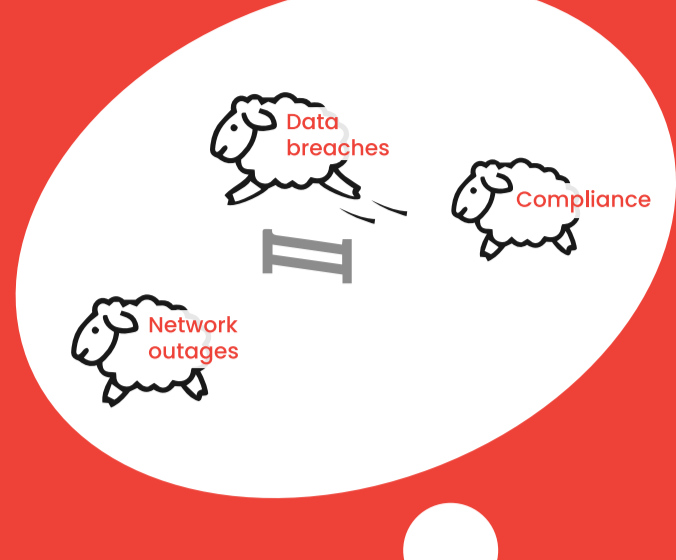


ENDLESSLY WORRYING ABOUT YOUR ENTERPRISE'S SECURITY?

Remediate your Security Concerns IN MINUTES



CISOs, what's keeping you up tonight?

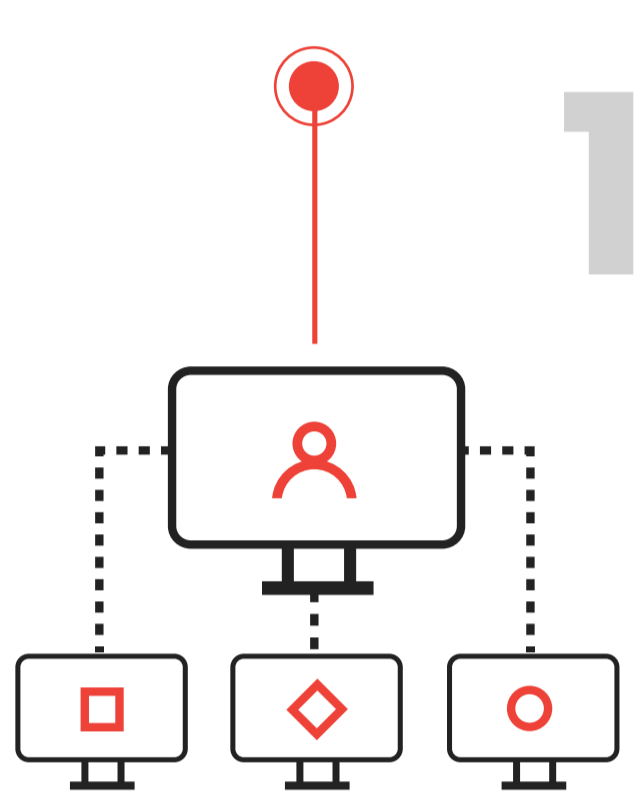
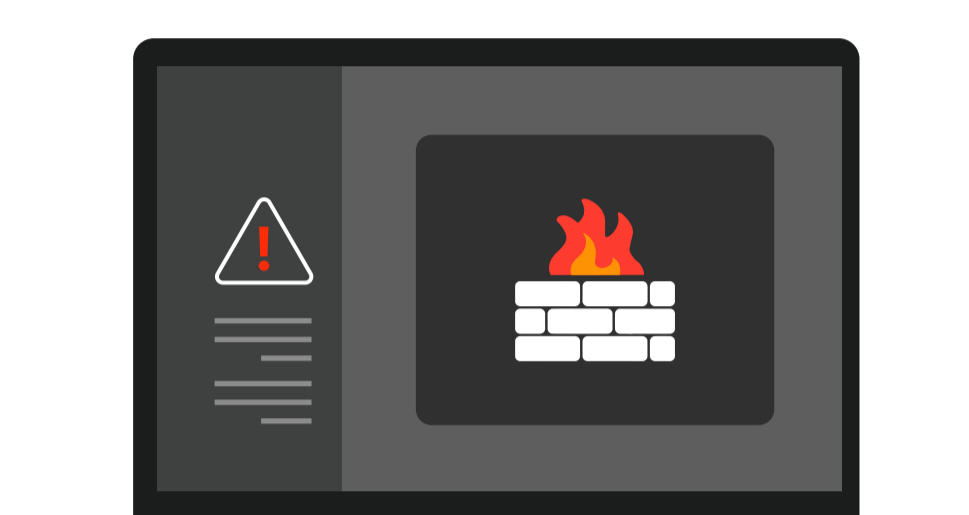
If you're a seasoned CISO, you would be spending sleepless nights worrying about your enterprise's security posture. "How safe am I from the perils of data breaches and network outages? Is my team well-equipped to recover unscathed from a potentially crippling incident? Was moving to the cloud really a good idea? Are the tools that I've invested in delivering the promised results, or are they just a big waste of budget?"

Here, we take a shot at answering those questions.

Consider the following scenario-

Let's say a network outage happened because someone accidentally messed up a network firewall configuration.

Now, we break down the problem into two parts-



1

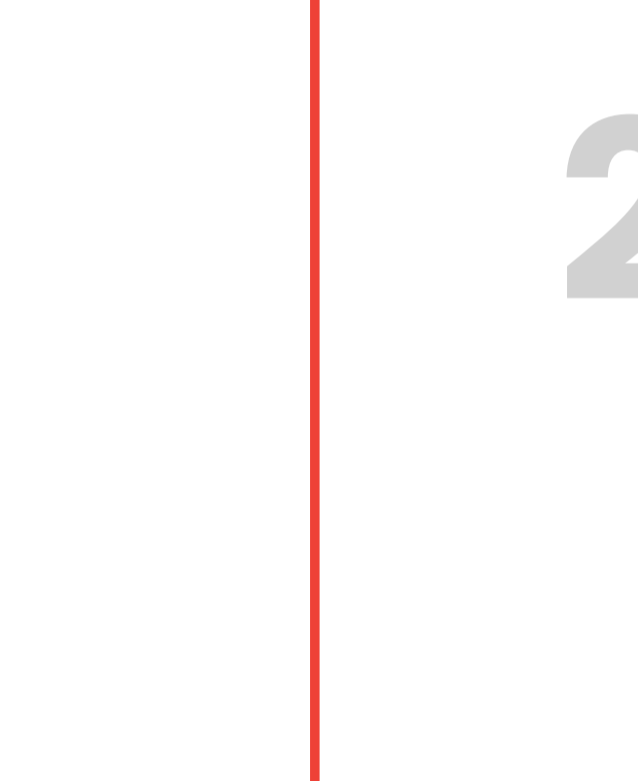
The person wasn't supposed to be meddling with network firewalls in the first place - only security admins were allowed to access and configure them. Our guy slipped through the cracks, and despite his good intentions, managed to bring the network down.

How could you have prevented it from happening?

Broker privileges with Role-Based Access Control (RBAC).

With AUTOMATION+ granular RBAC, you can make sure only authorized users have access to specific network parts, preventing both accidental and deliberate mishaps.

[Show Me How](#)



2

It's been a day since the incident took place. Your application and network data are in danger of being breached. Reports of exploitation have already started popping up. However, your security team still hasn't decoded the firewall rule that is the cause of all trouble, let alone troubleshoot it. What's more, it took them several hours to even figure out where the issue lay. With every passing minute, the danger rises.

How can you expedite troubleshooting and remediation?

Automation is key to quick remediation.

Automate patch management, perform context-aware troubleshooting and auto-remediation for instant, error-free resolution. AUTOMATION+ allows you to take scheduled or on-demand backups, both at the device and object level, for config checks, and rollbacks, and audits.

In this case, you can compare the current firewall configuration with the previous configuration, and figure out where exactly the fault occurred. You can then quickly roll back to the previous configuration, saving your network from downtime and data breaches.

[Watch How It Works](#)



Now, you may say this is a one-off incident. How do you ensure high performance, security, and compliance on a day-to-day basis? Especially as the DevOps, SecOps, and NetOps teams each have their own toolchain?



Collate validate conquer.

Perform pre- and post-validation checks when implementing a change, generate periodic risk reports, and maintain logs. Up your vulnerability mitigation game with improved monitoring, triage, and remediation.

AUTOMATION+ integrates with an array of DevSecOps tools like Ansible, Terraform, Jenkins, ServiceNow, etc., and provides a single pane of control from which you can monitor and orchestrate all that goes on in your network and application infrastructure. The result? Manual goes out, errors go down, and productivity skyrockets.

[See It in Action](#)



What if you happen to be cloud-hosted? Or use containerized, microservice deployments such as Docker or Kubernetes?

Whatever your environment is, you can rest assured it's free of risks. Perform service discovery, monitoring, and management, standardize processes, and enforce compliance - no sweat.

Sounds too good to be true? You don't have to take our word for it. Our experts will give you a product walkthrough tailored to your unique security requirements, you won't lose sleep again.

[Arrange a Tailored Review](#)