FortiPolicy delivers comprehensive and consistent controls to protect on-premises data centers, OT environments, their applications, as well as their data. It leverages agentless machine-learning (ML) technology, and through the Fortinet Security Fabric, enforces intention with a set of comprehensive controls including micro-segmentation, firewalling, and more.

This powerful, agentless, ML platform enhances the micro-segmentation and intent-based networking segmentation capabilities of the Security Fabric. It enables end-to-end visibility and connection-mapping of north-south and east-west traffic flows. FortiPolicy then applies ML to provide context to these workflows, enabling it to suggest security policies to the Security Fabric.

Data-center administrators are then able to learn relationships among workloads and applications and make decisions to allow or block that communication. These machine-learning enabled policies can be automated, which reduces complexity and improves efficiency in their implementation. This process of discovery, security, and automation offers a truly adaptive solution to protect your most sensitive assets. FortiPolicy then applies ML to provide context to these workflows, enabling it to suggest security policies to the Security Fabric for on-premises data centers and OT environments.

**Business Outcomes**

- **Improve network visibility**
  - Inspect all network traffic for malicious activity
  - Prevent or limit the damage of data breaches
  - Limit the pain of vulnerability management
- **Prevent malware propagation between critical systems**
  - Prevent lateral movement of malicious threats through micro segmentation
  - Limit the "blast radius" of a breach to the segment that gets compromised, trapping it within the initial attack surface
- **Improve perimeter security**
  - Protect workloads and applications from attacks and unauthorized access
- **Reduce the scope and cost of compliance initiatives**
  - Cordon off environments that hold specific, sensitive data and then apply the exact security measures you need to that area to maintain compliance
  - Reduce the scope of industry regulations
  - Ease the pain of compliance audits
- **Enable digital acceleration**
  - Provide automated security controls and application-level micro segmentation to enable new services to be rapidly deployed with security controls in place, decreasing the risk to business
FEATURE HIGHLIGHTS

Continuous Discovery and Machine Learning

Limited visibility of east-west traffic is often exploited by bad actors looking to gain access to sensitive data. To give IT administrators insight into critical resources and services where visibility is traditionally at its lowest, FortiPolicy observes, learns, and analyzes traffic and workflows between hosts—without installing an agent. It enables multi-tier application discovery and mapping so administrators understand how data is being accessed.

The speed and complexity of multi-tiered applications makes it difficult to determine the nature of workflows in the data center. With FortiPolicy, the broad visibility gathered through continuous discovery is coupled with ML to learn relationships among workloads and applications. This provides context that helps administrators to more effectively monitor workloads and connectivity. Discovery and analysis is ongoing, enabling administrators to map their environments in detail and in real time to understand normal verses abnormal patterns.

Dashboard - Critical Information at a Glance

- Simplified view of multi-tiered web applications
- Lateral movement detection
- Exploit control
- Malware control
- Malicious web filtering
- Lateral movement detection
- Built-in risk analysis
- Attacks detection
FEATURE HIGHLIGHTS

Security Fabric Integration
Integration into the Fortinet Security Fabric enables FortiPolicy to both gather and share information to develop and enforce more effective security in your on-premises data center environment. The Security Fabric enforces security through the FortiGate and FortiSwitch, expanding the security mesh to cover OT environments as well as the data center and the applications and workloads within. With the integration of FortiPolicy into the Security Fabric, information is shared and administrators are able to implement more robust perimeter security to protect workloads and applications from unauthorized access.

Security policies are able to extend beyond traditional north-south network segmentation and provide control and visibility for east-west traffic within a segment between workloads. This east-west visibility and control is key to prevent the lateral movement of threats within the network and data center.

Automation and Real Time Response
By utilizing visibility, ML, context, and Security Fabric integration, FortiPolicy is able to automate the creation of security policies, which significantly improves management efficiency. These security policies are created in real time as workflow relationships are discovered and anomalies detected. Administrators can review and approve policies before they are enforced by the Security Fabric.

Machine Learning and Environment Mapping
- Learns and indicates the relationships among workloads and applications
- Automates micro segmentation policy recommendations
- Policy automation applies security for east-west traffic with FortiGate and FortiSwitch in the data center, without network segmentation
- Enables visibility of multi-tier applications and user control of workloads

Machine Learning Segmentation
- Automated policy recommendation to the Security Fabric FortiOS and FortiSwitch for east-west traffic
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad**: Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated**: Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated**: Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.

FORTINET SERVICES

24/7 FortiCare™ Service

24x7 FortiCare technical support is delivered through our Global Technical Assistance Centers. Each geographical region has a Center of Expertise supplemented by regional support centers. This structure enables us to provide regional and local language support. Foundational FortiCare device-level support includes the following.

- Global toll-free numbers that are available 24x7
- Web chat for quick answers
- A support portal for ticket creation or to manage assets and life cycles
- Access to software updates and a standard next-business-day RMA service for the device

ORDER INFORMATION

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>SKU</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiPolicy is delivered as a virtual machine</td>
<td>FC1-10-PLVM1-527-01-DD</td>
<td>FortiPolicy VM Subscription license with FortiCare Premium Support for on-premise Micro-segmentation of 100 Workloads.</td>
</tr>
<tr>
<td></td>
<td>FC2-10-PLVM1-527-01-DD</td>
<td>FortiPolicy VM Subscription license with FortiCare Premium Support for on-premise Micro-segmentation of 500 Workloads.</td>
</tr>
<tr>
<td></td>
<td>FC3-10-PLVM1-527-01-DD</td>
<td>FortiPolicy VM Subscription license with FortiCare Premium Support for on-premise Micro-segmentation of 2500 Workloads.</td>
</tr>
</tbody>
</table>

www.fortinet.com

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet products and services to engage in, or support in any way, violations or abuses of human rights, including those involving censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA (https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf) and report any suspected violations of the EULA via the Fortinet Whistleblower Policy (https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf).