Deloitte.

Our clients continue to experience challenges through the firewall remediation cycle

Common Challenges
Clients have invested in Next Generation Firewall (NGFW) deployments without fully adopting the capabilities. A lack of automation makes it very difficult to conduct reviews of FW policy efficiently. The remediation strategy is not properly prioritized by risk reduction to the organization.

Marketplace offering
We offer five capabilities that amplify Cyber & Strategic Risk by leveraging automation to conduct NGFW enhancements to increase the speed of review up to 20x.

Quality-oriented
We bring together a powerful combination of accelerators to help expedite enhancement via automation, recertification, and industry knowledge with leading practices.
Our focus on quality and industry knowledge is essential to reducing false positives and creating actionable outputs your team can leverage to prioritize risk reduction.

This presentation contains general information only and Deloitte is not, by means of this presentation , rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation .

As used in this presentation, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com /us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Firewall (FW) enhancement marketplace

Firewall **rule review**

Leverage automation to review the customer's firewall policy, to help identify and prioritize the rules that are causing the significant risk to the organization.

Potential Benefit
Provide an executive risk profile dashboard illustrating organizational vulnerabilities, overly permissive rules, and underutilized Next-Gen firewall capabilities

Firewall **rule remediation**

We are leveraging the risk profiles to help prioritize and establish remediation backlog.

Potential Benefit
Enable the operations team to focus their efforts and resources toward remediating the rules that have the high-quality impact on risk reduction for the organization

Firewall **configuration** review

Assess the customer's firewall configuration against the industry-leading practice and baselines.

Potential Benefit
Third-party comparison of network architecture and design to help determine the organization's ability to continue to advance the ZeroTrust framework and principals

Firewall **rule certification/re-certification**

Develop a certification process to accept new firewall change requests and assign ownership for continued comparison and potential rule decommissioning

Potential Benefit
Established governance and inspect trails when managing firewall rules. Confirming new and existing rules to help maintain compliance with organizational standards and regulatory requirements

Continued maturity
Network segmentation

Cleanup of FW policy will inevitably lead to the more difficult actions of overly permissive rules. This will require traffic analysis and the removal of any-any rules whenever possible. Properly utilizing the FW deployment is essential to establish a strong foundation for the segmentation strategy.

Once a baseline is established, we can help the organization with applications segmentation strategy, user access, Secure Access Service Edge (SASE) requirements gathering, and adopting a zero-trust principal framework.

This may reveal vendor consolidation opportunities, a single pane of glass platform, and cost takeout.

How we help

Automated reporting & risk classification
Automation tactics have scaled the firewall security review process increase the speed up to 20X with an estimated 21,000 resource hours saved per year

Adoption of Application Programming Interface (API) based automation enhances the rate of clean-up for unused objects/rules

Establish governance standards
Develop and apply a consistent risk framework to standardize the analysis of firewalls

Provide risk classification of the rules through the review and remediation process

Enable zero trust model
Leverage zero-trust principles during remediation

An agile approach to threat defense that leverages automation capabilities to enhance security operations and proactively update policies before a threat occurs

Start the conversation

Mike Stevens
Cyber Managing Director
Deloitte & Touche LLP
mistevens@deloitte.com

Kent Gubler
Cyber Specialist Master
Deloitte & Touche LLP
kgubler@deloitte.com

Gary Moreau
Solutions Engineer
Deloitte Services LP
gmoreau@deloitte.com

Cary Hickerson
Sales Executive
Deloitte Services LP
chickerson@deloitte.com