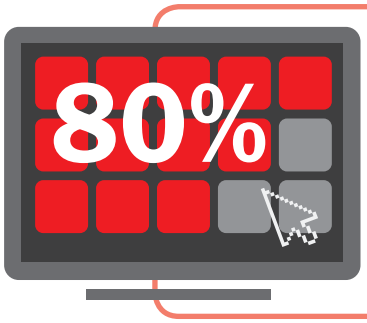
Four Keys to Effective 'Next-Generation' Security

COMBATING ADVANCED THREATS

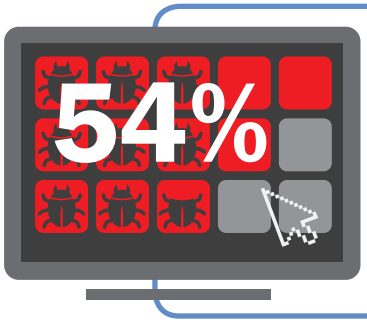
Today's targeted threats are often multi-vectored and exploit unknown vulnerabilities – their sophistication defying typical signature-only based inspection. Whether APTs or client-side threats, they use evasive techniques to penetrate our organizations, often purporting to be or riding on applications and exploiting trust relationships with which we've grown all too comfortable with.



Web application vulnerabilities account for more than 80% of the vulnerabilities being discovered.

Source: Top Cyber Security Risks, SANS Institute

To make matters worse, attackers have realized the inadequacies of traditional signature-based approaches and have accelerated the pace of change and obfuscated their code through polymorphic techniques. By doing so they can circumvent traditional static defenses.



54% percent of malware is active for just 24 hours.

Source: Leading Anti-virus vendor

NEXT-GENERATION FIREWALL (NGFW): SECURITY REBORN

As a result, companies are increasingly turning to application-layer defenses with the theory that, by reducing the attack surface, security teams can more narrowly focus remediation efforts and preventative measures. Witness the genesis for the current 'next-generation' security platform.

One relatively new arrival, the next-generation firewall (NGFW), typically combines the ability to identify and control application use with classic firewall functions. However, there is wide variance in what 'next-generation' really encompasses. This paper identifies crucial components that many deem elementary to true next-generation technology and that are required for effective protection from today's advanced threats.

There are four keys to effective next-generation security that will help ensure optimal defenses:

1

COMPLEX THREATS REQUIRE GREATER VISIBILITY

You cannot protect what you cannot see. Unfortunately, traditional security defenses are mostly blind to today's complex threats – those that exploit seemingly innocuous applications and web sites, and utilize sophisticated social engineering techniques to quietly invade an organization. Even many so-called next-generation firewalls that can detect risky applications and identify suspicious content are often unaware of network, user or other behavior, as well as underlying infrastructure anomalies that can provide early threat warning and increased threat insight. To thoroughly protect, security organizations need to fully understand their networks and the frequent changes occurring within. This requires asset mapping, contextual awareness, cross-source correlation, and total network visibility – and, importantly, the ability to continually analyze and respond to change as it occurs. Only in this manner will we eliminate blind spots that provide attackers the opportunity they seek.

2

CONTROL SHOULDN'T REQUIRE COMPROMISE

Today's next-generation firewalls eliminate unproductive and/or risky application access, and thereby reduce exploitable vulnerabilities, which allows organizations to reduce attack surface area and minimize risks. The exertion of this control, however, needs to be selective and flexible to suit each unique customer environment. Blanket policies alone (e.g. block all social media site access for all users) will likely meet strong resistance and/or lead to excessive false positives that become the bane of security and user organizations alike. A solution that provides fine-grained controls and allows detection and response customization is preferred.

Many next-generation firewalls bolt on under-performing, limited functionality and inflexible intrusion prevention systems (IPS) components to classic firewalls. There is definite operational value to a converged security infrastructure; however, customers should not have to sacrifice performancae, effectiveness, scalability or manageability to get the benefits of it. A next-gen solution should provide the confidence and capability to tailor defenses for targeted threats while protecting completely without compromise to security posture.

3

AUTOMATE SECURITY FOR AGILITY

Having network visibility and awareness, and the ability to control applications, while critical, is still insufficient to adequately address today's dynamic threats and ever-changing computing environment. Threats evolve too rapidly for manually tuned defenses to keep pace. IT consumerization, device mobilization, virtualization and cloud-based computing create a fluid, boundless world to secure. Customers need the agility to stay protected despite the rapid changes and complexity; security automation is the key to keeping pace and discerning what really matters.

New risks can be acted on quickly by tuning security defenses automatically – this can entail auto-applying additional signatures, auto-blocking unknown applications or users, auto-triggering authentication or remediation workflow, etc. Automated event analysis and assessment can also reduce actionable events, concentrating security staff remediation efforts on items of greatest importance. By automatically assessing changes and in turn tuning security policy, organizations can adapt responsively to ensure they maintain their security posture and stay protected.

4

MAINTAIN FLEXIBILITY AND OPENNESS

It is imperative to maintain flexibility when choosing next-generation security architecture. Additional security functions may be required to meet new threats – if the engine has sufficient power, the desired functionality can be layered on without under cutting the system as a whole. Ensure that your chosen solution has the built-in flexibility and performance to grow and scale with your needs and address new security requirements as they emerge.

Organizational factors such as who owns application security and who maintains control policy will influence the chosen path. A flexible security solution will accommodate varying managerial roles (and provide the correspondingly appropriate administrative privileges), so that administrators from each group can leverage the solution for their responsibilities.

Likewise, the ability to easily tailor rules and implement custom defenses for specialized or proprietary applications is important for accuracy and coverage. Many less flexible or closed solutions make this quite difficult if not impossible.

An architecture that can simultaneously perform multiple security functions effectively, while not impeding performance, manageability, scalability or customization, is crucial to achieving optimal advanced threat security protection.

Make sure your solution is architected for change – it is inevitable!

SOURCEFIRE: DELIVERING NEXT-GENERATION SECURITY

Sourcefire® pioneered network and user awareness and our appliances have delivered Next-Generation IPS functionality (an ingredient in true NGFWs) for years. Sourcefire is extending this leadership to provide advanced firewall with integrated application control in a universal, enterprise-ready platform for total network protection. No other solution brings together control and prevention in a flexible, high-performance engine to satisfy the larger need for complete enterprise visibility, adaptive security, and advanced threat protection.

Sourcefire is committed to delivering innovative technologies that help customers combat advanced threats. Visit www.sourcefire.com to learn about new products as they are announced.

If you are interested in learning more about the fight against advanced threats, visit http://blog.sourcefire.com/.

ABOUT SOURCEFIRE

The Sourcefire vision—Security for the Real World—is not only grounded in its history, but propels the company, and industry, forward.

Focused on its mission to be the leader in intelligent cybersecurity solutions, Sourcefire® is transforming the way Global 2000 organizations and government agencies manage and minimize network security risks. With solutions from the network to the endpoint, Sourcefire provides customers with Agile Security™ that is as dynamic as the real world it protects and the attackers against which it defends.

For more information visit www.sourcefire.com.