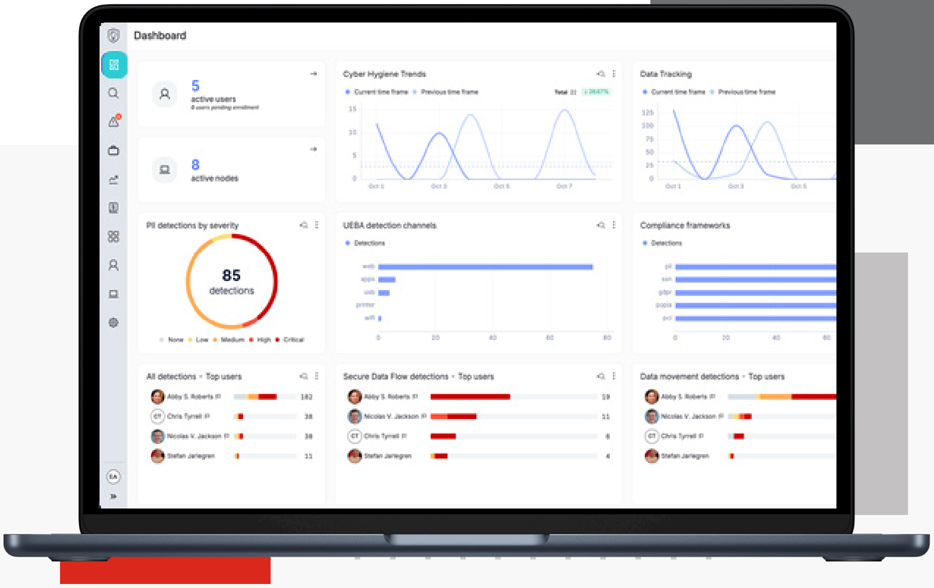
FortiDLP

Next Generation DLP Enhanced by AI



Key Use Cases

- Prevent data loss from exfiltration and accidental loss
- Monitor for insider threats and high-risk employees
- Secure data in use by SaaS and other applications
- Apply user and entity behavioral analysis at scale
- Educate users on proper data handling
- Identify Shadow AI usage and stop the upload of sensitive data
- Automatically maps detections to MITRE Engenuity™ Insider Threat TTP Knowledge Base

Next Generation DLP and Insider Risk Management Solution Anticipates and Prevents Data Theft

Overview: securing your cloud environments

Today's most valuable currency is data. Whether it's intellectual property, strategic plans, financial account details, patient records, or customer cardholder information, data is the lifeblood of digital organizations. It must always be protected from theft or exposure by threat actors, malicious insiders, and careless or untrained employees.

FortiDLP is a next-generation, AI-enhanced, cloud-native endpoint data protection solution that helps your security team anticipate and prevent data leaks, detect behavior-related insider risks, and train employees on proper cyber hygiene at the point of access to sensitive data including intellectual property—starting from day one. With FortiDLP, your organization can not only prevent data loss but also gain immediate visibility into data, derive insights into business data flows, detect high-risk activity across all users, endpoints and cloud drives, and drive prioritized investigations.

Challenges: traditional DLP fails to deliver in today's world

Legacy DLP tools address modern data security challenges with cumbersome data classification and complex static policies before offering any visibility into your organization's data loss risks or controls to mitigate them. As a result, data security teams are overburdened by constant policy creation, inefficient data classification, false positives, and noisy alarms.

FortiDLP overcomes these legacy DLP challenges, by combining machine learning algorithms integrated into FortiDLP's lightweight agent and localized real-time context and content inspection to deliver data protection across all data egress points on managed and unmanaged devices.

Available in

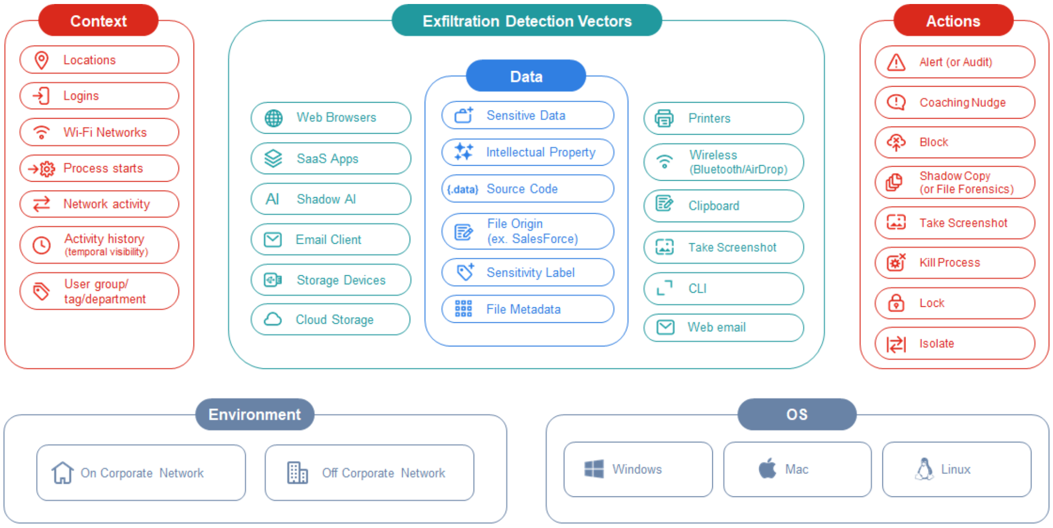
Cloud

Our Approach

A data-driven solution

FortiDLP applies a modern and unified approach to data protection, combining Data Loss Prevention, Insider Risk Management, SaaS Data Security, Behavioral Analytics, and Risk-Informed User Education.

FortiDLP provides immediate visibility into data movement and activity across devices and collaboration platforms, empowering organizations to assess risk and enforce DLP and Insider Risk policies with proactive data security actions in real time.



FortiDLP's scalable, lightweight agent collects and records data regardless of network connection and location, meaning you get full protection of your employees' data flows whether they're in the office, working remotely, or on the road. This delivers data protection that doesn't rely on sending your critical business data to a cloud-based file scanning engine, reduces bandwidth costs and addresses data residency requirements.

Track Data From Its Origin

Through Secure Data Flow, FortiDLP can also automatically identify and track data based on its origin, such as Workday or a source code repository. DLP and insider risk policies can be enforced based on where the data originated and whether a corporate or non-corporate account was used to egress data.

Enhanced with Artificial Intelligence

From day one, FortiDLP applies machine learning—integrated into FortiDLP's agent—to baseline individual user activity and uses behavioral analytics algorithms to detect typical versus novel or anomalous behavior. Additional powerful analysis and analytics capabilities provide insights at an organizational level.

In addition, FortiDLP utilizes FortiAI (AI Assistant) to summarize and contextualize data associated with high-risk activity to accelerate incident analysis. Activities are mapped to MITRE ENGENUITY™ Insider Threat Tactics, Techniques, and Procedures (TTP) Knowledge Base.

Highlights

Addresses Key Compliance Controls Involving Data Security and Awareness

FortiDLP enables teams to adopt a proactive stance in meeting key compliance requirements, including PCI DSS, HIPAA, ISO 27001, NIST, and others, to prevent the egress of sensitive data by providing deep visibility into user activities, data access, and systems. In addition, FortiDLP raises awareness of security hygiene through user education at the point of data access.

Prioritizing privacy, especially under regulations like GDPR and CCPA, FortiDLP leverages built-in data minimization techniques—such as pseudonymization and localized forensics storage—to help security teams detect and mitigate threats while safeguarding employee confidentiality.

FortiDLP

- Integrates Data Loss Prevention, Insider Risk Management, SaaS Data Security, Behavioral Analytics, and Risk-Informed User Education in a single solution
- Is cloud-native, allowing organizations to turn on services and gain data risk visibility in minutes to protect sensitive data on day one
- Utilizes lightweight agent technology for Windows, macOS and Linux operating systems for seamless deployment and automated updating at enterprise scale
- Detects and responds to data manipulation and anomalous activity using AI and ML
- Monitors SaaS application usage, including Shadow AI tools like Gen-AI, while incorporating risk-informed user education at the point of access to sensitive data
- Provides administrators with a fully featured, always up-to-date management console and behavior analytics system to monitor, report and enable automated actions
- Delivers immediate policy-free visibility into data movement and business processes
- Accurately detects Intellectual Property and sensitive data using advanced data classification, data origin and identity-based data tracking (Secure Data Flow)
- Addresses regulatory compliance controls involving data loss prevention with minimal effort using templated PII/PHI/PCI policies
- Applies a Privacy-first approach to data protection by: 1) Storing forensics logs at customer-controlled in-region data centers, 2) Minimizing pseudonymized investigation data sets and, 3) Including out-of-the-box investigation authorization workflows for analysts

Supported Operating Systems

Windows	Windows 10 and Windows 11 Windows Server 2012 R2+
MacOS	OS 10.14 Mojave+
Linux	Red Hat Enterprise Linux 7+ CentOS 7+ Ubuntu 16.04 LTS & 17.10+ Debian 8+

Google Workspace

Microsoft 365

Cloud Drive Connectors

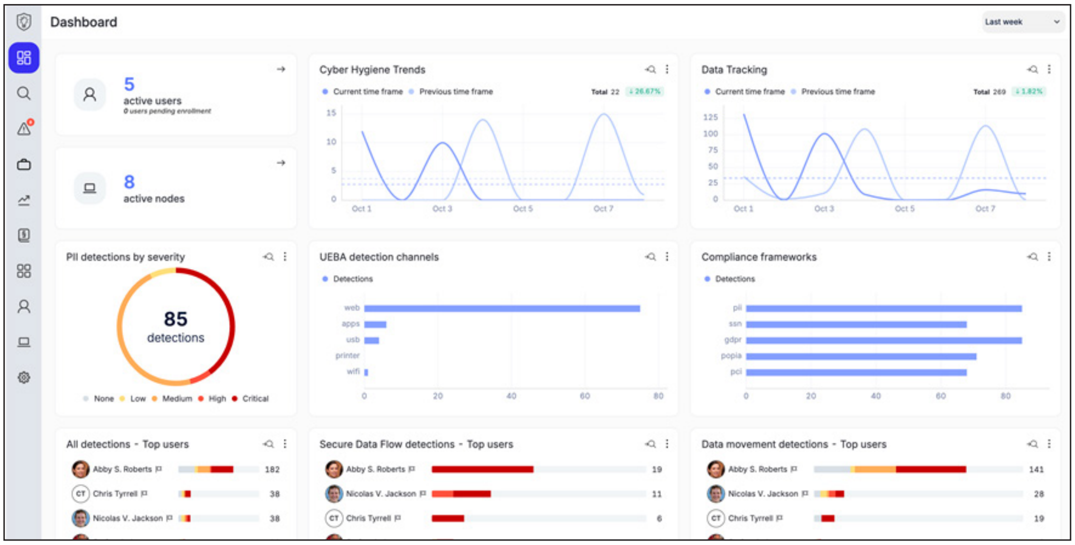
Integrations

FortiDLP provides MDM profiles, event steaming, webhooks, and an open API for integration with your existing MDM, SIEM, SOAR, automation, and service desk tools.

Use Cases

Data Loss Prevention

FortiDLP provides rich out-of-the-box data visibility, risk assessment, and data protection policies to protect critical information assets on and off the network. FortiDLP analyzes what and how data is being used, and allows you to determine how to best respond.



FortiDLP doesn’t require pre-built policies. FortiDLP classifies and tracks data in real time for immediate visibility and data protection. Whether your business or other organization relies on structured or unstructured data, FortiDLP can track, and take active steps to protect it all.

FortiDLP agents, browser extensions, and cloud connectors automatically collect, enrich, and index activity across event types (e.g. authentication, web, email, applications, USB, file creation, sharing and download activity).

This data set is then used to:

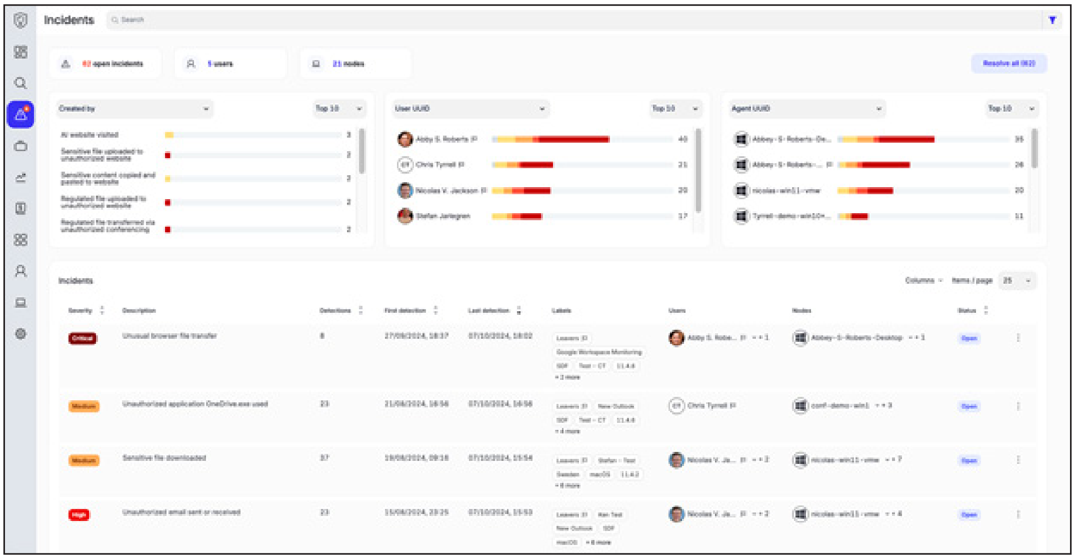
- Highlight and report on data movement and exposure risk
- Create data protection policies
- Provide analysts with a rich activity data set to support investigations

Unlike legacy DLP’s static policies and binary “block” OR “allow,” FortiDLP’s risk-adaptive policies consider risk factors and let you decide which actions to take, such as notifying users via Microsoft Teams or Slack, capturing file and screen forensics, isolating or locking an endpoint, killing a process, or blocking high-risk activity.

Features

Insider Risk Management

FortiDLP tracks and traces sensitive information flows and user interactions within the organization. It identifies and mitigates insider threats through advanced user behavior analytics, automatically blocking suspicious activities.



Created by	
AI website visited	3
Sensitive file uploaded to unauthorized website	2
Sensitive content copied and pasted to website	2
Regulated file uploaded to unauthorized website	2
Regulated file transferred via unauthorized conferencing	2

User UUID	
Abby S. Roberts	40
Chris Tyrrell	21
Nicolas V. Jackson	20
Stefan Jarlegren	17

Agent UUID	
Abbey-S-Roberts-De...	35
Abbey-S-Roberts-...	26
nicolas-win11-vmw	20
Tyrell-demo-win10-...	11

Incidents

Severity	Description	Detections	First detection	Last detection	Labels	Users	Nodes	Status
Critical	Unusual browser file transfer	8	27/09/2024, 18:37	07/10/2024, 18:02	Leavers Google Workspace Monitoring SDF Test - CT 11.4.8 + 2 more	Abby S. Robe... + 1	Abbey-S-Roberts-Desktop + 1	Open
Medium	Unauthorized application OneDrive.exe used	23	21/08/2024, 16:56	07/10/2024, 16:56	Leavers New Outlook SDF Test - CT 11.4.8 + 4 more	Chris Tyrrell	conf-demo-win1 + 3	Open
Medium	Sensitive file downloaded	37	19/08/2024, 09:18	07/10/2024, 15:54	Leavers Stefan - Test Sweden macOS 11.4.2 + 8 more	Nicolas V. Ja... + 2	nicolas-win11-vmw + 7	Open
High	Unauthorized email sent or received	23	15/08/2024, 23:25	07/10/2024, 15:53	Leavers Ken Test New Outlook SDF macOS + 8 more	Nicolas V. Ja... + 2	nicolas-win11-vmw + 4	Open

FortiDLP's activity feed provides analysts with a comprehensive, streamlined, and time-sequenced view of user, data, and device activity before, after, and during an incident. High-risk activity detections are mapped to MITRE ENGENUITY™ Insider Threat TTP Knowledge Base and automatically sequenced into risk-scored incidents make analysts more effective and efficient by prioritizing investigations.

Depending on the severity of the risk, Security Analysts can prompt an employee with an on-screen message, take a screenshot of a user's computer screen, kill a process, kill and block connections to a device, or lock a device keyboard and mouse.

Integrated case management and risk reports highlight instances of careless, malicious, and accidental behavior over time, allowing you to assess the effectiveness of your security controls and identify areas for improvement. Reports can also be easily exported to share with leadership.

SaaS Data Protection

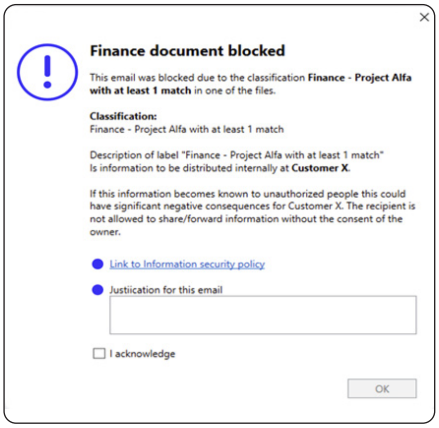
FortiDLP provides comprehensive visibility into user interactions with data in the cloud and maintains protection as data moves out of the cloud. This ensures continuous protection of sensitive information, regardless of its location or access method.

The solution builds a comprehensive risk-scored inventory of SaaS applications and GenAI tools utilized across an organization, with insights into data ingress, egress, and credentials. It also fortifies defenses against potential data breaches stemming from business data exposure via unauthorized app usage, nudging employees to use authorized tools.

Features

Risk-Informed User Education

FortiDLP champions being proactive in risk mitigation, making employees part of the organization’s security posture and enabling a more resilient security culture. Customized prompts and nudge notifications reinforce security policy awareness and can direct users to acceptable alternatives when unauthorized apps are detected. Notifications can be sent via endpoint dialogue, email, Microsoft Teams, and Slack messaging systems.



Finance document blocked

This email was blocked due to the classification **Finance - Project Alfa with at least 1 match** in one of the files.

Classification:
Finance - Project Alfa with at least 1 match

Description of label "Finance - Project Alfa with at least 1 match"
Is information to be distributed internally at **Customer X**.

If this information becomes known to unauthorized people this could have significant negative consequences for Customer X. The recipient is not allowed to share/forward information without the consent of the owner.

- Link to Information security policy
- Justiication for this email

□ I acknowledge

With risk-informed training, you can train your employees to make the right decisions based on detection of unacceptable behavior, reinforce corporate security policies, and promote good cyber hygiene.

Pre-built rules detect poor cyber hygiene practices, such as employees uploading confidential files to unexpected locations, connecting to unsecured Wi-Fi networks, inserting malicious hardware devices, or using unsanctioned applications for cloud or USB storage.

FortiDLP provides constant enforcement without exception–whether employees are remote or working offline. Enforcing employee adherence to corporate policies such as Acceptable Use Policy (AUP), Information Security Policy (ISP) and more.

Shadow AI

FortiDLP enables the safe use by employees of publicly available generative-AI tools such as OpenAI’s ChatGPT, Google’s Gemini and other AI tools. Administrators can set policy actions to alert on proper data handling practices while allowing employees to continue using these tools. The result is a balance between enabling greater productivity while securing the organization against the sharing of sensitive data with these tools.

Features

Scalable, Lightweight Agent—Minimize the Impact of Processes

FortiDLP's unique technology inspects content and data in movement, lowering the CPU and memory impact on your employees' computers. As a cloud-native solution, FortiDLP scales to your organization's needs regardless of size.

Context and Content Analysis—Perform Real-time Inspection

FortiDLP solution applies AI-enhanced functionality to perform both contextualized analysis and real-time content-level inspection (at the time of access) to determine if data is sensitive, how it needs to be protected, and perform automated actions based on policies.

Expansive Policy Actions—Take Action That Best Suits Circumstances

Unlike legacy DLP's binary "block" or "allow" policy actions, with FortiDLP you can respond as your business demands. FortiDLP's adaptive controls let you decide what actions to take such as logging, isolating an endpoint, or blocking actions.

Insider Risk Sequence Detection—Sequence High-Risk Attack Campaigns

FortiDLP automatically identifies, sequences, and scores high-risk activity chains. This capability enables analysts to prioritize their investigation time and move away from manually reviewing thousands of atomic "DLP incidents."

Detections are also automatically mapped using MITRE ENGENUITY™ Insider Threat TTP Knowledge Base.

Secure Data Flow—Track Data's Movement From its Origin

Secure Data Flow revolutionizes data protection by addressing the limitations of traditional DLP solutions. By tracking the "What, Where, Who, and How" of data's origin, movements, and modifications, Secure Data Flow protects data based on its origin and gives analysts performing an investigation the full history of data's journey.

Secure Data Flow automatically identifies and tracks data based on its origin, such as Workday or a source code repository. DLP and insider risk policies can be enforced based on where the data originated and whether a corporate or non-corporate account was used to egress data.

AI Powered Assistant—Accelerate Security Operations and Incident Response

FortiDLP's AI-powered assistant takes security analysts to the next level with streamlined data loss and insider threat analysis. FortiDLP enhances incident analysis by using Generative Pre-trained Transformer technology or GenAI to summarize and contextualize data associated with observed high-risk activity, mapped to MITRE Insider Threat Tactics, Techniques, and Procedures (TTP) Knowledge Base, for easy consumption by analysts and peers. Analysts benefit from optimized workflows, a reduction in time to contain and resolve threats, and the empowerment to contribute to the business at a higher level.

Features (DLP)

FEATURES	STANDARD	ENTERPRISE	MANAGED
DLP			
Integrated Device Control	✓	✓	✓
Inline DLP Web, Email, Cloud Drive, and Connected Media	✓	✓	✓
Real-time Advanced Data Classification	✓	✓	✓
Generative AI and SaaS Applications Risk Analysis	✓	✓	✓
Secure Data Flow	✓	✓	✓
Employee Coaching and Block Actions	✓	✓	✓
Regulatory Compliance Policy Library	✓	✓	✓
Microsoft MIP/AIP Label Support	✓	✓	✓
File Forensics	✓	✓	✓
Incident Management and DLP Activity Timeline	✓	✓	✓
Dynamic Risk Adaptive Policies	✓	✓	✓
Insider Risk			
User and Endpoint Activity Monitoring		✓	✓
Machine Learning-Powered Behavior Analytics		✓	✓
Data Manipulation Detection		✓	✓
Endpoint Isolate and Real-time Lock		✓	✓
Data Lineage Tracking		✓	✓
Risk Scored Sequence Detection Incidents		✓	✓
Forensics Screen Capture		✓	✓
Case Management		✓	✓
MITRE ATT&CK®-mapped Insider Threat Detection Library		✓	✓
SaaS Data Security			
Google Workspace Connector		✓	✓
Microsoft Office 365 Connector		✓	✓
File Sharing Controls		✓	✓
Managed Service			
Product Deployment and Provisioning			✓
Optimize DLP Rules			✓
Update Product Configuration			✓
Deploy New Use Cases			✓
Quarterly Reports			✓

Ordering Information

SOLUTION	DESCRIPTION	NUMBER OF ENDPOINTS	SKU	MOQ
SUBSCRIPTION LICENSES				
Standard-Endpoint DLP	Cloud-native endpoint DLP with FortiCare Premium	50-499	FC2-10-DLPEP-1097-02-DD	200
		500-1999	FC3-10-DLPEP-1097-02-DD	
		2000-9999	FC4-10-DLPEP-1097-02-DD	
		10 000+	FC5-10-DLPEP-1097-02-DD	
Enterprise-Endpoint DLP with Insider Risk and cloud drive integration	Cloud-native endpoint DLP, Insider Risk, and SaaS integration with FortiCare Premium	50-499	FC2-10-DLPEP-1098-02-DD	
		500-1999	FC3-10-DLPEP-1098-02-DD	
		2000-9999	FC4-10-DLPEP-1098-02-DD	
		10 000+	FC5-10-DLPEP-1098-02-DD	
MANAGED SERVICE				
Managed-Enterprise DLP license with managed service	Managed cloud-native Enterprise DLP, Insider Risk, and SaaS integration with FortiCare Premium	50-499	FC2-10-DLPEP-1099-02-DD	200
		500-1999	FC3-10-DLPEP-1099-02-DD	
		2000-9999	FC4-10-DLPEP-1099-02-DD	
		10 000+	FC5-10-DLPEP-1099-02-DD	
FORTICARE BEST PRACTICES CONSULTATION SERVICE				
Forticare Best Practices Consultation Service (BPS)*	Number of endpoints/users	Up to 999	FC1-10-DLBPS-310-02-DD	—
		1000-9999	FC2-10-DLBPS-310-02-DD	
		10 000+	FC3-10-DLBPS-310-02-DD	

* BPS required.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

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's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

www.fortinet.com

November 7, 2024