



**FORTINET<sup>®</sup>**



# FortiAnalyzer & Fortimanager

Max Zeumer

Products & Solutions Marketing



# Maximize Posture with FortiAnalyzer

Easy to scale and accelerate growth to all levels of maturity



Stop Advanced Threats with FortiAnalyzers Deep Integration Across The Fortinet Security Fabric

# What is FortiAnalyzer?

Security Fabric Log management, analytics and reporting



## Solution: FortiAnalyzer

- ✓ End to end security management + security loggings with real time detection/analytics
- ✓ Single platform for IT, NOC & SOC visibility
- ✓ Advanced Threat Protection with Security Fabric Automation capabilities

 SOC and NOC teams can use FortiAnalyzer for IOC, event handling and reporting

# FortiAnalyzers Key Capabilities



# FortiAnalyzer Use Cases Overview

Consolidated Security Fabric analytics, single-pane-of-glass visibility and high value automation across the portfolio



FortiAnalyzer

## Security Fabric Analytics

Simplify Visibility Across the Security Fabric,  
Strategically Consolidating Operations



Improve Single Pane Visibility

## Automated Compliance

Compliance Leveraging Security Rating



Reduce Complexities

## Advanced Threat Detection

Detect Network & Security Anomalies in Real-  
Time Reducing MTTD



Improve SOC Effectiveness

## Security Automation

Automation for faster operations, maximizing  
existing staff and SOC augmentation

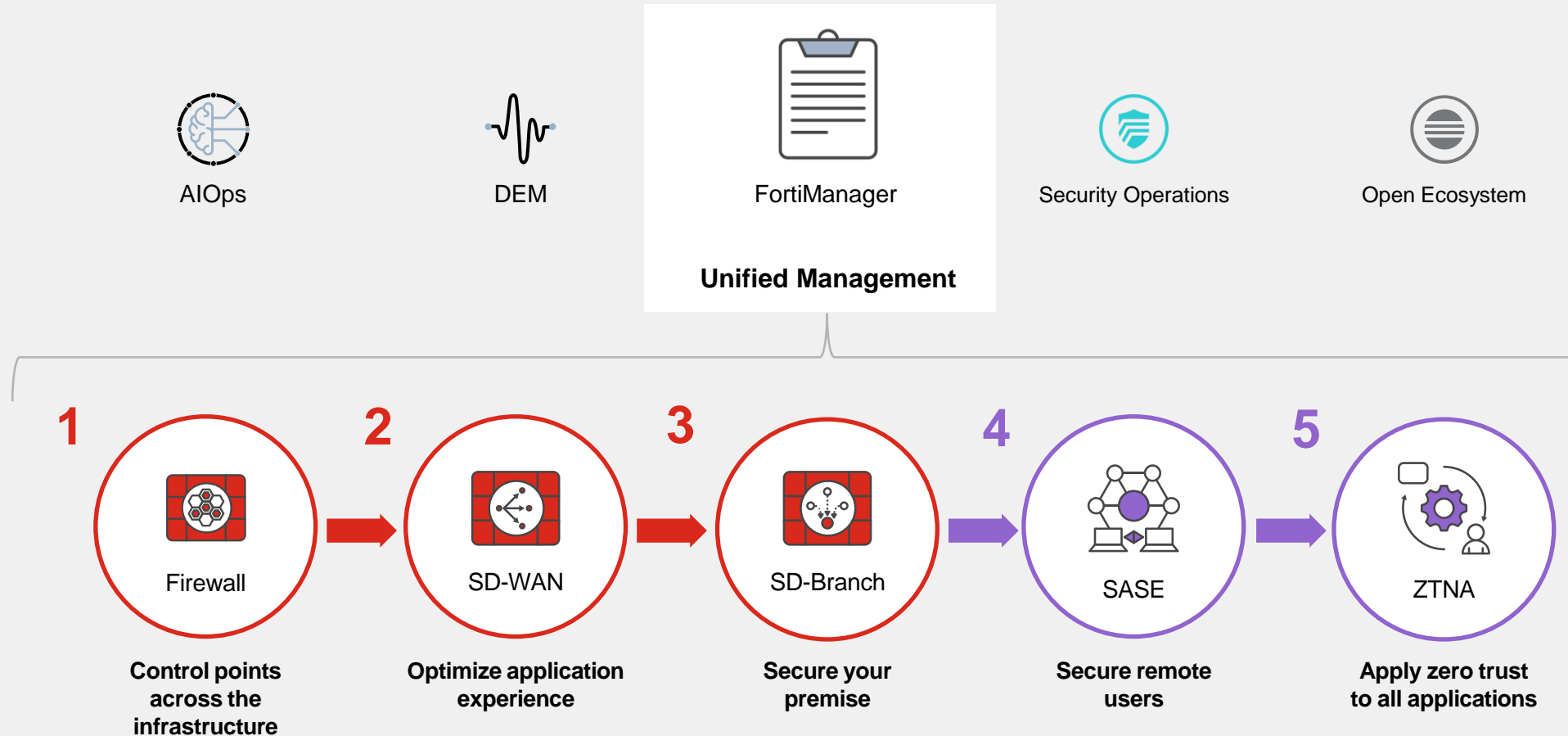


Accelerate L1-L3 Maturity



# FortiManager Powers the Secure Networking Journey

- One platform, one network, one security, one unified management, one journey



## Automation-Driven Management of Fortinet Security Fabric At Scale



# What does FortiManager do?



## Streamline workflows

Mass provisioning and security policy management



## Ongoing Monitoring

Real-Time visibility and analytics of the entire network



## Automation and Orchestration

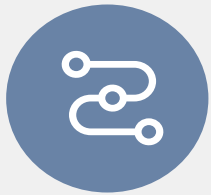
Network Orchestration via ecosystem integrations

✓ **Single-Pane Visibility**

✓ **Network Security**

✓ **Operational Efficiency**





# Streamline Workflows

Granular & secure administration  
(RBAC & ADOM)



Real-time security updates, analytics and insights from integrated SoC



FortiManager

Unified Policy

Config changes and backups

Template

ZTP

Centrally Manage the entire network



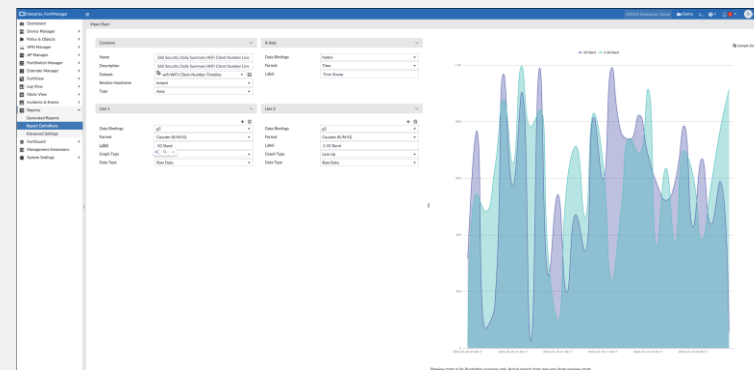
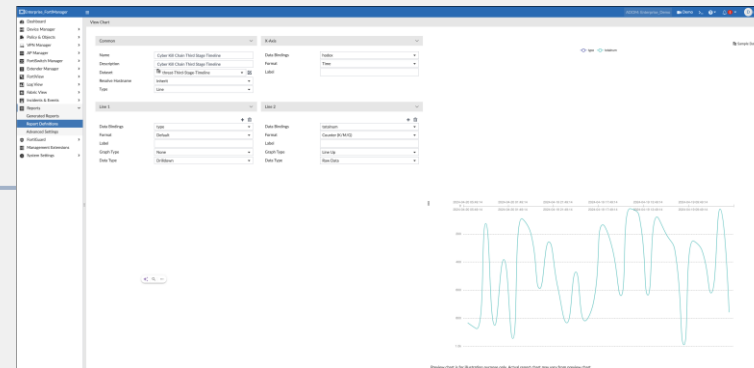
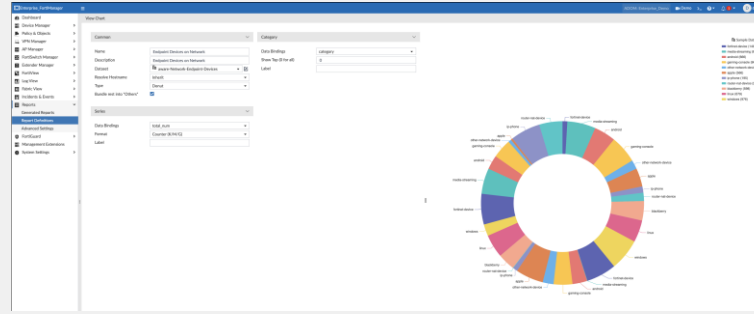




# Ongoing Monitoring for Real-Time Insights



FortiManager



**Audit Logging with customizable templates**  
NoC/SoC Reporting (performance, event and usage)

**Security Posture**  
Identify configuration weaknesses and best practice violations in your deployment.

-499.60  
-1615.13 (-144.79%) Since 4 hours ago

**B**

- Audit Logging & Monitoring
- Endpoint Management
- Fabric Security Hardening
- Firmware & Subscriptions
- Network Design & Policies
- FortiGuard Outbreak Detection
- Threat & Vulnerability Management

**Fabric Coverage**  
Identify in your overall network, where Security Fabric can enhance visibility and control.

450.10  
0.00 (0.00%) Since 4 hours ago

**B**

- Audit Logging & Monitoring
- Firmware & Subscriptions
- Network Design & Policies
- Threat & Vulnerability Management

**Optimization**  
Optimize your fabric deployment.

-437.61  
0.00 (0.00%) Since 4 hours ago

**C**

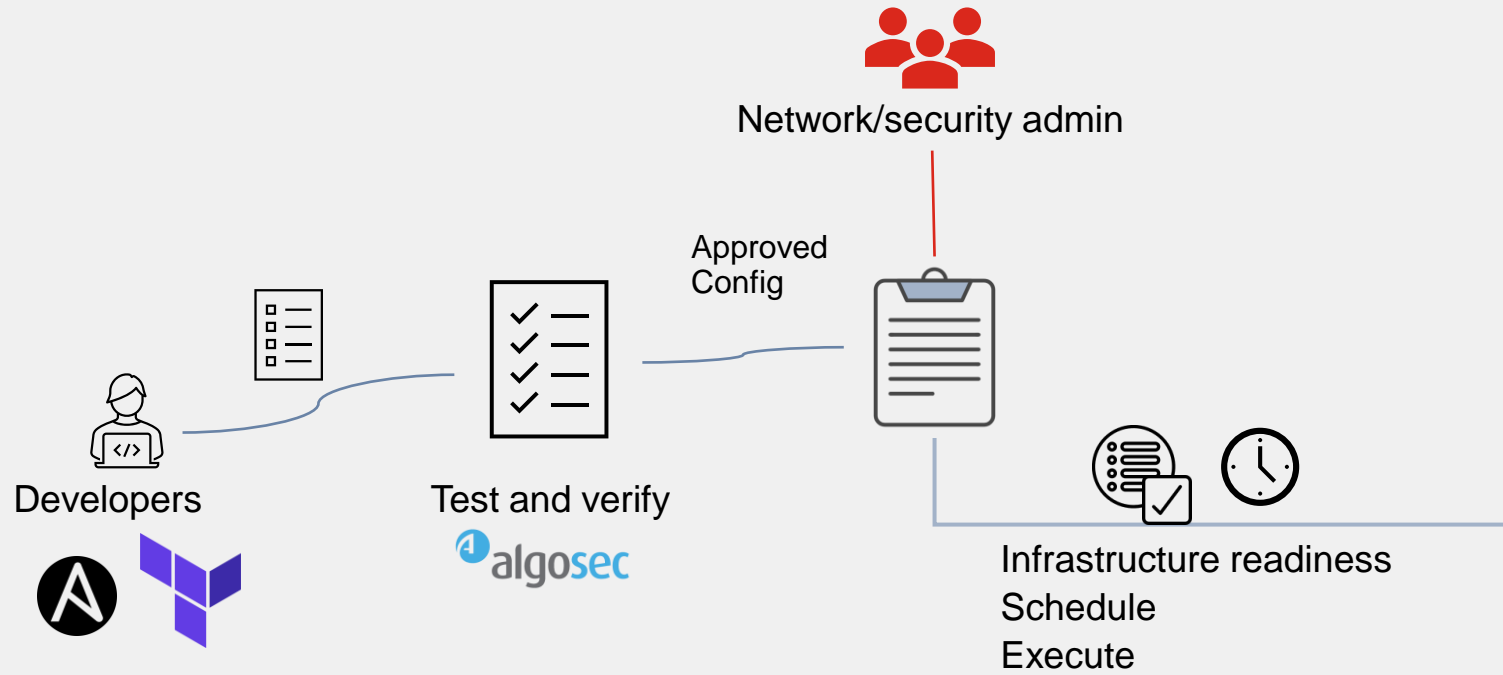
- Firmware & Subscriptions
- Network Design & Policies
- Performance Optimization

**Compliance Reports and Security Rating**





# Automation and Orchestration



Firewalls, SD-WAN, SD-Branch and more

Continuous delivery of changes and backups

Category	Change Summary	User
IPsec Policy	added (1)	admin (Details)
Policy Object - added (5) changed (3) deleted (106) (Details)		
Category	Change Summary	User
CA Certificate	added (1)	admin
Local User	deleted (1)	admin
User Group	deleted (1)	admin
Device Group	deleted (1)	admin
Local Category	added (1)	admin
Web Filter Profile	changed (1) deleted (6)	admin
Address	added (1) changed (1) deleted (1)	admin
MultiCast Address	deleted (1)	admin
IPv6 Address	deleted (1)	admin

Track historical changes



# FortiManager in Your Automation Journey

Day 0

Day 1

Day N



## PLAN & DESIGN

- Templates
- ADOMs



## IMPLEMENTATION

- FortiZTP
- Software, Config and Policy Changes
- Compliance Check
- Security Update Distribution
- Scripting and External Connectors.



## MONITOR & OPTIMIZE

- In-depth Analytics via FortiAnalyzer
- Real-time Alert Generation
- Event Response via Pre-Defined Workflows
- Automation Stitches
- API Integration with 3rd Party Tools.

