Get next-generation defenses with IBM QRadar Network Security (XGS)

Guard your network with security that goes far beyond pattern-based detection
Why network security demands more than point solutions

There was a time in the recent past when securing your network was thought of as a straightforward proposition. One would deploy a firewall to block the obvious threats and use an intrusion prevention system (IPS) to look for known exploits by using pattern-matching—the same type of approach used by typical anti-virus software. Then the goal was to keep these point products updated with the latest firmware and any new pattern-based signatures to protect against known threats.

Unfortunately, this reactive approach falls short in the face of today’s threats, such as advanced persistent threats, targeted application attacks and designer malware, and is often ineffective against unknown, zero-day or mutated threats. Deep security demands instead an adaptive, behavior-based approach.

It’s not just the limitations of pattern-matching detection, however, that calls for new approaches to network security. Attackers know that simply using common encryption methods such as secure socket layer (SSL) and transport layer security (TLS) can bypass last-generation defenses. In addition, the growth within organizations in the number of mobile users and the adoption of cloud-based computing increases the risk of security breaches beyond those coming from criminals outside. Changing norms in how users get and use software plays a role, too: cloud-based email and ubiquitous social media expose organizations to a wide range of threats. Using these applications and platforms can accustom users to interactions that attackers can easily exploit.

Even organizations that have made an effort to face threats by deploying a sprawl of point products—firewalls, IPS deployments, URL filtering tools, vulnerability management or other technologies—can lack visibility into and control of their whole network infrastructure.

Learn more about protecting against targeted attacks with next-generation network security.

1 Based on IBM X-Force Exchange data.
Introducing IBM QRadar Network Security (XGS)

Along with ever more sophisticated attacks, the rise of social media, a more mobile workforce and ubiquitous web applications have all raised the stakes for enforcing and ensuring network security—and security professionals are deluged with threats and alerts.

IBM® QRadar® Network Security (XGS) helps meet those threats, delivering an integrated security approach that provides SSL/TLS inspection, application control and IP reputation analytics in a single appliance, along with outstanding visibility and control of network traffic. The QRadar XGS appliance collects data and analyzes all traffic flowing across your network, using next-generation features that enable the critical insight, visibility and control you need. QRadar XGS extends your network investment with interchangeable network interface options to suit your existing environment. It offers flexible licensing so you can budget for the level of performance you need, without the need for costly rip-and-replace upgrades.

Most importantly, QRadar XGS defends your network by guarding vulnerabilities and recognizing malicious network activity by the way it behaves, rather than simply watching for pattern-based malware signatures.

Designed to overcome the weaknesses of conventional network security appliances, the IBM solution:

• Provides critical insight and visibility into network activity, including encrypted traffic
• Integrates with IBM QRadar Security Intelligence Platform for threat detection and prioritized incident response
• Delivers superior zero-day threat protection and security intelligence powered by IBM X-Force® research
• Enables granular control of both web and non-web applications by users and groups
• Helps reduce cost and complexity by consolidating point solutions into a single, extensible network security platform
• Helps control non-critical, high-bandwidth activity to provide additional cost savings

QRadar XGS blocked 100% of encrypted and unencrypted threats and 100% of evasion attacks in third-party testing.1

Learn more about the next-generation network security offered by QRadar XGS.

Gain greater protection by integrating XGS with QRadar SIEM

QRadar XGS is a powerful stand-alone tool, but its greatest strength emerges when integrated within a comprehensive security framework. This combination enables the security team to take full advantage of the solution’s intelligent, adaptive approach to recognizing active malicious threats on the network. Unlike a simpler pattern-matching IPS, QRadar XGS can identify traffic as potentially malicious, even if it doesn’t match a known pattern, such as with a zero-day exploit.

With its out-of-the-box integration with IBM QRadar Security Intelligence Platform, QRadar XGS benefits from two-way communications between different parts of the security environment. When QRadar XGS spots a potential threat using its vulnerability-based intelligent approach, it can send that event information to IBM QRadar SIEM and alert security analysts to the threat. QRadar administrators can then analyze suspicious activity spotted by QRadar XGS, and—if they determine the activity to be an active threat—update the QRadar XGS network policies to block that threat going forward, or to quarantine affected endpoints, all from within the QRadar SIEM console.

QRadar XGS can work with QRadar SIEM, too, to deliver consistent and comprehensive threat detection. The network flow data and event information QRadar XGS gathers helps make QRadar SIEM smarter, while QRadar XGS puts the insights gathered through QRadar SIEM into action. An enterprise’s most valuable assets, such as customer databases or financial and accounting systems, might be blocked to machines known to contain specified vulnerabilities (or exploitable combinations of vulnerabilities), while users can still reach less sensitive systems while vulnerabilities are being addressed.

Learn more in this webinar about how QRadar SIEM and XGS work together.

1 "Offense management," IBM Knowledge Center.
Next-generation features give you a closer look at network traffic

Next-generation features set QRadar XGS apart from conventional IPS solutions to help administrators deal with today’s threats.

SSL/TLS inspection isn’t fooled by simple encryption
Conventional network security appliances cannot peer into the contents of SSL/TLS-encrypted network traffic, giving attackers uninspected access to the network. Only with a separate SSL/TLS inspection device could an enterprise actually monitor the encrypted traffic, adding cost, complexity and latency. So even as encryption has become the norm for an increasing share of network traffic, attackers know they can use SSL/TLS to evade detection by first-generation solutions.

QRadar XGS, by contrast, provides onboard, low-latency capabilities for inspecting both outbound and inbound SSL/TLS connections. (It also enables policy-based SSL/TLS inspection, allowing organizations to bypass decryption of SSL/TLS sessions that are protected by law or overriding privacy needs, such as in online banking or the transmission of healthcare information.)

Deep packet inspection with PAM
QRadar XGS also includes the Protocol Analysis Module (PAM) from IBM X-Force for deep packet inspection. Pattern-matching analysis alone is useful but brittle; small changes by malware operators can result in a stealthier attack that triggers no alarm. Using advanced heuristics techniques, the PAM engine can detect evolving threats that have been modified to avoid detection by traditional IPS signature-based products. Instead of looking through a database table to watch for specific signatures, PAM analyzes what packets are doing, and hones in on attempts to reach known vulnerabilities.

PAM deep packet inspection is nearly 2x as effective as pattern matching.¹

Watch this webinar to learn why deep packet inspection is important for intrusion prevention.

Putting network traffic into global context for improved security

To help protect against advanced threats such as spear-phishing attacks, organizations need multi-layered protection that exceeds the capabilities of standard IPS technology. Next-generation network security enables security administrators to create more specific and aggressive threat-response rules, supplementing the policies of an existing firewall. QRadar XGS yields sophisticated additional tools based on IBM X-Force data:

**IP reputation analysis**
QRadar XGS integrates a continuously updated IP reputation feed from IBM X-Force, providing an evaluation based on a curated list of suspect source and destination IP addresses. Even if an attacker manages to bypass other detection methods, QRadar XGS can still detect and block traffic based on the use of known-bad addresses. The protection goes deeper, too. If a protected machine accesses an IP address known to be home to a botnet command-and-control server, the communication can be blocked and security administrators alerted that the machine is likely compromised by malware.

**URL filtering**
QRadar XGS leverages a database of more than 32 billion URLs to provide deep intelligence on anomalous network activity. As a result, organizations are better prepared to defend against the latest internet threats based on their source. This helps set intelligent bandwidth use policies and reduce the risk of application-originated attacks.

**Geographic analysis**
The reputation feed also provides valuable geographic information, so QRadar XGS can base decisions on the location of the IP address to identify the originator as being from a country that is rated high for malicious activities such as spreading spam and malware.

Learn more about how IBM X-Force Exchange lets security professionals research and share threat intelligence.
Why QRadar XGS?

As part of the comprehensive IBM Security portfolio, QRadar XGS is a critical tool for providing network protection. QRadar XGS is designed to deliver the highest levels of network security, from protection against mutating network-based attacks to greater visibility into what is happening on your network, and immediate reaction to threats as they appear. When you deploy QRadar XGS, you get:

• Out-of-the-box integration with IBM QRadar Security Intelligence Platform for comprehensive threat detection
• 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
• 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

• Research from IBM X-Force, the industry pioneer in security research and development, with visibility into billions of events per day across the globe
• 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.

Learn how one QRadar XGS customer experienced 340% ROI and a payback period of less than two months.

For more information

To learn more about IBM QRadar Network Security, please contact your IBM representative or IBM Business Partner, or download the free trial at: http://ibm.co/1KdN913

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 and development, provides security intelligence to help organizations holistically protect their people, 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