



**ECHELON
RISK +
CYBER**

Managed Firewall Security

Fortify your Firewall Defenses

Managing a firewall manually can be challenging and prone to errors, leading to security gaps from risky, overly permissive, or duplicate rules. This process is time-consuming and can inadvertently expose your assets.

Given that most firewalls are positioned at your perimeter as the first line of defense, it's crucial that they are securely configured, audit-ready, and continuously monitored. Our Managed Firewall Service addresses these challenges by streamlining firewall management, reducing risks, and enhancing your overall security posture.

We ensure that your firewalls are optimized and effectively safeguard your organization, so you can concentrate on achieving your business goals

Services and Solutions, Right-Sized for You

Our Managed Firewall Service not only identifies vulnerabilities but also ensures they are continuously addressed in real-time.

We provide comprehensive firewall management that includes monitoring, automated risk assessments, and detailed compliance reporting. Our solutions are tailored to your needs, featuring streamlined policy optimization, proactive change management, and a unified interface for complete visibility.

By offering scalable and effective cybersecurity, we protect your organization from evolving threats while ensuring your firewall setup is always optimized for performance and compliance. This approach not only strengthens your security posture but also supports your broader business objectives.



We defend the basic human right to security and privacy.

echeloncyber.com

Outcomes and Benefits of Managed Firewall Service

Continuous assessments and threat intelligence to keep you ahead of potential attacks

Security Policy Optimization and Risk Reduction

We focus on cleaning up and improving the overall configuration of security policies. We streamline your security policies by eliminating unused, duplicate, overlapping, or expired rules, consolidating and reordering rules for better organization, and tightening overly permissive settings. This leads to a more efficient and secure policy framework with fewer vulnerabilities, better organization, and more restrictive settings.

Risky Rules Assessment Reports

We identify and evaluate risky security policy rules that could expose critical assets or create vulnerabilities. By assessing the usage of these rules and their impact on your most critical applications, we prioritize and address the most impactful risks. This ensures that your security policies not only become more efficient but also more effective in reducing risks, protecting assets, and improving your overall security posture.

Change Management Risk Assessment

We provide visibility into any changes made on your firewalls and proactively analyze proposed changes before implementation, mitigating potential risks, vulnerabilities, and compliance issues.

Governance & Compliance Assessments & Reports

We conduct thorough assessments to identify network gaps and evaluate compliance with key frameworks such as CIS Benchmarks, FFIEC, HIPAA, NIST, PCI-DSS, as well as custom policies and best practices. Our assessments include the use of CIS Benchmarks and STIGs to ensure devices are configured according to recognized security standards. We also evaluate and implement secure baseline configurations to ensure all devices meet stringent security standards, providing a comprehensive view of your organization's compliance and security posture.

Regular Firewall Technical Support Meetings

We will provide ongoing technical support and operational oversight for firewall management. Each session focuses on reviewing past changes, addressing any emerging issues from reports, and discussing upcoming modifications.

Vulnerability Prioritization Roadmap

We deliver a clear, actionable roadmap to prioritize and address vulnerabilities and misconfigurations, guiding you to focus on the most critical issues first for effective risk management.

