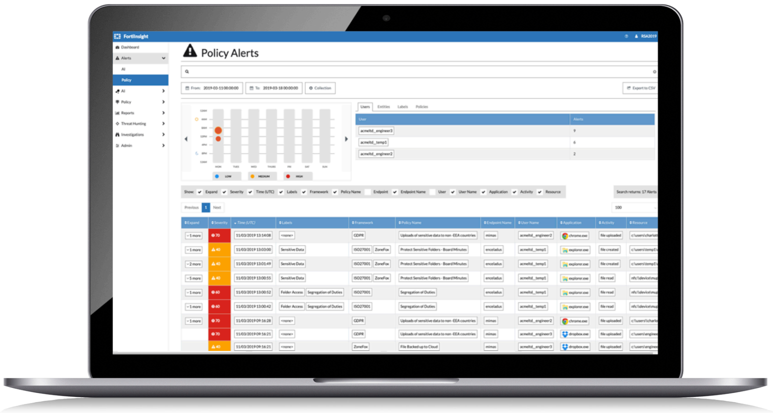
DATA SHEET

FortiInsight™

Cloud

Monitor. Detect. Respond.



Policy Alerts

From: 2019-03-11 00:00:00 | To: 2019-03-18 00:00:00 | Collection | Export to CSV

User	Alerts
acmeltd_engineer3	9
acmeltd_temp1	6
acmeltd_engineer2	2

Show: ✓ Expand ✓ Severity ✓ Time (UTC) ✓ Labels ✓ Framework ✓ Policy Name □ Endpoint ✓ Endpoint Name □ User ✓ User Name ✓ Application ✓ Activity ✓ Resource

Search returns: 17 Alerts

Previous 1 Next — 100

Expand	Severity	Time (UTC)	Labels	Framework	Policy Name	Endpoint Name	User Name	Application	Activity	Resource
1 more	70	11/03/2019 13:14:08	<none>	GDPR	Uploads of sensitive data to non -EEA countries	mimas	acmeltd_engineer2	chrome.exe	file uploaded	c:\users\charlot
1 more	40	11/03/2019 13:03:00	Sensitive Data	ISO27001 ZoneFox	Protect Sensitive Folders - Board Minutes	enceladus	acmeltd_temp1	explorer.exe	file created	c:\users\temp1\
2 more	40	11/03/2019 13:01:49	Sensitive Data	ISO27001 ZoneFox	Protect Sensitive Folders - Board Minutes	enceladus	acmeltd_temp1	explorer.exe	file created	c:\users\temp1\
5 more	40	11/03/2019 13:00:55	Sensitive Data	ISO27001 ZoneFox	Protect Sensitive Folders - Board Minutes	enceladus	acmeltd_temp1	explorer.exe	file read	nfs:\\device\mu
1 more	60	11/03/2019 13:00:52	Folder Access Segregation of Duties	ISO27001	Segregation of Duties	enceladus	acmeltd_temp1	explorer.exe	file read	nfs:\\device\mu
1 more	60	11/03/2019 13:00:42	Folder Access Segregation of Duties	ISO27001	Segregation of Duties	enceladus	acmeltd_temp1	explorer.exe	file read	nfs:\\device\mu
1 more	70	11/03/2019 09:16:28	<none>	GDPR	Uploads of sensitive data to non -EEA countries	mimas	acmeltd_engineer2	chrome.exe	file uploaded	c:\users\charlo
	70	11/03/2019 09:16:21	<none>	GDPR	Uploads of sensitive data to non -EEA countries	mimas	acmeltd_engineer3	dropbox.exe	file uploaded	c:\users\enginee
	40	11/03/2019 09:16:21	<none>	ZoneFox	File Backed up to Cloud	mimas	acmeltd_engineer3	dropbox.exe	file uploaded	c:\users\enginee

FortiInsight is a unique data security and threat detection solution that delivers advanced threat hunting to help you spot, respond to and manage risky behaviors that put your business-critical data at risk. We combine powerful and flexible Machine Learning with detailed forensics around user actions to bring focus to the facts more rapidly than other solutions.

Augmented Intelligence (AI)

Enhanced data visibility with machine learning and User and Entity Behavior Analysis (UEBA). Machine learning optimizes each stage of the investigation pipeline, identifying emerging threats, from compromised accounts to data theft.

Regulatory Compliance Support

Get full visibility of how data is accessed, used, and moved within your organization, and create compliance framework-specific rules, reporting, and analysis to identify, respond to, and manage non-compliant behavior.

Monitoring and Forensic-level Reporting

Monitor data movement and endpoint activity 24/7 regardless of location or whether users are on or off your network. Compile a full forensic history of user behavior, enabling thorough investigation and detailed reporting.

Highlights

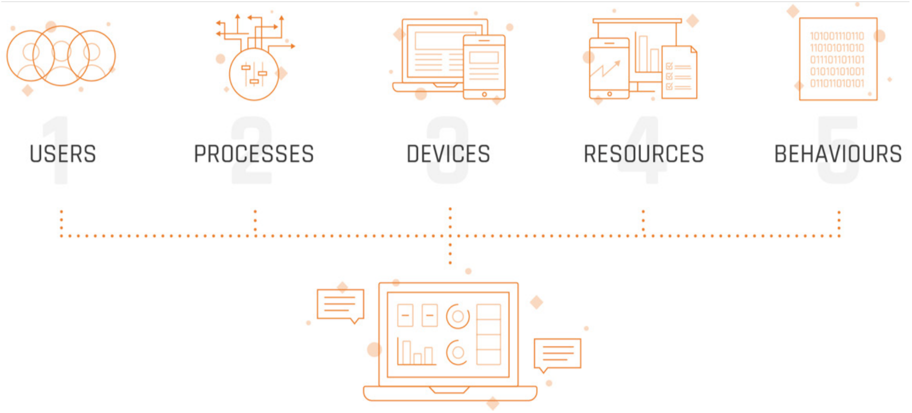
- Endpoint agents result in a very low touch on system resources, with only endpoint meta-data collected.
- Instant insights around your data activities as agents collect data from the moment they are installed.
- Real-time data processing and analysis of user behavior results in rapid incident response capabilities.
- Learns what normal activity is at user, system and network layers to provide complete coverage of your environment and deep forensic capability.
- FortiInsight integrates with FortiSIEM, or your SIEM of choice, via an API that allows you to consume Policy and AI alerts, giving you the capability for the first time to correlate from the perimeter to the centre of your network.

HIGHLIGHTS

Key Features and Operating Information

Our award-winning technology provides complete visibility of activities around your data — the who, what, where and when — by monitoring user behavior and data movement both on and off the network, and instantly alerting to anomalous activities. Security posture is strengthened, sensitive information is protected, and regulatory compliance is supported.

- FortiInsight is a hosted solution.
- Endpoint Agent technology provides visibility on files being moved to or from cloud storage applications, Skype, Instant-Messenger, etc. complete with tracking of file names being moved via encrypted means.
- UEBA, powered by rule sets and augmented with AI, detects known and unknown threats ranging from malicious insider activity to compromised accounts.
- Recording of user, machine, application, file, behavior and network destinations/source activities results in a complete forensic level of detail for investigation and compliance purposes.
- The big data storage architecture of endpoint meta-data allows for retroactive rules and the ability to "go-back-in-time" to see past events in the current context.
- The Endpoint Agent "store-and-forward" capability reports on potentially suspicious activity when offline eliminating network blind spots.
- Using the latest big data technology, FortiInsight collects billions of events which are collated, analyzed, and presented to your security team giving you near instant access to the information collected. For example, who downloaded the payroll database? Why is someone uploading a customer list to that IP address? How many people are using unapproved cloud storage apps?
- Endpoint agents are available for Windows.



How FortiInsight Works

The zero-config, lightweight agent installed on each system performs no analysis or preventative actions on the endpoint. Rather, the agent simply gathers and sends data for alerting or investigation. This 'endpoint agent' approach has significant advantages as it presents a smaller attack surface to sophisticated attackers, reduces performance drain on the endpoint, and sends telemetry to a cloud-based service that stores, analyzes and presents data to the security team. By centralizing the data, FortiInsight is able to correlate and machine learn across your entire estate, providing you with unparalleled insights into user and data behavior.

With FortiInsight, the sophisticated rules-based engine bolstered by smart machine learning ensures all activities are monitored on and off the network. Rules are drawn up to agree what constitutes acceptable user activity. The rules are applied and if activity takes place that breaches these rules, an alert is sent to the administrator. This feature-set is also harnessed extensively to deliver insight into potential breaches around compliance regimes (such as GDPR and HIPAA).

The FortiInsight solution utilizes machine learning which examines behavior around data — and data flow — to spot anomalies such as users who are acting out of character, for example, looking at files they don't normally seek out, or unusual changes in work patterns, compromised accounts or changes in peer group activities.

ORDER INFORMATION

FortiInsight is offered by seat-based annual subscription pricing model, with stackable 25 agent licenses. There is a minimal order of 20 pack (500 seats) for new customers. License includes cloud-based hosting.

Product	SKU	Description
FortiInsight	FC1-10-FUEBA-225-02-DD	25 Agent Subscription License. Minimum order 500 agents. Includes 24×7 FortiCare.

FORTINET®

www.fortinet.com