App Overview & FAQ

Forescout OT Network Security Monitoring App

The Forescout OT Network Security Monitoring App for Splunk

Overview

The Forescout OT Network Security Monitoring App for Splunk lets you act on OT/ICS threats and vulnerabilities using three intuitive Splunk dashboards. By integrating configurable alert data from Forescout eyeInspect (formerly SilentDefense™) with device information and other relevant network activity, this App provides Splunk users with unparalleled contextual information required to identify threats, manage remediation workflows and secure their ICS environment.

Details

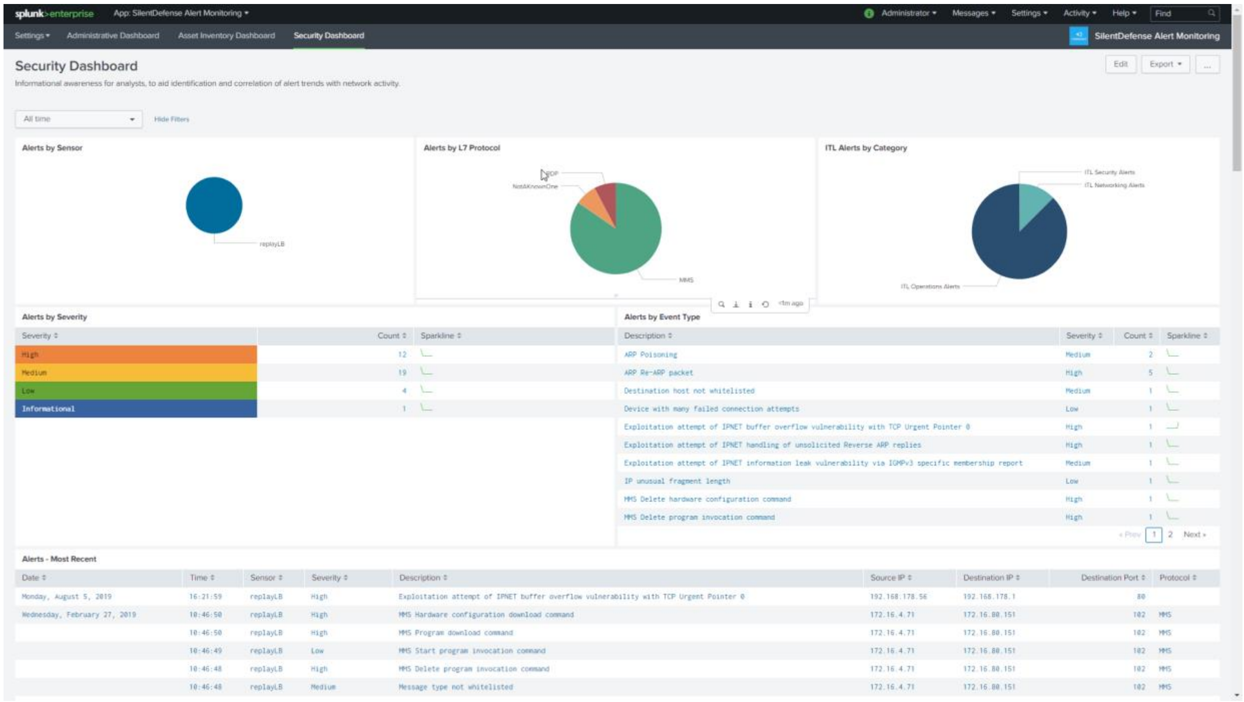
The Forescout OT Network Security Monitoring App for Splunk is the ideal solution for industrial asset owners who want to integrate rich OT asset intelligence and threat detection capabilities into their Splunk installation. With the App, you can leverage the exceptional OT device visibility and threat detection capabilities of eyeInspect to defend their OT/ICS networks from both operational failures and cyberattacks, such as Ripple20, EKANS, WannaCry, NotPetya, TRITON and many more.

The **Forescout OT Network Security Monitoring App for Splunk** contains three pre-built Splunk Dashboards:

- The **Security Dashboard** helps you identify alert trends and correlate them with other network activity, enabling faster detection of anomalies, cyberthreats, dangerous commands sent to OT devices and device misbehavior. It also helps reduce mean time to response by providing the context needed to determine the best mitigation action.
- The **Asset Inventory Dashboard** lets analysts access high-value device information and context to better identify unexpected changes in the network, prioritize investigations and quickly acknowledge new assets, communication patterns or protocols seen within the network, helping to help asset inventory and maintenance processes.
- The **Administrative Dashboard** provides deep insights on system health status and user activity performed on eyeInspect appliances to prevent system failure and detect undesired user activity.

Frequently Asked Questions

Security Dashboard



Security Dashboard

Informational awareness for analysts, to aid identification and correlation of alert trends with network activity.

Alerts by Severity

Severity ⇕	Count ⇕	Sparkline ⇕
High	12	
Medium	19	
Low	4	
Informational	1	

Alerts by Event Type

Description ⇕	Severity ⇕	Count ⇕	Sparkline ⇕
ARP Poisoning	Medium	2	
ARP Re-ARP packet	High	5	
Destination host not whitelisted	Medium	1	
Device with many failed connection attempts	Low	1	
Exploitation attempt of IPNET buffer overflow vulnerability with TCP Urgent Pointer 0	High	1	
Exploitation attempt of IPNET handling of unsolicited Reverse ARP replies	High	1	
Exploitation attempt of IPNET information leak vulnerability via IGMPv3 specific membership report	Medium	1	
IP unusual fragment length	Low	1	
MMS Delete hardware configuration command	High	1	
MMS Delete program invocation command	High	1	

Alerts - Most Recent

Date ⇕	Time ⇕	Sensor ⇕	Severity ⇕	Description ⇕	Source IP ⇕	Destination IP ⇕	Destination Port ⇕	Protocol ⇕
Monday, August 5, 2019	16:21:59	replayLB	High	Exploitation attempt of IPNET buffer overflow vulnerability with TCP Urgent Pointer 0	192.168.178.56	192.168.178.1	80	
Wednesday, February 27, 2019	10:46:50	replayLB	High	MMS Hardware configuration download command	172.16.4.71	172.16.80.151	102	MMS
	10:46:50	replayLB	High	MMS Program download command	172.16.4.71	172.16.80.151	102	MMS
	10:46:49	replayLB	Low	MMS Start program invocation command	172.16.4.71	172.16.80.151	102	MMS
	10:46:48	replayLB	High	MMS Delete program invocation command	172.16.4.71	172.16.80.151	102	MMS
	10:46:48	replayLB	Medium	Message type not whitelisted	172.16.4.71	172.16.80.151	102	MMS

CHALLENGE: Are there any urgent threats that I need to focus on, and what should I do to respond?

RESPONSE: The Security Dashboard helps you identify alert trends and correlate them with other network activity, enabling faster detection of anomalies, cyberthreats, dangerous commands sent to OT devices and device misbehavior. It also helps reduce mean time to response by providing the context needed to determine the best mitigation action.

Q. What are the latest alerts in my network?

A: The "Recent OT Network Security Monitoring Alerts" widget displays the most recent alerts with details like originating Sensor, Severity, Description, Source IP, Destination IP, Destination Port and Layer 7 Protocol. The "ITL Alerts (24h/1h)" widget helps to monitor whether the alert trend has been increasing or decreasing in the selected time interval.

Q. Are there any critical alerts I need to focus on immediately?

A: The "Alerts by Severity" widget categorizes alerts as Informational, Low, Medium, High and Critical for immediate visibility and response to urgent issues.

Q: From where do my problems/threats originate?

A: The "Alerts by Sensor Name", "Alerts by L7 Protocol" and "Alerts by Sensor Name by Protocol" widgets help to identify the origin of the alert. In particular, originating sensor information helps to identify the network affected and protocol information allows you to better drill down into potential threat vectors and the processes involved.

Q. Is my network affected by cyber, operational or networking issues?

A: The "ITL Alerts by Category" widget displays the alerts generated by the eyeInspect Industrial Threat Library (ITL). The ITL detects threats that may impact one of the following three areas of responsibility: Operations, Security and Networking. This lets you immediately assign the investigation and initiate response through the most appropriate personnel.

Q. What type of problems/threats am I dealing with?

A: The “Alerts by Event Type” widget displays statistics about the number of events per type. This helps you identify which problems or threats occur more frequently.

Q. Which assets are the most impacted?

A: The “Alert Types by IP” widget displays the number of alerts associated with the top 15 assets (source and/or destination). The “Alert Types by Source IP” widget helps identify the source of the anomalous changes of behavior.

Q. Are there any relevant DNS requests that could provide useful context for my analysis?

A: The “DNS Queries - Top 15, DNS Queries – Fewest 10, Resolved DNS Queries – Top 10, Resolved DNS Queries - Fewest 10” widgets allow you to ensure that assets only communicate with legitimate domains. Suspicious or blacklisted domain names may indicate that the asset is infected (e.g., trying to reach out to malware C&C) or attempting unauthorized communications.

Q. Is there any unauthorized network access to my assets?

A: Many OT protocols allow authentication on clear text protocols. It is important to monitor successful and failed authentication attempts to critical assets for accountability and security reasons. The “Authentication Success”, “Authentication Failures” and “Authentication Details” aid in this analysis.

Q. Are there any encrypted connections with unauthorized SSL certificates in my network?

A: The “SSL Certificates Requested” widget Identifies SSL certificates used in the network in listing their Issuer, Validity, Expiration, Cipher Suite used, Source IP and Destination IP. This lets you identify (attempted) encrypted communications with unauthorized or invalid certificates.

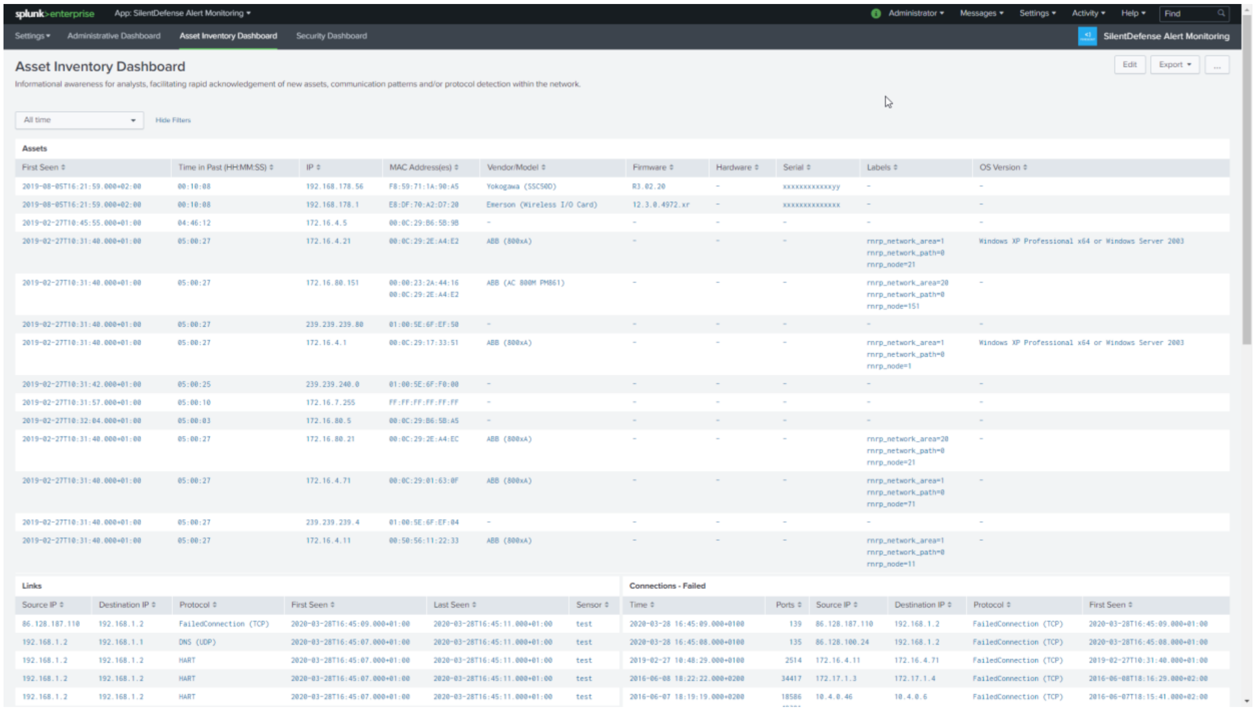
Q. Are there any unexpected file transfers that may indicate lateral movement?

A: The “File Activity” widget shows file access and transfers happening on the network, such as file reads, writes or deletes. The file name indicated in the widget helps to identify whether the operation is legitimate or represents, for instance, an exfiltration attempt of sensitive information or malware lateral movement.

Q. Are there any unexpected file transfers that may indicate lateral movement?

A: The “File Activity” widget shows file access and transfers happening on the network, such as file reads, writes or deletes. The file name indicated in the widget helps to identify whether the operation is legitimate or represents, for instance, an exfiltration attempt of sensitive information or malware lateral movement.

Asset Inventory Dashboard



Asset Inventory Dashboard

Informational awareness for analysts, facilitating rapid acknowledgement of new assets, communication patterns and/or protocol detection within the network.

Assets

First Seen	Time in Past (HH:MM:SS)	IP	MAC Address(es)	Vendor/Model	Firmware	Hardware	Serial	Labels	OS Version
2019-08-05T16:21:59.000+02:00	00:10:08	192.168.178.56	F8:59:71:1A:90:A5	Yokogawa (SSC50D)	R3.02.20	-	xxxxxxxxxxxxyy	-	-
2019-08-05T16:21:59.000+02:00	00:10:08	192.168.178.1	E8:DF:70:A2:D7:20	Emerson (Wireless I/O Card)	12.3.0.4972.xr	-	xxxxxxxxxxxxxx	-	-
2019-02-27T10:45:55.000+01:00	04:46:12	172.16.4.5	00:0C:29:B6:5B:9B	-	-	-	-	-	-
2019-02-27T10:31:40.000+01:00	05:00:27	172.16.4.21	00:0C:29:2E:A4:E2	ABB (800xA)	-	-	-	rnrp_network_area=1 rnrp_network_path=0 rnrp_node=21	Windows XP Professional x64 or Windows Server 2003
2019-02-27T10:31:40.000+01:00	05:00:27	172.16.80.151	00:00:23:2A:44:16 00:0C:29:2E:A4:E2	ABB (AC 800M PM861)	-	-	-	rnrp_network_area=20 rnrp_network_path=0 rnrp_node=151	-
2019-02-27T10:31:40.000+01:00	05:00:27	239.239.239.80	01:00:5E:6F:EF:50	-	-	-	-	-	-
2019-02-27T10:31:40.000+01:00	05:00:27	172.16.4.1	00:0C:29:17:33:51	ABB (800xA)	-	-	-	rnrp_network_area=1 rnrp_network_path=0 rnrp_node=1	Windows XP Professional x64 or Windows Server 2003
2019-02-27T10:31:42.000+01:00	05:00:25	239.239.240.0	01:00:5E:6F:F0:00	-	-	-	-	-	-
2019-02-27T10:31:57.000+01:00	05:00:10	172.16.7.255	FF:FF:FF:FF:FF:FF	-	-	-	-	-	-
2019-02-27T10:32:04.000+01:00	05:00:03	172.16.80.5	00:0C:29:B6:5B:A5	-	-	-	-	-	-
2019-02-27T10:31:40.000+01:00	05:00:27	172.16.80.21	00:0C:29:2E:A4:EC	ABB (800xA)	-	-	-	rnrp_network_area=20 rnrp_network_path=0 rnrp_node=21	-
2019-02-27T10:31:40.000+01:00	05:00:27	172.16.4.71	00:0C:29:01:63:0F	ABB (800xA)	-	-	-	rnrp_network_area=1 rnrp_network_path=0 rnrp_node=71	-
2019-02-27T10:31:40.000+01:00	05:00:27	239.239.239.4	01:00:5E:6F:EF:04	-	-	-	-	-	-
2019-02-27T10:31:40.000+01:00	05:00:27	172.16.4.11	00:50:56:11:22:33	ABB (800xA)	-	-	-	rnrp_network_area=1 rnrp_network_path=0 rnrp_node=11	-

Links

Source IP	Destination IP	Protocol	First Seen	Last Seen	Sensor
86.128.187.110	192.168.1.2	FailedConnection (TCP)	2020-03-28T16:45:09.000+01:00	2020-03-28T16:45:11.000+01:00	test
192.168.1.2	192.168.1.1	DNS (UDP)	2020-03-28T16:45:07.000+01:00	2020-03-28T16:45:11.000+01:00	test
192.168.1.2	192.168.1.2	HART	2020-03-28T16:45:07.000+01:00	2020-03-28T16:45:11.000+01:00	test
192.168.1.2	192.168.1.2	HART	2020-03-28T16:45:07.000+01:00	2020-03-28T16:45:11.000+01:00	test
192.168.1.2	192.168.1.2	HART	2020-03-28T16:45:07.000+01:00	2020-03-28T16:45:11.000+01:00	test

Connections - Failed

Time	Ports	Source IP	Destination IP	Protocol	First Seen
2020-03-28 16:45:09.000+0100	139	86.128.187.110	192.168.1.2	FailedConnection (TCP)	2020-03-28T16:45:09.000+01:00
2020-03-28 16:45:08.000+0100	135	86.128.100.24	192.168.1.2	FailedConnection (TCP)	2020-03-28T16:45:08.000+01:00
2019-02-27 10:48:29.000+0100	2514	172.16.4.11	172.16.4.71	FailedConnection (TCP)	2019-02-27T10:31:40.000+01:00
2016-06-08 18:22:22.000+0200	34417	172.17.1.3	172.17.1.4	FailedConnection (TCP)	2016-06-08T18:16:29.000+02:00
2016-06-07 18:19:19.000+0200	18586	10.4.0.46	10.4.0.6	FailedConnection (TCP)	2016-06-07T18:15:41.000+02:00

CHALLENGE: Are there any unexpected changes in my network?

RESPONSE: The Asset Inventory Dashboard lets analysts access high-value device information and context to better identify unexpected changes in the network, prioritize investigations and quickly acknowledge new assets, communication patterns or protocols seen within the network, helping to streamline asset inventory and maintenance processes.

Q. Is there any new device or relevant change in my network?

A: The "Assets – Added to Inventory" widget displays the list of assets seen by eyeInspect listing IP, MAC Address(es), Vendor/Model, Firmware version or Hardware version. In addition, the "Assets with Modules – Added to Inventory" widget shows if new backplane modules have been added to PLCs.

Q. Is there any new communication I've never seen?

A: The "Links - Last Seen 20" widget displays the last 20 communication links seen on the network within the selected time interval.

Q. Are there any network connectivity issues?

A: The "Failed Connections" widget displays failed connections seen within the network that may indicate connectivity problems.

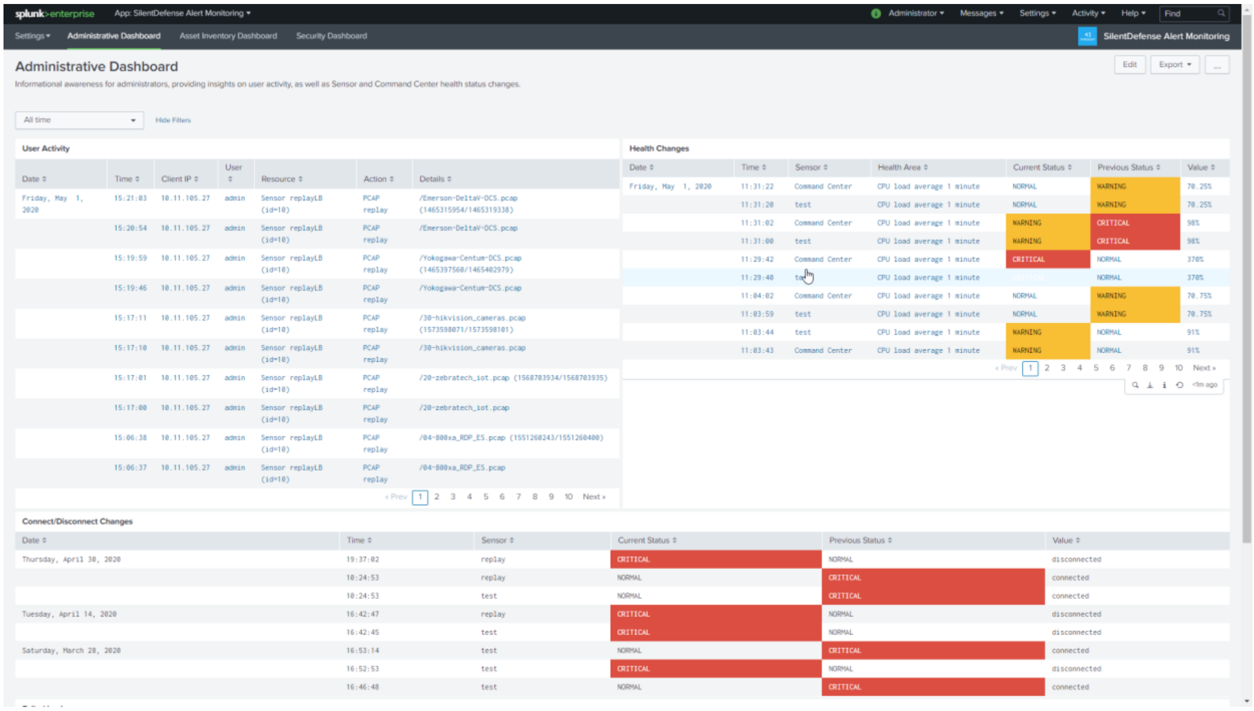
Q. Did an asset go offline? Or are my assets attempting to communicate with unknown assets?

A: The "Ghost Nodes" widget displays ghost assets (i.e., assets receiving network requests but never responding).

Q. Is someone using insecure protocols like TELNET or uncommon protocols for OT like DHCP?

A: The "TELNET Protocol Used" and "DHCP Protocol Used" widgets help identify the usage of these protocols.

Asset Inventory Dashboard



Administrative Dashboard

Informational awareness for administrators, providing insights on user activity, as well as Sensor and Command Center health status changes.

User Activity

Date ⇕	Time ⇕	Client IP ⇕	User ⇕	Resource ⇕	Action ⇕	Details ⇕
Friday, May 1, 2020	15:21:03	10.11.105.27	admin	Sensor replayLB (id=10)	PCAP replay	/Emerson-DeltaV-DCS.pcap (1465315954/1465319338)
	15:20:54	10.11.105.27	admin	Sensor replayLB (id=10)	PCAP replay	/Emerson-DeltaV-DCS.pcap
	15:19:59	10.11.105.27	admin	Sensor replayLB (id=10)	PCAP replay	/Yokogawa-Centum-DCS.pcap (1465397560/1465402979)
	15:19:46	10.11.105.27	admin	Sensor replayLB (id=10)	PCAP replay	/Yokogawa-Centum-DCS.pcap
	15:17:11	10.11.105.27	admin	Sensor replayLB (id=10)	PCAP replay	/30-hikvision_cameras.pcap (1573598071/1573598101)
	15:17:10	10.11.105.27	admin	Sensor replayLB (id=10)	PCAP replay	/30-hikvision_cameras.pcap
	15:17:01	10.11.105.27	admin	Sensor replayLB (id=10)	PCAP replay	/20-zebratech_iot.pcap (1568703934/1568703935)
	15:17:00	10.11.105.27	admin	Sensor replayLB (id=10)	PCAP replay	/20-zebratech_iot.pcap
	15:06:38	10.11.105.27	admin	Sensor replayLB (id=10)	PCAP replay	/04-800xa_RDP_ES.pcap (1551260243/1551260400)
	15:06:37	10.11.105.27	admin	Sensor replayLB (id=10)	PCAP replay	/04-800xa_RDP_ES.pcap

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Health Changes

Date ⇕	Time ⇕	Sensor ⇕	Health Area ⇕	Current Status ⇕	Previous Status ⇕	Value ⇕
Friday, May 1, 2020	11:31:22	Command Center	CPU load average 1 minute	NORMAL	WARNING	70.25%
	11:31:20	test	CPU load average 1 minute	NORMAL	WARNING	70.25%
	11:31:02	Command Center	CPU load average 1 minute	WARNING	CRITICAL	98%
	11:31:00	test	CPU load average 1 minute	WARNING	CRITICAL	98%
	11:29:42	Command Center	CPU load average 1 minute	CRITICAL	NORMAL	370%
	11:29:40	te	CPU load average 1 minute	CRITICAL	NORMAL	370%
	11:04:02	Command Center	CPU load average 1 minute	NORMAL	WARNING	70.75%
	11:03:59	test	CPU load average 1 minute	NORMAL	WARNING	70.75%
	11:03:44	test	CPU load average 1 minute	WARNING	NORMAL	91%
	11:03:43	Command Center	CPU load average 1 minute	WARNING	NORMAL	91%

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Connect/Disconnect Changes

Date ⇕	Time ⇕	Sensor ⇕	Current Status ⇕	Previous Status ⇕	Value ⇕
Thursday, April 30, 2020	19:37:02	replay	CRITICAL	NORMAL	disconnected
	10:24:53	replay	NORMAL	CRITICAL	connected
	10:24:53	test	NORMAL	CRITICAL	connected
Tuesday, April 14, 2020	16:42:47	replay	CRITICAL	NORMAL	disconnected
	16:42:45	test	CRITICAL	NORMAL	disconnected
Saturday, March 28, 2020	16:53:14	test	NORMAL	CRITICAL	connected
	16:52:53	test	CRITICAL	NORMAL	disconnected
	16:46:48	test	NORMAL	CRITICAL	connected

CHALLENGE: How is the health of my Forescout eyeInspect installation?

A: The Administrative Dashboard provides deep insights on system health status and user activity performed on eyeInspect appliances to prevent system failure and detect undesired user activity.

Q. What is my eyeInspect system health status?

A: The “Health Changes” and “Connect/Disconnect Changes” widgets display the latest health status changes of eyeInspect components. For example, it displays when sensors are at a critical memory usage level and when sensors frequently connect and disconnect from a Command Center to enable quick response on issues that – if unattended – may lead to system failure.

Q. Can I have complete accountability of the users’ behavior on eyeInspect?

A: The “User Activity” widget shows the activity being performed by eyeInspect users, such as logins or changes to sensor configuration. The “Failed Logins” widget shows recent login attempts and failures to highlight potential breaches.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com