RESOLVE

EXECUTIVE PLAYBOOK

NETWORK SECURITY · FIREWALL CHANGE

The Firewall Change *Automation* Playbook

How network and security leaders turn firewall requests into orchestrated, verified and audit-ready policy changes across every vendor and cloud.

PUBLISHED
October 2026

READING TIME
30 minutes

OVERVIEW

Firewall Policy Moves At The Speed Of Its Slowest Handoff

Firewall estates now span several vendors, clouds and teams, yet most change processes still run on tickets, spreadsheets and console sessions. A simple access request bounces between requesters, engineers, security reviewers and change boards before anyone types a rule. This playbook gives leaders a model for running firewall change as orchestrated, verified and self-documenting workflows.

EXECUTIVE SUMMARY

One in three organizations sees more than ten application disruptions a year from firewall changes, and most rules in a typical rule base have no documented owner. Leaders who orchestrate change from request to verified rule shorten lead time, prove every change did exactly what was asked, and keep rule bases clean and audit-ready.

Key Findings

01 **Changes break production.** One in three organizations sees more than ten application disruptions a year from firewall changes, and 29% miss partner SLAs because of change management.

02 **Rule bases outgrow their owners.** 62.6% of firewall rules lack an owner or documentation, about 30% are completely unused, and 60% of enterprise firewalls fail high-severity compliance checks at first evaluation.

03 **The edge is the target.** Edge devices and VPNs accounted for 22% of vulnerability exploitation in breaches, up from 3%, with a median of 32 days to remediate.

04 **Manual process is the bottleneck.** Half of organizations call manual change management their biggest policy challenge, and half still rely on Excel or manual tools.

Recommendations

01 **Turn access requests into workflows.** Run intake, path analysis, risk scoring and implementation as one flow, with approval gates on high-risk changes.

02 **Verify every change.** Post-change connectivity tests and diffs confirm each rule does exactly what was requested.

03 **Give every rule an owner and an expiry.** Recertify on a schedule and retire unused rules automatically.

04 **Make threat blocking one action.** Push a block to every firewall and cloud edge from a single trigger.

05 **Generate evidence as you execute.** Capture every request, approval, diff and test result for PCI DSS, NIST and SOX.

PLANNING ASSUMPTION

By 2028, enterprises that orchestrate firewall change end to end will implement standard access requests in minutes and spend review time only on the changes that carry real risk.

PLANNING ASSUMPTION

By 2028, auditors will expect every firewall rule to carry an owner, a business justification and an expiry, recorded by the system that implemented it.

ANALYSIS

01 The Change Gap

Security investment has concentrated on the controls themselves: next-generation firewalls, cloud security groups and zero trust architectures. The risk now sits in how policy on those controls changes, because every request depends on a chain of handoffs and every push depends on someone typing it correctly.

The research points the same way from three directions: changes break production, rule bases outgrow the people who own them, and attackers increasingly target the edge itself.

Exhibit 1. Three Signals That Firewall Change Is A Board-Level Risk

THIRD-PARTY RESEARCH

1 in 3

organizations sees more than ten application disruptions a year caused by firewall configuration changes.

Source: Tufin, State of Firewall Management, Dec 2024

62.6%

of firewall rules lack an owner or documentation, so nobody can safely retire them.

Source: FireMon Insights analysis, 2025

22%

of vulnerability exploitation in breaches targeted edge devices and VPNs, up from 3% a year earlier.

Source: Verizon, 2025 Data Breach Investigations Report

Exhibit 2. Rule Bases And Change Processes Under Strain

SHARE OF RULES OR ORGANIZATIONS

RULE BASE FINDINGS		OPERATING PRESSURE	
No owner or documentation	62.6%	Rely on Excel or manual tools	50%
Completely unused	~30%	Miss partner SLAs	29%
Redundant or shadowed	10%+	Miss SLAs, large enterprises	43%

Sources: FireMon Insights analysis of enterprise rule bases, 2025 (left); Tufin State of Firewall Management, survey of 105 IT and security leaders, Dec 2024 (right). Bars drawn on a common 0 to 100% scale.

IMPLICATION

Firewall change is now an operational capability to be engineered, measured and audited. The fastest teams treat policy change as software: requested in a structured way, analyzed before it lands and verified after.

DIAGNOSIS

02 Six Places Firewall Change Breaks Down

Reviews of slow or failed firewall changes tend to name the same handful of causes. Each one is a gap between what the policy says and what a team can execute at volume, and each one closes when the step becomes an orchestrated action with a defined owner, input and check.

FAILURE POINT	WHAT IT LOOKS LIKE	BUSINESS CONSEQUENCE	RESOLVE COUNTERMEASURE
Incomplete Requests	Requests arrive with hostnames instead of IPs, missing ports or no business justification.	Days lost to back-and-forth before any work starts.	Structured intake enriched from CMDB and IPAM before an engineer sees it.
Manual Path Analysis	Engineers trace routes and zones by hand across vendors and clouds.	Changes land on the wrong device or miss one in the path.	Automated path calculation across every firewall and cloud control.
Approval Queues	Every change waits for the weekly change board regardless of risk.	Low-risk work queues behind high-risk work and SLAs slip.	Risk scoring routes standard changes through pre-approved policy and gates the rest.
Fat-Finger Implementation	Rules typed into consoles one device at a time.	Overly broad rules, typos and outages from configuration changes.	Consistent pushes through vendor APIs with pre-checks and automated rollback.
Rule Sprawl	Rules are added for every project and never removed.	Unused and shadowed rules widen the attack surface and slow every audit.	Owners, expiry dates and scheduled recertification on every rule.
Audit Scramble	Evidence pulled from tickets, emails and console screenshots.	Findings, failed compliance checks and weeks of rework.	Every request, approval, diff and test result logged as it executes.

LEADER ACTION Pull your last 50 firewall changes, measure the elapsed time from request to verified rule, and mark where each one waited. The longest waits are your first automation backlog.

FRAMEWORK

03 The Resolve Change Execution Model

Every firewall change runs through five phases. Resolve carries the enrichment, analysis, implementation and checks at machine speed, while people make the calls that carry security risk with the facts in front of them.

Exhibit 3. Five Phases Of An Orchestrated Firewall Change RESOLVE FRAMEWORK

Request & Enrich
Structured intake pulls IPs, owners and zones from CMDB and IPAM before analysis starts.

Analyze
Path calculation, existing-rule checks and risk scoring against zone policy and PCI scope.

Approve
Standard changes pass under pre-approved policy; high-risk changes reach an approver in Teams or Slack.

Implement
Resolve pushes the narrowest rule to every device in the path through vendor APIs and CLI.

Verify & Document
Connectivity tests, diffs and approvals post to the ticket and the audit record.

HOW THE RESOLVE PLATFORM MAPS TO THE MODEL

BUILD
Jarvis
Describe a change pattern in plain language and Jarvis assembles the workflow for review and testing.

START FAST
The Automation Vault
Prebuilt workflows and building blocks for rule requests, threat blocks and recertification.

CONNECT
Integrations
API and CLI reach across Palo Alto, Fortinet, Check Point, Cisco, AWS and Azure, plus ServiceNow and Jira.

KNOW
Knowledge Agent
Surfaces policy standards, zone maps and prior change history in the moment.

EXECUTE
Automation Agent
Executes changes across vendors with pre-checks, logging and rollback paths built in.

GUIDE
Agent Assist
Guides engineers through risk decisions and gives requesters a conversational view of status.

ASSESSMENT

04 The Firewall Change Maturity Model

Use the five levels to place your program and set a realistic next step. Level 3 for standard access requests is achievable within a quarter once the first workflows reach production.

L1 Ticket-Driven

HOW CHANGE RUNS
Requests arrive by email or ticket. Engineers analyze and implement by hand in each vendor console.

TESTING & EVIDENCE
Changes are confirmed by the requester, if at all. Audits are assembled manually once a year.

NEXT MOVE
Measure change lead time and map every firewall, manager and cloud control in scope.

L2 Scripted

HOW CHANGE RUNS
Engineers use scripts and vendor managers per platform. Intake, analysis and approvals stay manual.

TESTING & EVIDENCE
Some pre-checks per vendor. Evidence is collected by hand after each change.

NEXT MOVE
Connect intake, path analysis and implementation into one workflow with a single approval gate.

L3 Orchestrated

HOW CHANGE RUNS
Standard access requests run end to end from intake to verified rule, with approval gates on high-risk changes.

TESTING & EVIDENCE
Every change is verified after the push, and evidence is captured automatically.

NEXT MOVE
Add rule ownership, expiry dates and scheduled recertification.

L4 Continuously Compliant

HOW CHANGE RUNS
Rules carry owners and expiry dates, recertification runs on schedule and configs are checked against baseline daily.

TESTING & EVIDENCE
Compliance evidence is generated continuously and mapped to PCI DSS and NIST controls.

NEXT MOVE
Extend coverage to cloud security groups and threat-driven changes.

L5 Intent-Based

HOW CHANGE RUNS
Policy intent drives changes across vendors and clouds. Agents propose the narrowest rule from live traffic and present it for approval.

TESTING & EVIDENCE
Continuous verification, with live policy posture reported to leadership.

NEXT MOVE
Extend the model to zero trust segmentation and application onboarding.

SELF-CHECK If your team cannot tell you who owns a given rule and why it exists within five minutes, your program is operating at Level 2 or below, regardless of what the policy document says.

USE CASES

05 Eight Firewall Workflows To Orchestrate With Resolve

Automated step Human approval gate

01 Access Request To Verified Rule

ACCESS REQUESTS

TRIGGER

A user or application team submits a connectivity request in the ServiceNow or Jira catalog.

ORCHESTRATED RESPONSE

1. Validate request fields and resolve hostnames to IPs and objects from CMDB and IPAM.
2. Calculate the network path and identify every firewall and cloud control in it.
3. Check existing policy and close the request if access is already allowed.
4. Score risk against zone policy, PCI scope and security standards.
5. **Gate:** security approves high-risk changes; standard changes proceed under pre-approved policy.
6. Push the narrowest rule to each device, run a connectivity test and close the request with evidence.

SYSTEMS IN SCOPE

ServiceNow, Jira, CMDB, IPAM, Palo Alto Panorama, FortiManager, Check Point

IN PRODUCTION

A multinational cable and telecom group automates firewall change implementation on Resolve across its affiliates.

KPI TO TRACK

Lead time for standard changes

02 Emergency Threat Blocking Across Every Edge

THREAT RESPONSE

TRIGGER

SIEM, EDR or a threat intelligence feed confirms a malicious IP address, domain or URL.

ORCHESTRATED RESPONSE

1. Enrich the indicator with threat intelligence and check it against business-critical destinations.
2. **Gate:** the SOC lead approves the block when the indicator touches a critical asset.
3. Push the block to dynamic address groups and block lists on every firewall and cloud edge.
4. Verify the block is active on each enforcement point.
5. Set an expiry and review date, then update the incident record.

SYSTEMS IN SCOPE

SIEM, EDR, threat intelligence platform, Palo Alto, Fortinet, Check Point, AWS and Azure

WHY IT MATTERS

Edge devices and VPNs were 22% of vulnerability exploitation in breaches last year, up from 3%.

KPI TO TRACK

Time to block on every enforcement point

03 Rule Recertification And Cleanup

RULE HYGIENE

TRIGGER

A quarterly schedule, or a rule that records zero hits for 90 days.

ORCHESTRATED RESPONSE

1. Pull hit counts, last-used dates and owners for every rule across vendors.
2. Flag unused, shadowed, redundant and expired rules.
3. Send each owner a recertification request in Teams or Slack with usage data attached.
4. **Gate:** the owner certifies the rule or approves its retirement.
5. Disable retired rules, watch for impact through a grace period, then remove them and record the decision.

SYSTEMS IN SCOPE

Firewall managers, cloud security groups, Teams or Slack, ServiceNow, GRC platform

WHY IT MATTERS

About 30% of rules are completely unused, and 62.6% have no owner or documentation.

KPI TO TRACK

Share of rules with an owner and current certification

04 Time-Bound Vendor And Project Access

TEMPORARY ACCESS

TRIGGER

A request for vendor, contractor or project access with a defined end date.

ORCHESTRATED RESPONSE

1. Validate the sponsor, vendor record and requested scope.
2. **Gate:** the sponsor approves scope and duration.
3. Create the firewall rule and VPN access with an expiry tag.
4. Notify the sponsor before expiry and offer a one-click extension.
5. Remove the rule and revoke VPN access at expiry, then confirm removal on every device.

SYSTEMS IN SCOPE

ServiceNow, VPN gateways, firewall managers, identity provider, Teams or Slack

IN PRODUCTION

A managed IT services provider automates VPN access grants on Resolve across HP Service Manager, Jira and Ansible.

KPI TO TRACK

Expired rules removed on schedule

05 Application Decommission Cleanup

LIFECYCLE

TRIGGER

A decommission change request, or a server status change in the CMDB.

ORCHESTRATED RESPONSE

1. Find every rule, object and NAT entry tied to the servers' addresses across vendors and host firewalls.
2. **Gate:** the application owner confirms the decommission scope.
3. Disable the rules and confirm no traffic through a monitoring window.
4. Remove rules and objects, then update CMDB and IPAM records.

SYSTEMS IN SCOPE

CMDB, IPAM, firewall managers, Windows and Linux host firewalls, ServiceNow

IN PRODUCTION

A global retailer automates adding and deleting Windows and Linux host firewall rules, plus open port audits, on Resolve.

KPI TO TRACK

Orphaned rules remaining after decommission

06 Cloud Security Group Drift Remediation

MULTI-CLOUD

TRIGGER

A cloud change event, or a scheduled scan of AWS security groups and Azure network security groups.

ORCHESTRATED RESPONSE

1. Compare security groups and NSGs against the approved baseline policy.
2. Flag any-to-any rules, internet-exposed management ports and unapproved changes.
3. **Gate:** cloud security approves remediation for production workloads.
4. Revert to baseline or apply the approved rule, then notify the resource owner.
5. Log the drift and the remediation to the audit record.

SYSTEMS IN SCOPE

AWS, Azure, cloud APIs, Splunk, ServiceNow, Teams or Slack

WHY IT MATTERS

Only 20% of organizations consistently manage firewall policy across on-premises and cloud assets.

KPI TO TRACK

Time to remediate cloud policy drift

07 Configuration Backup And Compliance Drift

COMPLIANCE

TRIGGER

A nightly schedule, or a configuration change event in syslog.

ORCHESTRATED RESPONSE

1. Back up the running configuration from every firewall and manager.
2. Diff it against the golden baseline and the last approved change.
3. Run PCI DSS and CIS benchmark checks on the result.
4. **Gate:** security reviews any unauthorized change and approves the revert.
5. Revert or open a change record, with the diff and evidence attached.

SYSTEMS IN SCOPE

Firewalls and managers via API and CLI, syslog, Splunk, ServiceNow, GRC platform

IN PRODUCTION

A North American fiber infrastructure provider automates network device configuration backups on Resolve.

KPI TO TRACK

Time to detect an unauthorized change

08 Change Window Execution With Automated Rollback

CHANGE EXECUTION

TRIGGER

An approved change reaches its scheduled window.

ORCHESTRATED RESPONSE

1. Pre-check HA pair status, session counts and configuration sync.
2. Snapshot the configuration and push the change.
3. Run post-change tests for application reachability and performance.
4. Roll back automatically if a test fails, and notify the change owner.
5. **Gate:** the change manager reviews results and closes the change.

SYSTEMS IN SCOPE

Palo Alto, F5, Cisco, Fortinet, ServiceNow, monitoring tools

IN PRODUCTION

A global travel technology provider automates Palo Alto change, configuration and reboot workflows on Resolve.

KPI TO TRACK

First-time-right change rate

BUILD IT IN JARVIS

"When a ServiceNow firewall request for the payments zone is approved, find every firewall in the path between source and destination, check whether existing rules already allow the traffic, and if they do not, create the narrowest rule on Panorama and FortiManager with a 90-day expiry. Run a connectivity test, attach the diff and test result to the request, and close it."

Example prompt. Jarvis turns a plain-language description into a workflow your team reviews, tests and versions before it runs in production.

FIELD EVIDENCE

06 Network And Security Workflows Resolve Customers Run Today

ACROSS THE RESOLVE CUSTOMER BASE

Network Automation Proven At Carrier Scale

200K+
closed-loop network automations every day at a global telecom carrier

$97M
saved annually with automated network recovery at a global telecom services provider

99%
faster MTTR delivered for Resolve customers

100%
of overtime eliminated at Syniverse

MULTINATIONAL CABLE AND TELECOM GROUP

Firewall Change Implementation

Firewall changes run as standardized workflows as the group consolidates automation across its affiliates.

- Firewall change implementation automation
- Alarm and log collection across network devices
- Load balancer farm alarm handling

CA Spectrum, Remedy, SMTP, network devices

$1M a year saved at one affiliate, with 4,800 fewer tickets a month at another

GLOBAL TRAVEL TECHNOLOGY PROVIDER

Palo Alto Change And Configuration

Firewall and load balancer changes run as validated workflows in an operation handling 200,000 changes a month.

- Palo Alto change, configuration and reboot
- Load balancer pair failover, sync and validation
- Flapping circuit diagnosis and traffic rerouting

Palo Alto, F5, Cisco, IBM MQ

60% of incident types addressed by the first 16 runbooks

GLOBAL RETAILER

Host Firewall Rule Lifecycle

Host firewall rules and port audits run as self-service workflows with consistent execution across the server estate.

- Add and delete Windows firewall rules
- Add and delete Linux firewall rules
- Open port inventory on Windows and Linux

Windows, Linux, VMware vCenter, Active Directory, easyVISTA

66 infrastructure and IT workflows in the library

LEADING EUROPEAN TELECOM OPERATOR

VPN Fulfillment From Inventory Data

Fulfillment data arrives over REST, is enriched with inventory information and drives VPN creation automatically.

- Fulfillment data retrieval over REST
- Enrichment with CMDB inventory data
- VPN creation through the fulfillment subsystem

BMC Remedy, IBM MQ, Micro Focus, CMDB via REST

90% of L1 NOC operations fully automated

MANAGED IT SERVICES PROVIDER

Self-Service VPN Access

VPN access requests flow from the service desk into automated grants, alongside the provider's most common operational fixes.

- Grant VPN access
- Failed web service remediation
- Password resets and mailbox fixes

HP Service Manager, Jira Service Desk, Splunk, Ansible

9 automated workflows in the library

GLOBAL IT SERVICES PROVIDER

Privileged Access And Security Audits

Security audits of privileged groups and local administrators run as repeatable actions across hundreds of client accounts.

- Active Directory high-privilege group audits
- Local administrator extraction for audit
- Admin access security reporting

Active Directory, PowerShell, ServiceNow, Exchange

20–40% workload reduction across accounts

NORTH AMERICAN FIBER INFRASTRUCTURE PROVIDER

Device Backups And Proactive Alerting

Network device backups and customer outage alerts run automatically from the NOC event stream.

- Optical device configuration backups
- Proactive alerts to customers on impacting outages
- NOC alarm ticketing and enrichment

Netcool, Salesforce, Assure1

7 network operations workflows in the library

UK TELECOM CARRIER

Automated Network Service Verification

Tickets trigger end-to-end diagnostics that verify IP data and WLAN services across provider and customer edge devices.

- Automation triggered from Remedy tickets
- Juniper and Cisco edge diagnostics
- End-to-end service tests and monitoring

BMC Remedy, Juniper, Cisco, SQL, Exchange

13M+ automation executions a year

THE PATTERN

Customers start with the repetitive, well-defined changes: VPN grants, host firewall rules, configuration backups and standard access. Once those run reliably as workflows, the same building blocks compose into cross-vendor policy change, threat response and continuous compliance.

Customer use cases and results from the Resolve customer use case library. Results are customer-reported and reflect each customer's broader Resolve deployment. Customers are described by industry.

SCENARIO

07 Urgent Access Request At 09:05: Two Ways The Change Lands

A payments team needs a new service to reach a database across three firewalls and a cloud security group. The firewalls, policies and people are identical in both timelines. The difference is how the change executes.

Manual Process — 3d 6h

- **Mon 09:05** Request submitted with a hostname and "needs port 443."
- **Mon 13:40** Firewall team asks for source IPs and a business justification.
- **Tue 10:20** Requester replies. An engineer traces the path by hand across three firewalls.
- **Tue 16:00** Change queued for the weekly change board.
- **Thu 11:00** Change board approves.
- **Thu 13:30** Rule pushed by hand. One destination object is wrong and the test fails.
- **Thu 15:05** Corrected and live. Evidence is rebuilt from tickets at audit time.

Orchestrated With Resolve — 17m

- **09:05** Request submitted. Hostnames resolved from CMDB and IPAM automatically.
- **09:06** Path calculated across three firewalls and a cloud security group.
- **09:07** No existing rule allows the flow. Risk scored as standard against payments zone policy.
- **09:08** Approved under pre-approved policy, with owner and 90-day expiry recorded.
- **09:14** Narrowest rule pushed to every device in the path.
- **09:19** Connectivity test passes from source to destination.
- **09:22** Request closed with diff, test result and approval trail attached.

275x
faster from request to verified rule in this scenario

2 min
from request to a scored risk decision

0 hrs
spent assembling audit evidence after the change

Illustrative scenario. Timings are modeled for planning purposes and will vary by environment, policy and approval model.

MEASUREMENT

08 The Firewall Change Scorecard

Report these seven measures to leadership every quarter. Each comes straight from workflow execution and policy analysis data, so the scorecard updates itself as changes run.

METRIC	DEFINITION	WHY LEADERS CARE	TARGET
Change Lead Time	Median time from request to verified rule for standard changes	The speed the business feels on every request	Under 1 hour
First-Time-Right Rate	Share of changes that pass post-change verification on the first attempt	Every failed change is an outage risk	98%+
Rule Ownership	Share of rules with a named owner and business justification	Unowned rules never get retired	100%
Recertification Coverage	Share of rules recertified in the last two quarters	Keeps the rule base aligned with the business	100%
Rule Base Hygiene	Share of rules that are unused, shadowed or redundant	Every stale rule widens the attack surface	Under 5%
Time To Block	Minutes from confirmed indicator to block on every enforcement point	Response speed at the edge	Under 10 min
Unauthorized Change Detection	Time from an unapproved configuration change to detection	Drift is where exposure starts	Under 24 hrs

WHERE EACH NUMBER COMES FROM

EXECUTION LOGS

Every Change

Timestamps on each step feed change lead time, first-time-right rate and time to block.

POLICY ANALYSIS

Every Rule

Hit counts, owners and recertification records feed ownership, coverage and hygiene.

EVIDENCE PACKS

Every Audit Record

Configuration baselines and diffs mapped to PCI DSS, NIST and SOX feed drift detection.

ACTION PLAN

09 The 90-Day Firewall Change Roadmap

Start with two workflows that prove value quickly: standard access requests for one firewall domain and emergency threat blocking, then expand on a predictable cadence.

Days 0–30

Baseline

- Inventory firewalls, managers and cloud controls across vendors.
- Measure lead time and first-time-right rate for the last quarter.
- Export rule hygiene: unused, shadowed and unowned rules.
- Select two pilot workflows from The Automation Vault.

EXIT CRITERIA

Baseline scorecard published to leadership.

Days 31–60

Orchestrate

- Build access request and threat block workflows with Jarvis.
- Define standard change policy, risk scoring and approval gates.
- Connect ServiceNow, CMDB and IPAM for enrichment.
- Run the first changes with post-change verification.

EXIT CRITERIA

First standard changes live and verified in under an hour.

Days 61–90

Prove And Expand

- Launch recertification with owner notifications.
- Add configuration backup and compliance drift checks.
- Report the first quarter-over-quarter scorecard.
- Set the backlog for cloud security groups and decommission cleanup.

EXIT CRITERIA

Standard changes operating at Level 3 or above.

FOR THE BOARDROOM

Six Questions Your Board Will Ask

Q1
How long does a standard firewall change take today, from request to verified rule?

Q2
How many of our firewall rules have no owner or business justification?

Q3
Could we block an active threat on every firewall and cloud edge within ten minutes?

Q4
Who approved the rules that expose our payment and customer data zones?

Q5
How would we know if someone changed a firewall outside the change process?

Q6
Can we hand auditors evidence for every rule change last quarter within the hour?

EVIDENCE

10 Evidence And Methodology

1 **Tufin, State of Firewall Management Research Report, December 2024.** Survey of 105 IT and cybersecurity leaders at organizations with 20 or more firewalls, fielded September 2024, margin of error ±9.5 points. Source of the disruption, manual process, Excel, SLA and hybrid management findings. lp.tufin.com/State-of-Firewall-Research-Report-Dec2024

2 **FireMon Insights analysis of enterprise firewalls, July 2025.** Anonymous deployment data across large enterprises and regulated industries. Source of the ownership, unused rule, redundant rule and compliance check findings. securitybrief.news/60-of-enterprise-firewalls-fail-initial-compliance-study

3 **Verizon, 2025 Data Breach Investigations Report.** Source of the edge device and VPN exploitation share and the 32-day median remediation time. cyberscoop.com/verizon-data-breach-investigations-report-2025

4 **Resolve customer use case library.** Source of the field evidence in section 06 and the In Production notes in section 05. Workflow counts reflect use cases recorded per customer. Results are customer-reported and reflect each customer's broader Resolve deployment. Customers are described by industry.

5 **Standards context.** PCI DSS v4.0 Requirement 1 on network security controls, NIST SP 800-41 Rev. 1 firewall policy guidelines and CIS benchmarks inform the compliance use cases and scorecard.

HOW TO READ THIS PLAYBOOK

Key Findings draw on third-party research cited above. Recommendations, the execution model, the maturity model and scorecard targets reflect Resolve's point of view and field experience. Planning assumptions are forward-looking judgments intended to support strategy and budgeting.

ABOUT THE SCENARIO

The access request scenario in section 07 is illustrative. It holds firewalls, policies and people constant and varies only the execution method, to isolate the effect of orchestration on change lead time.

NEXT STEP

Turn Every Firewall Change Into A Verified Workflow

Start with standard access requests. Resolve helps your team build, test and prove its first orchestrated change workflow, then scale it across every vendor, cloud and zone.

Get Started

Explore The Automation Vault

RESOLVE

© 2026 Resolve. This playbook is provided for planning purposes. Third-party research is cited in section 10. Customer results are customer-reported and vary by environment. resolve.io