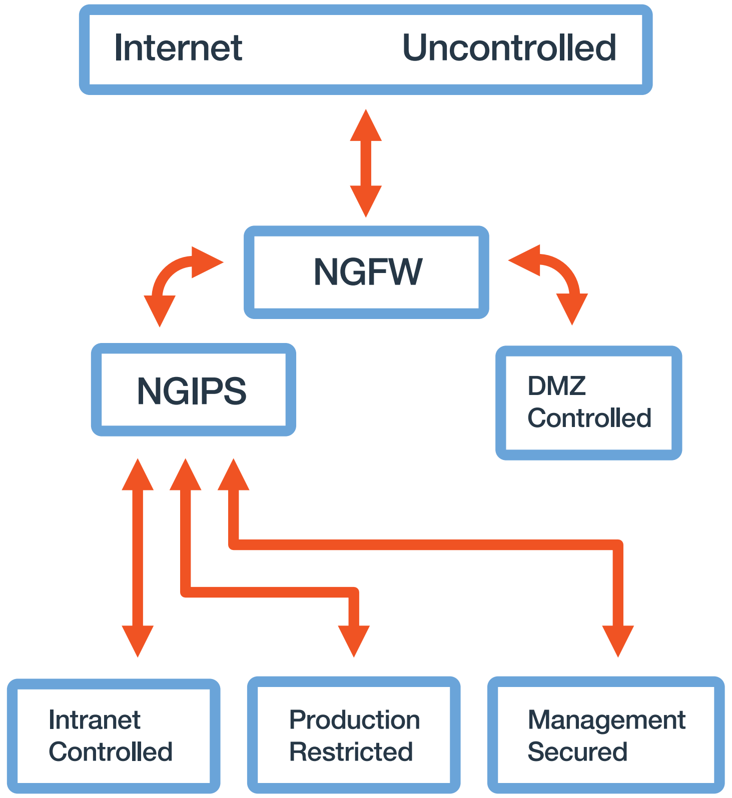
Maximizing your network protection: A closer look

Cybercriminals are continuously evolving their tools and methods to ensure that their attacks are as effective as possible. You need to do the same with your security defenses.

For network security, this means deploying a next-generation intrusion prevention system (NGIPS), a network protection solution to guard against a wide spectrum of Layer 2 through Layer 7 exploits. An NGIPS provides a purpose-built threat detection and prevention engine to generally provide superior security efficacy. Additionally, an NGIPS includes features such as application and user control, and IP reputation feeds to help better protect your network with greater levels of visibility and control. Unlike traditional IPS solutions, an NGIPS can also inspect encrypted traffic.

An NGIPS solution provides an extra layer of security to stop attacks that may get through the perimeter NGFW. Additionally, an NGIPS can protect internal network segments and prevent “east-west” lateral attacks within the network that never touch the perimeter. As a Layer 2 “bump in the wire” device, an NGIPS can be deployed behind the perimeter without requiring the network re-architecture typically needed to deploy an NGFW on the interior network.

DMZ with one NGFW appliance



- Learn more about intrusion prevention in the IBM white paper.

The IBM solution: Working together with your firewall

The IBM NGIPS solution, IBM® Security Network Protection (XGS), offers an impressive record in protecting against previously-unknown attacks and exploits. Augmenting traditional perimeter security measures such as NGFW, XGS provides protection against attacks the NGFW fails to detect. Additionally, XGS also helps protect against insider threats—whether from malicious users or innocent errors—as well as attacks that previously crossed the firewall and are now traversing the network laterally.

To do this, XGS inspects all network traffic—including SSL/TLS encrypted traffic—and understands hundreds of network and application protocols and file formats. It uses constantly updated IP and URL reputation data to prevent users and systems from inadvertently accessing malicious sites. It also provides granular network access control so network bandwidth is consumed only for legitimate business purposes.

XGS provides native bi-directional integration with IBM QRadar® Security Intelligence Platform, which aggregates security information and activity-related data to detect and prioritize advanced threats. Using this integration, XGS sends network flow data and security events to IBM QRadar SIEM for analysis. If a security analyst determines an attack is in process, the analyst can immediately send a quarantine/block command to XGS with the click of a mouse, directly from the QRadar console. XGS also exposes a web services application programming interface (WS-API) to integrate with other, existing security assets deployed in your environment.

- Get an overview of XGS in the IBM video.
- Learn more about XGS and QRadar integration in the IBM webinar.

IBM XGS blocked

100%

of encrypted and unencrypted threats and

100%

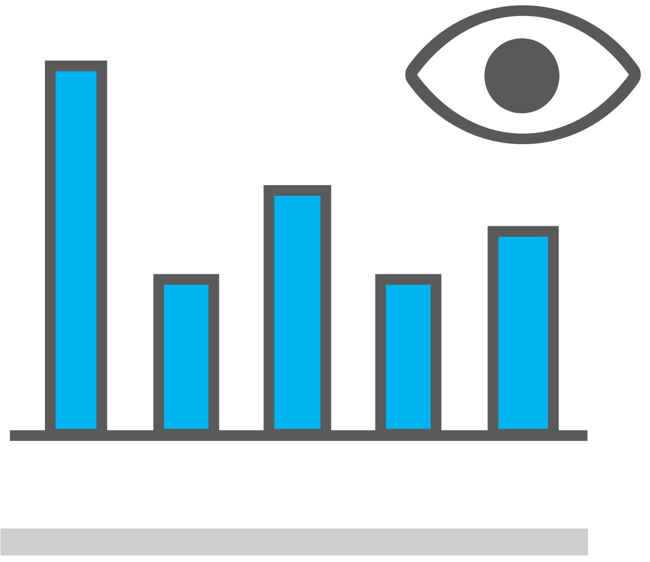
of evasion attacks in third-party testing.[1]

[1] “IBM Security Network Protection XGS7100: Next Generation Intrusion Prevention System (IPS) Efficacy and Performance Evaluation,” *Tolly Enterprises*, February 12, 2016.

Multiple methods add up to superior network protection

While many NGFW and NGIPS solutions rely on pattern-matching to detect attacks—a reactive and brittle approach that is effective only for known threats—XGS employs a fundamentally different approach, using vulnerability protection, heuristics and behavior-based analysis to provide Ahead of the Threat® protection. The IBM Protocol Analysis Module (PAM) is the modular deep packet inspection engine in XGS. It employs multiple methods for identifying exploits and blocking attacks:

- **Vulnerability decodes**—Vulnerability protection that helps secure against entire classes of exploits, regardless of mutation or obfuscation techniques
- **Application layer heuristics**—Proprietary algorithms designed to block malicious use of applications
- **Web injection logic**—Protection against web-based attacks, such as SQL injection and cross-site scripting
- **Shellcode heuristics**—Behavioral protection that identifies and blocks malicious code based on its behavior, rather than matching a particular attack signature or pattern; helpful in protection against evolving threats that change to evade traditional IPS solutions
- **Content analysis**—File and document inspection and anomaly detection that blocks sensitive data, such as personally identifiable information or credit card numbers, from flowing over network segments where it doesn’t belong
- **Protocol anomaly detection**—Network traffic analysis that identifies deviant behavior outside the accepted norms, enabling XGS to detect anomalous behavior without relying on signatures



PAM deep packet inspection is nearly

2x

as effective as pattern matching.[1]

- Get an overview of PAM in the IBM video.
- Dive deeper into PAM in the IBM webinar.

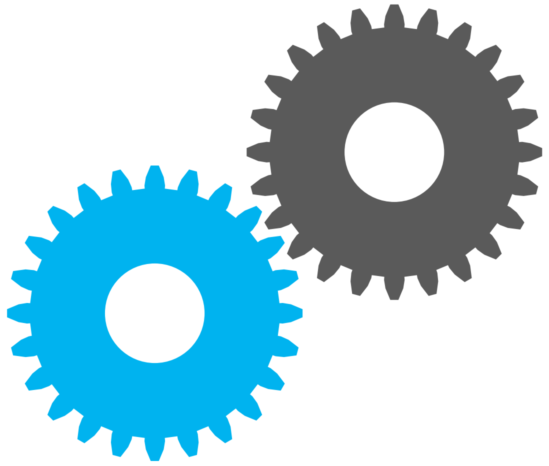
[1] “IBM Security Network Intrusion Prevention System GX7800: Comparative Efficacy and Performance Evaluation,” *Tolly Enterprises*, December 2012.

The right tools can boost your security and network performance

When it comes to security, stopping cyber attacks is critical. Your NGFW or NGIPS—or both, working together—need to detect and prevent attacks. Period. But beyond security efficacy, they also need to maintain network performance.

While every network is unique, performance impacts can occur when the IPS feature is activated in an NGFW. Enabling IPS on an NGFW typically slows throughput and can cause significant traffic disruption if the NGFW was not properly sized. For most organizations, going without an IPS is simply not an option. But deploying a dedicated NGIPS such as XGS—which allows an organization to turn off the NGFW IPS without sacrificing intrusion prevention—creates a powerful combination that both enhances security and avoids potential slowdown.

When deployed inside the network, XGS monitors not only traffic arriving from outside, but also traffic moving within the network—with minimal impact on both speed and network architecture. At the same time, advanced behavioral analysis and heuristics provided by PAM, and automated threat intelligence provided by IBM X-Force®, increase security performance. This Ahead of the Threat protection—in many cases more than seven years ahead of a threat's discovery[1]—provides protection against entire classes of exploits.



IBM XGS delivered

26 Gbps

inspected throughput in third-party testing.[2]

Learn more about improving network security visibility and control in the IBM video.

[1] "Shell_Command_Injection," *IBM X-Force Exchange*.

[2] Keith Bormann, "Data Center Intrusion Prevention System Test Report: IBM Security Network Protection XGS 7100," *NSS Labs*, 2016.

Security is the goal, but you can reap financial benefits, too

While the promise of an all-in-one NGFW may appear more cost-effective than also adding NGIPS to the network, XGS has been shown to yield significant cost advantages when protection solutions are deployed together. A recent study found, in fact, that a large financial services organization deploying XGS achieved a 340 percent return on investment (ROI) over a three-year period.[1]

The company, a bank with 2,500 employees and a customer base of 30,000 merchants, deployed XGS across all its networks to upgrade from traditional IPS appliances to take advantage of the latest capabilities and enhancements. The bank also sought to reduce manual work for its security team. With XGS, the bank was able to streamline and automate security processes and more confidently manage network traffic—with improved network performance, increased security and high network availability.

Better performance came from a significant reduction in inbound traffic. Better security came from an improved ability to mitigate the risk of a breach—with the corresponding savings of millions of dollars. And high availability came from a reduction in downtime due to an improved ability to both detect and block incoming attacks. Increased availability reduced the risk of lost revenue and regulatory fines due to breach-related downtime.

One IBM XGS customer experienced

340%

ROI and a payback period of less than two months.[1]

- Read about the business benefits of XGS in the Forrester Research report.

[1] Ben Harris and Jon Erickson, “The Total Economic Impact Of IBM Security Network Protection (XGS): Cost Savings And Business Benefits Enabled By IBM XGS,” *Forrester Research, Inc.*, February 2016.

Why IBM?

As part of the comprehensive IBM Security portfolio, XGS is a critical element in providing protection you need.

XGS is designed to deliver the highest levels of network security, from protection against mutating network-based attacks to visibility into what is happening on your network. When you deploy XGS as a component in your perimeter and internal network security plan, you get:

- **Attack protection** against zero-day attacks, mutated threats and obfuscated exploits—in some instances achieving 100 percent protection as demonstrated in recent third-party testing[1]
- **Research from IBM X-Force**, the industry pioneers in security research and development, with visibility into billions of events per day across the globe
- **Visibility and control** over application and user actions with granular network policies for specific groups, individuals and applications, as well as protection for the network interior
- **Out-of-the box integration** with IBM Security solutions, including QRadar Security Intelligence Platform
- **Flexible performance licensing** that allows you to pay for the security you need today, while allowing you to easily upgrade later via a software license, avoiding costly "rip-and-replace" of hardware

With IBM, you get technology, expertise and integration with the full portfolio of IBM Security solutions to protect your network perimeter and its internal operations in today's dangerous threat environment.

Download

a 30-day trial of IBM Security Network Protection (XGS).

- Read a description of the XGS product in the IBM data sheet.
- Learn more about IBM X-Force.

[1] "IBM Security Network Protection XGS7100: Next Generation Intrusion Prevention System (IPS) Efficacy and Performance Evaluation," *Tolly Enterprises*, February 12, 2016.

For more information

To learn more about IBM Security Network Protection (XGS), please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/network-protection

To download a 30-day trial of IBM Security Network Protection (XGS), visit: **ibm.com**/developerworks/downloads/security/xgs/index.html

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research, provides security intelligence to help organizations holistically protect their infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
October 2016

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

WGW03231-USEN-00