

## SOLUTION GUIDE

# Pragmatic Steps Toward a Zero Trust Future

*Connect the dots between your current perimeter-based security infrastructure to a zero trust future with security policy management from FireMon.*

*First defined over a decade ago, zero trust has picked up momentum in recent years. The Federal Government has made its adoption a priority for many agencies, and many private enterprises are beginning to follow suit. Zero trust offers many long-term advantages to organizations looking to secure their assets, protect their users and customers, and harden their defenses.*

*However, the complexity of adopting a true zero trust approach leaves most organizations wondering where to start—and how far to go. Many midsize companies may find that the added security of a full migration to a zero trust architecture (ZTA) simply isn't worth the expense or complexity. For some, strategically adopting key zero trust workflows will produce the best improvement to security posture with minimal disruption to operations.*

*This solution guide outlines the challenges of establishing a ZTA foundation, and describes the best technological and operational methods around them. We will discuss approaches to satisfying the National Institute of Standards and Technology (NIST) requirements around aggregating network traffic data and capturing the current state of enterprise assets, which are among FireMon's many NIST- and executive order-compatible capabilities.*

## Cost, Continuity, and Complexity: The Barriers to Zero-Trust

Zero trust is often described in terms of a journey or a process, and a big reason for that metaphor is that a pure ZTA would be exceedingly difficult to implement instantaneously. Cost and operational continuity are the main impediments, as the expense and logistical difficulties of replacing individual systems can be significant, let alone wholesale replacement of entire workflows.

Another difficulty with adopting a ZTA is that that migrating systems to zero trust often introduces significantly more complexity. Security policies can proliferate with increased network segmentation, constant verification, and flexible context-dependent access paths.

But even more importantly, zero trust is as much about approach and operations as it is technology. NIST even calls this out specifically within SP 800-207: “[transitioning] to ZTA is a journey concerning how an organization evaluates risk in its mission and cannot simply be accomplished with a wholesale replacement of technology.” Moving to zero trust means changing how the entire organization thinks about security and adapts that to their day-to-day workflows.

## Leverage Your Existing Infrastructure Investments for Zero Trust

The good news in all of this is that many organizations already have more zero trust capabilities within their tech stack than they realize—they just need to make the most out of them.

FireMon supports the complex network security policy management needs of large enterprises today, while providing the flexibility to effectively adopt zero trust workflows as the organization is ready to do so. For many organizations, IP address remains the best way to identify a trusted device, and the paths between them are represented by security policies—managing those policies is key to managing identity. Additionally, FireMon provides advanced device discovery/identification, workflow automation, comprehensive risk analysis, policy lifecycle management, traffic flow analysis, microsegmentation support, and more: helping organizations take the first steps toward zero trust without additional technology spend.

This means you don't have to choose between maximizing your existing technology investments or a move toward zero trust: you can organize, manage, and strengthen your existing network infrastructure as the basis of your hybrid zero trust-perimeter hybrid architecture.

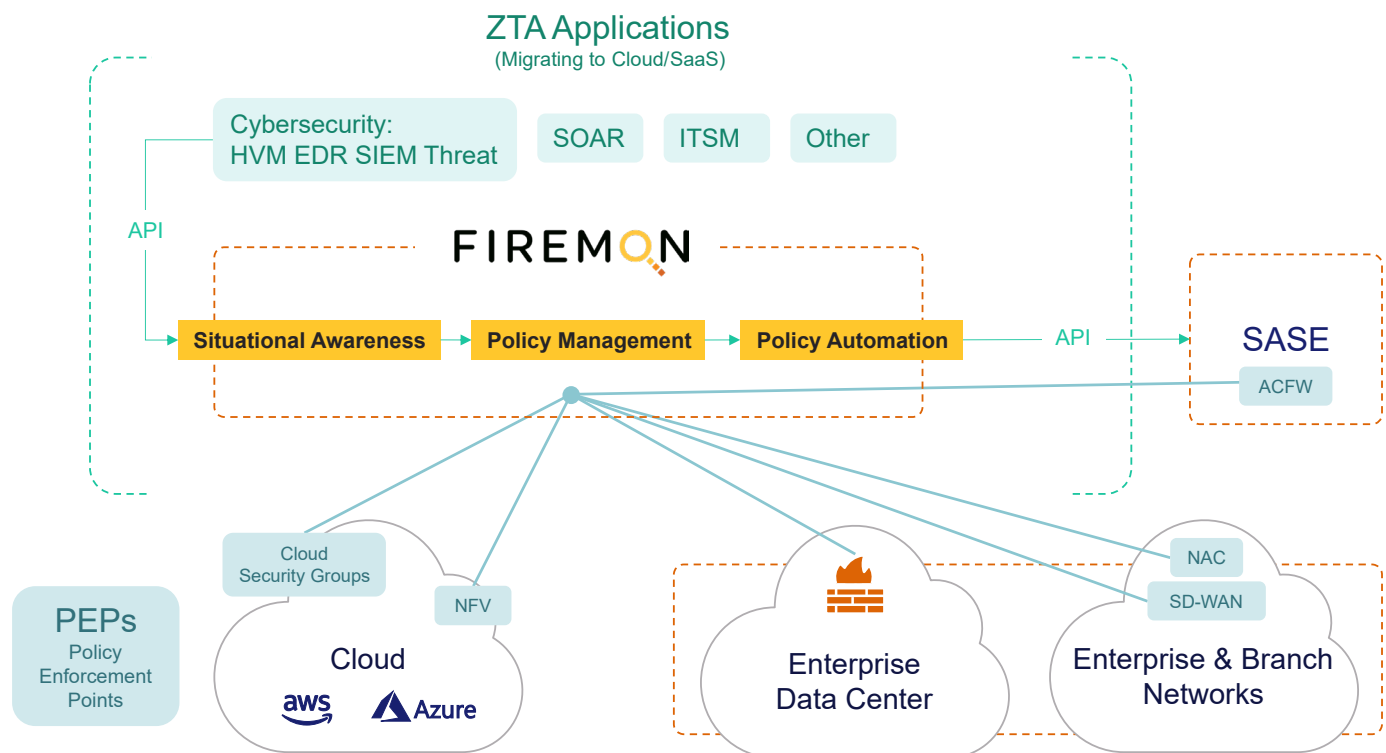


Figure 1: FireMon Zero Trust Reference Architecture

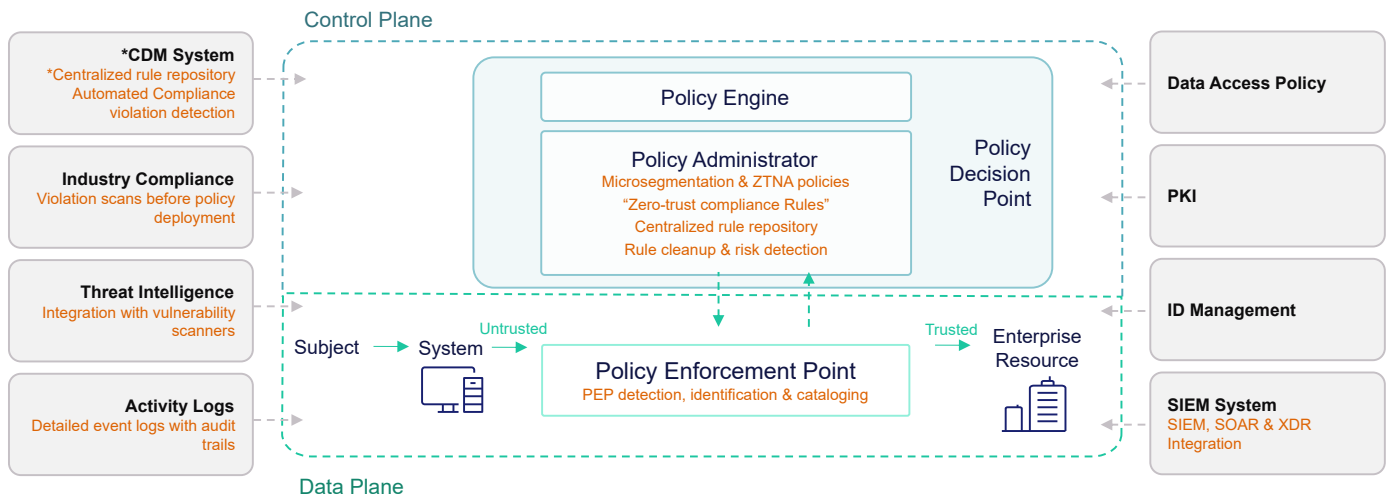
## Improve Security Operations to Support Core Zero Trust Tenets

Policy management sits at the heart of zero trust: the ability to visualize, normalize, manage, and monitor rules across the entire network from the datacenter to the cloud. FireMon's platform delivers the necessary scalability, flexibility, and real time visibility to support zero trust.

The old cliché “you can't protect what you can't see” goes even farther under a zero trust paradigm: you also can't protect what you can't manage. Security policy management from FireMon allows security teams to create and enforce consistent policies across complex networks spanning from the datacenter to the cloud, with the flexibility to adapt to the constantly-evolving nature of a zero trust approach.

## Mapping FireMon to the NIST 800-207 Logical Components

Component	NIST Description (Abridged)	NSPM Offers	Only from FireMon
<b>Policy administrator</b>	Responsible for establishing and/or shutting down the communication path between a subject and a resource. It would generate any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. It is closely tied to the PE and relies on its decision to ultimately allow or deny a session. If the session is authorized and the request authenticated, the PA configures the PEP to allow the session to start. If the session is denied (or a previous approval is countermanded), the PA signals to the PEP to shut down the connection. Some implementations may treat the PE and PA as a single service; here, it is divided into its two logical components. The PA communicates with the PEP when creating the communication path.	NSPM is a central repository for all policy rules across all vendors throughout the entire environment; although NSPM does not directly control PEPs or policy engines, it is a critical element in ensuring policies are consistent and secure.	Highly-scalable policy management across complex, multi-vendor enterprise environments; custom "zero-trust compliance" rules for network security policies; finely-tuned global microsegmentation and ZTNA policies; clean reused, redundant and overly-permissive access policies to close security gaps
<b>Policy enforcement point</b>	Responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and/or receive policy updates from the PA. This is a single logical component in ZTA but may be broken into two different components: the client (e.g., agent on a laptop) and resource side (e.g., gateway component in front of resource that controls access) or a single portal component that acts as a gatekeeper for communication paths. Beyond the PEP is the trust zone (see Section 2) hosting the enterprise resource.	NSPM provides policy management and distribution across all PEPs.	Detection, identification and cataloging of all PEPs across the entire environment (on-premises, cloud, and hybrid environments including SASE, SDN, NFV, FWaaS, and SD-WAN
<b>Continuous diagnostics and mitigation (CDM) system</b>	This gathers information about the enterprise asset's current state and applies updates to configuration and software components. An enterprise CDM system provides the policy engine with the information about the asset making an access request, such as whether it is running the appropriate patched operating system (OS), the integrity of enterprise-approved software components or presence of non-approved components and whether the asset has any known vulnerabilities. CDM systems are also responsible for identifying and potentially enforcing a subset of policies on non-enterprise devices active on enterprise infrastructure.	Real-time automated detection and response for compliance violations, high-risk events, misconfigurations, and policy changes	Thorough access path analysis to discover and mitigate vulnerabilities/leaks; attack simulations to uncover network security policy weaknesses
<b>Industry compliance system</b>	This ensures that the enterprise remains compliant with any regulatory regime that it may fall under (e.g., FISMA, healthcare or financial industry information security requirements). This includes all the policy rules that an enterprise develops to ensure compliance.	Automatic compliance violation detection and mitigation; compliance violation detection as part of workflows before policies are deployed	Real-time detection and alerts; continuous compliance
<b>Threat intelligence feed(s)</b>	This provides information from internal or external sources that help the policy engine make access decisions. These could be multiple services that take data from internal and/or multiple external sources and provide information about newly discovered attacks or vulnerabilities. This also includes newly discovered flaws in software, newly identified malware, and reported attacks to other assets that the policy engine will want to deny access to from enterprise assets.	Integrated with threat feeds to detect known policy-related vulnerabilities	Integration with Qualys, Rapid7, and Tenable
<b>Network and system activity logs</b>	This enterprise system aggregates asset logs, network traffic, resource access actions, and other events that provide real-time (or near-real-time) feedback on the security posture of enterprise information systems.	Detailed policy-related event logging with audit trails	Expandable log history based on available storage
<b>SIEM system</b>	This collects security-centric information for later analysis. This data is then used to refine policies and warn of possible attacks against enterprise assets.	Event detection and response integration with SIEM, SOAR, and XDR systems	Open APIs enable custom integrations with SIEM platforms for visibility and control



\* NIST Core Components

\* How FireMon Supports NIST

Figure 2: FireMon Security Policy Management supports a broad range of core zero trust logical components.

## See the Whole Picture: Comprehensive Real-Time Visibility

Knowing your network is critical to zero trust. NIST's ZTA requires an always-up-to-date view of the IP address space in use, layer 3 (L3) forwarders and policy enforcement points (PEPs), routed path topology, and subnets. But most tradecraft "discovery" falls short of this definition, as it is often focused solely on endpoint assets.

FireMon gives visibility to security teams in a variety of ways. At a fundamental level, FireMon provides both rule usage analysis and network traffic flow analysis, giving administrators granular detail about which assets are communicating with which, via which services, down to individual IP addresses. And this is key: for many organizations, the IP address remains the single most reliable source of identity truth in the network. In terms of network security rules, zero trust often requires the replacement of a single relatively-broad rule with a series of very granular rules applying to specific devices in specific contexts: FireMon provides all the data and the fine controls needed to achieve this.

And FireMon's Lumeta takes that visibility a step further, and gives organizations a comprehensive view of their networks: even what they don't know about. Everything from physical, cloud, virtual, and software-defined network infrastructure and endpoints to operational technology and internet of things (OT/IoT). It starts with an examination of the forwarders and routes in the network and assumes that any target address space provisioned is simply the beginning.

Lumeta provides an accurate view of the infrastructure based on the actual L3 topology and forwarders. This leads to a thorough view of the address space, a complete endpoint census and, crucially, the location (subnet, switch-port, nearest gateway/router, firewall, and potentially geo-location) of those endpoints on the network. These insights into network traffic data and the current state of enterprise assets are important characteristics in any ZTA by NIST standards.

## Tame Complexity and Improve Security Hygiene: Risk and Security Policy Management

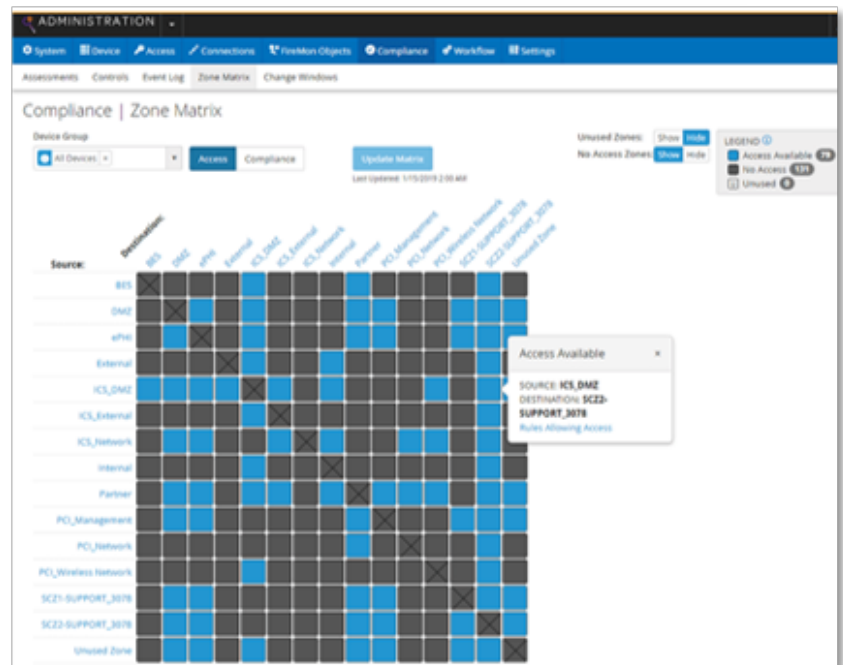
Policy management and decision-making are essential aspects of a ZTA. Since no access request should be implicitly trusted more than any other, the ability to construct, manage, and maintain compliance with compound policies is critical. Increasingly, policy management and the access-engine are control-plane services handled separately from the PEP functions (including firewalls and cloud security groups) that remain within the data-plane. As most organizations need to maintain these policies across complex, hybrid multi-vendor environments, manual policy management is untenable.

And at an even more fundamental level, ensuring that security policies meet requirements without being overly-broad is absolutely critical. Enterprises must proactively manage the entire rule lifecycle, from design to implementation to review to decertification. Rules allowed to outlive their utility open forgotten attack vectors. Rules implemented without fully analyzing their impact can create new ones.

FireMon Security Manager is the industry-defining solution: we created the NSPM market. It normalizes policy content across environments containing multiple firewall vendors, cloud security groups, and SD-WAN and SASE offerings. This capability allows the tenets of zero trust to be actualized in the organization among policy engine, policy administrator, and policy enforcement point components, all while facilitating the acute policy management necessary to maintain zero trust operations.

Normalization of policies across a complex environment allows security architects to have a unified view, enabling near real-time audits and assurance that the policy infrastructure is secure and compliant. As the number and variety of PEPs increase within ZTA microsegmentation zones, the ability of the policy administrator to automatically establish and shut down communication sessions is essential.

Finally, FireMon combines the comprehensive knowledge of the organization's security policies with vulnerability data from industry-leading scanners such as Qualys and Rapid7 to identify high-risk assets as well as the potential access paths attackers could use to reach them. Security and network teams can see vulnerabilities and remediate them (even simulate change effects to help prioritize patching) before they're exploited.



*Figure 3: The unified view of policy in FireMon Security Manager facilitates elimination of overly-permissive, redundant, or unused policies across a complex multi-vendor ZTA environment without resorting to “swivel-chair” management—accessing each vendor management console to implement changes.*

## Simplify Processes: Workflow and Policy Automation

The journey to a ZTA requires automating the policy design, planning, and change approval process. Proliferation and scaling of policy decisions within enforcement points contained in various vendor offerings drive the need for automation to be deployed within the context of a ZTA. The sheer volume of security policies required to maintain zero trust workflows makes manual management incredibly risky at best, and impossible at worst.

This workflow is often facilitated via API integration into an IT Service Management (ITSM) process such as ServiceNow. As the number of security controls increases within a micro-segmented network, FireMon Automation pushes security policy into all policy enforcement points. The capability to automate ZTA security policies from design to decommissioning frees up security teams for more intensive, mission-critical tasks. Change management across the entire environment is orchestrated from a single FireMon user experience.

A next step along the ZTA journey with FireMon automation may be to improve security team efficiency through integrated threat and vulnerability management. Using a rich set of RESTful APIs, FireMon Automation integrates with SOAR and XDR solutions to provide another layer of security against malicious activity.

## Conclusion

Moving toward a zero trust architecture is not as daunting as it may first appear. There are concrete steps that organizations may take with existing infrastructure that can help both harden security and fulfil core zero trust tenets. Focusing on the fundamentals is key: shoring up security hygiene, tightening policy management, and ensuring network visibility in breadth and depth.

While building a pure zero trust architecture from the ground up overnight is often unrealistic, organizations can quickly improve their visibility, manage their policies, and automate their policy workflows with NSPM from FireMon as they migrate their perimeter-based workflows to ZTA.

The road to zero trust is long, but the journey is worth the effort in the long run. With each step along the path, security is hardened, visibility is improved, and compliance is streamlined. And the first step to zero trust is by improving fundamental security operations with FireMon.

### Further Reading: Key resources on zero trust architecture, planning, implementation, and operation.

#### **NIST SP 800-207**

<https://doi.org/10.6028/NIST.SP.800-207>

#### **CISA Zero Trust Security Model** (Draft)

[https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model\\_Draft.pdf](https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf)

#### **Planning for a Zero Trust Architecture – NIST White Paper** (Draft)

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf>

#### **DoD Zero Trust Reference Architecture**

[https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT\\_RA\\_v1.1\(U\)\\_Mar21.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf)

#### **OMB – Federal Zero Trust Strategy**

<https://zerotruster.cyber.gov/federal-zero-trust-strategy/>

## FIREMON

FireMon is the only real-time security policy management solution built for multi-vendor hybrid enterprise environments. FireMon provides policy automation for the latest network security technologies, helping organizations achieve continuous compliance while minimizing firewall policy-related risk. Only FireMon delivers complete visibility and control across an organization's entire IT landscape [www.firemon.com](http://www.firemon.com)