ADVANCED FIREWALL MANAGEMENT SYSTEM

Maximum Protection From Day One

Firewalls are fundamental to your infrastructure security layers, but tend to lose effectiveness over time if not closely managed. CISO Global's Advanced Firewall Management ensures your firewalls give you the same effective protection they did on day one. CISO will log, monitor, flag, investigate, and remediate any changes made to your firewalls.

IT personnel develop strengths and expertise specific to the demands of their environment. In most cases, firewalls are not on the list of daily tasks that must be completed to keep your systems up and running smoothly. What that means is that while your teams undoubtedly have wide expertise, the level required for ongoing patching, remediation, and potentially even reconfiguration is not likely on that list. That doesn't mean your teams are not experts in their own right, just that they don't spend 24/7 tending to firewalls. Our deep bench of expertise includes specialists who focus on complex firewalls daily and maintain the certifications and specialized knowledge that enables them to address this burden quickly and easily on your behalf.

Compliance frameworks such as HIPAA, PCI DSS, and the GDPR require your firewalls to be properly configured, maintained, and aligned to your network as part of the security controls that help you establish a compliant security strategy Whether we are helping install new– or working with existing– firewalls, a comprehensive review of your organization's business requirements, security policies, and compliance framework(s) will ensure that your firewalls are configured for maximum effectiveness to protect you from attacks and continue to update them to keep the same effective protection they did on day one.

CISO experts will keep your firewalls aligned, effective, patched, and up-to-date, using specialized knowledge that comes from working with firewall technologies day-in and day-out

Common Problems Solved by Advanced Firewall Management

Network Changes

Preexisting protocols and controls can lose relevance or become misaligned resulting in compliance violations. CISO can update devices proactively, reducing the risk of a security incident.

Setting Changes Post-Roll Out

A typical oversight to make daily tasks easier can leave your system open to attack. CISO documents, tracks, and traces all changes and ensures rules keep their original effectiveness.

Patches and Updates

Unpatched and not updated firewalls are prime targets for attackers. CISO will keep your firewalls patched and up-to-date, utilizing specialists who focus on complex firewalls daily.

ADVANCED FIREWALL MANAGEMENT

STRATEGY & RISK

- Gap Analysis
- Audit/Assessment
- Third Party Risk Management
- FedRAMP
- StateRAMP
- CMMC
- Advisory
- Virtual CISO
- Managed Compliance
- Managed GRC

CYBER DEFENSE OPERATIONS

- Extended Detection & Response
- Managed Detection & Response
- SIEM as a Service
- Threat Hunting
- Cyber Threat Intelligence
- Digital Forensics
- Vulnerability Management Program
- Attack Surface Reduction
- Cyber Incident Response

CISO

SECURITY ARCHITECTURE & ENGINEERING SOLUTIONS

- Secured Managed Services
- Advanced Firewall Management
- Identity & Access Management
- Cloud Security
- Data Protection
- Remediation

READINESS & RESILIENCY

- Penetration Testing
- Tabletop Exercises with Incident Response Retainer
- Training Programs

AICPA SOC aicpa.org/soc4so

SOC 2® Type II Audited

CISO GLOBAL

480-389-3444 | ciso.inc