Physical Layer Security

Physical layer security is driven by real-time documentation, comprehensive event logs that provide insight into every physical layer change, and the ability to **set off actions in response to network changes.**

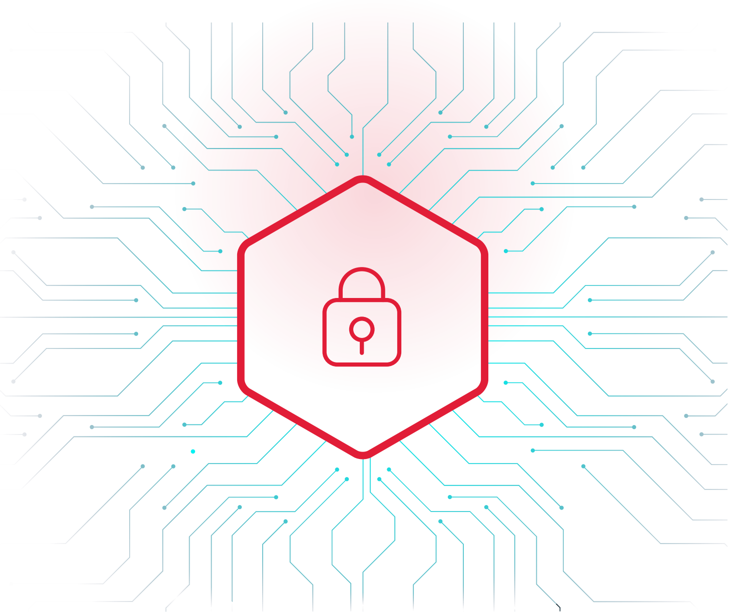
Introduction

The physical layer is an essential component of any network infrastructure as it serves as the foundation for all network activities. Any issues or vulnerabilities at this level can potentially compromise the entire network, making it crucial to ensure that the physical layer is secure and well-maintained. Our solution recognizes the significance of the physical layer in a data center and proposes a redesign that integrates security and intelligence features to optimize data center agility.

At Fiber Mountain, we prioritize physical layer security by providing real-time documentation and comprehensive event logs that offer visibility into every change made at this level. This level of visibility enables our solution to detect any suspicious activity or potential security breaches at the physical layer promptly. Additionally, our solution can trigger automated actions based on changes in the network. These automated responses can help prevent security breaches and minimize their impact if they occur.

Fiber Mountain's integrated security and intelligence features at the physical layer offer robust protection for any data center by prioritizing physical layer security and implementing real-time monitoring and automated responses.

We Have a **Zero Trust** Policy



As experts in physical layer security, we understand that a zero-trust policy is essential in ensuring the security of the network. This policy is implemented by making the physical layer transparent. This means that we aim to make it easy for network administrators to identify, monitor, and track the physical layer of the network. By doing so, we can identify any potential security threats or breaches and take appropriate action in a timely manner.

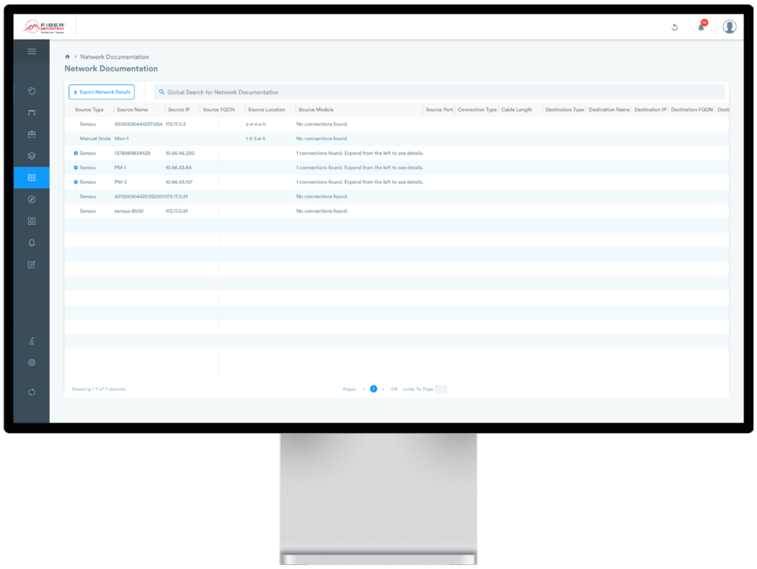
Transparency in the physical layer involves a number of techniques and tools, such as the use of specialized equipment and software that enable real-time monitoring of the physical layer. This can be managed via AllPath® Director that can detect any anomalies or changes in the physical layer, which may indicate the presence of an unauthorized device or an attempt to breach the network.

By implementing a zero-trust policy and making the physical layer transparent, we can ensure that the network remains secure and that any potential security threats are identified and addressed before they can cause damage.

Automated Documentation

Our solutions offer unprecedented visibility and flexibility for data center operations. By automating real-time and precise documentation, we enable efficient management of data center operations, quicker response to security issues, compliance demands, and unplanned outages.

Previously, the physical layer of data center infrastructure, consisting of patch panels, cables, and connection points, was only visible through manual documentation by human technicians. With our solution of automated documentation, this obstacle is eliminated, allowing the physical layer to be directly visible and controllable by software, without requiring human intervention to input data into spreadsheets.



Network Documentation

Network Documentation

Source Type	Source Name	Source IP	Source FQDN	Source Location	Source Module	Source Port	Connection Type	Cable Length	Destination Type	Destination Name	Destination IP	Destination FQDN	Desti
Sensus	6515269044415371264	172.17.0.2		z-e-e.s-h	No connections found.								
Manual Node	Man-1			1-2-3.4-5	No connections found.								
Sensus	1378989834429	10.66.46.250			1 connections found. Expand from the left to see details.								
Sensus	PM-1	10.66.43.84			1 connections found. Expand from the left to see details.								
Sensus	PM-2	10.66.43.157			1 connections found. Expand from the left to see details.								
Sensus	6515269044203520000	172.17.0.21			No connections found.								
Sensus	sensus-8500	172.17.0.51			No connections found.								

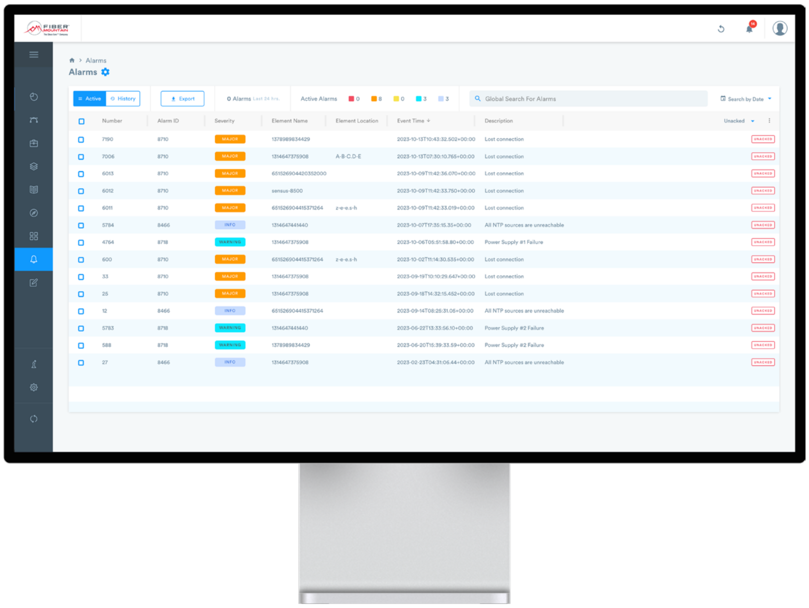
Showing 1-7 of 7 records

One of the major benefits of our technology is that AllPath® Director comprehends the connections between intelligent cables and creates automated documentation of the topology, including MACs, with complete accuracy. This means that physical layer documentation is always precise and up to date, resulting in a stress-free and harmonious data center environment.

Alarms

The ability to promptly detect and respond to unplanned changes in a data center is crucial in preventing physical security breaches and unintentional cabling errors that can cause damage and downtime. With Fiber Mountain solutions, data centers can achieve the necessary visibility and agility to address physical changes either through software or by precisely deploying technicians for manual corrections.

APD's alarm notifications are an essential component of this process, providing detailed information such as problem description, severity, time of occurrence, device location, port, and even fiber. The combination of automated documentation and alarms notifies network operators of unscheduled changes, such as power supply failures, fiber disconnects, and unauthorized repatching, streamlining and accelerating the troubleshooting and correction process.

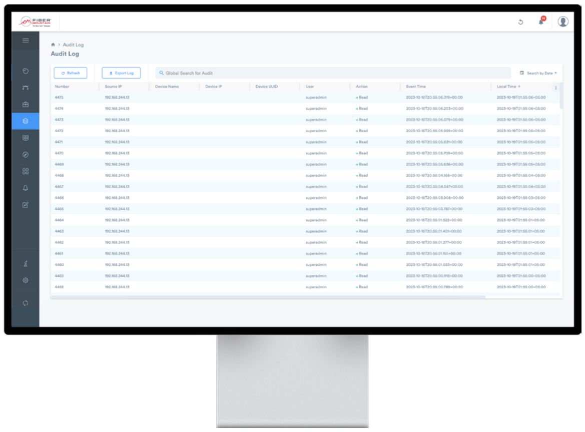


□	Number	Alarm ID	Severity	Element Name	Element Location	Event Time	Description	Unacked
□	7190	8710	MAJOR	1378989834429		2023-10-13T10:43:32.502+00:00	Lost connection	UNACKED
□	7006	8710	MAJOR	1314647375908	A-B-C.D-E	2023-10-13T07:30:10.765+00:00	Lost connection	UNACKED
□	6013	8710	MAJOR	651526904420352000		2023-10-09T11:42:36.070+00:00	Lost connection	UNACKED
□	6012	8710	MAJOR	sensus-8500		2023-10-09T11:42:33.750+00:00	Lost connection	UNACKED
□	6011	8710	MAJOR	651526904415371264	z-e-e.s-h	2023-10-09T11:42:33.019+00:00	Lost connection	UNACKED
□	5784	8466	INFO	1314647441440		2023-10-07T17:35:15.35+00:00	All NTP sources are unreachable	UNACKED
□	4764	8718	WARNING	1314647375908		2023-10-06T05:51:58.80+00:00	Power Supply #1 Failure	UNACKED
□	600	8710	MAJOR	651526904415371264	z-e-e.s-h	2023-10-02T11:14:30.535+00:00	Lost connection	UNACKED
□	33	8710	MAJOR	1314647375908		2023-09-19T10:10:29.647+00:00	Lost connection	UNACKED
□	25	8710	MAJOR	1314647375908		2023-09-18T14:32:15.452+00:00	Lost connection	UNACKED
□	12	8466	INFO	651526904415371264		2023-09-14T08:25:31.05+00:00	All NTP sources are unreachable	UNACKED
□	5783	8718	WARNING	1314647441440		2023-06-22T13:33:56.10+00:00	Power Supply #2 Failure	UNACKED
□	588	8718	WARNING	1378989834429		2023-06-20T15:39:33.59+00:00	Power Supply #2 Failure	UNACKED
□	27	8466	INFO	1314647375908		2023-02-23T04:31:06.44+00:00	All NTP sources are unreachable	UNACKED

By leveraging this integrated approach, what could have been an extended shutdown or long-term security breach can be promptly resolved. The solution provides a rapid and effective response to physical network issues, ensuring the continuity and security of data center operations.

Audit Trails

In addition to Alarms, the Audit Trail feature of APD enhances data center network security by increasing awareness of both the network's present state and the timing and location of all past changes. This is crucial for minimizing vulnerabilities and ensuring compliance with regulations. The Audit Trail delivers an additional layer of visibility by documenting all data center events in an immutable record that cannot be changed or deleted by anyone.



Audit Log

Audit Log

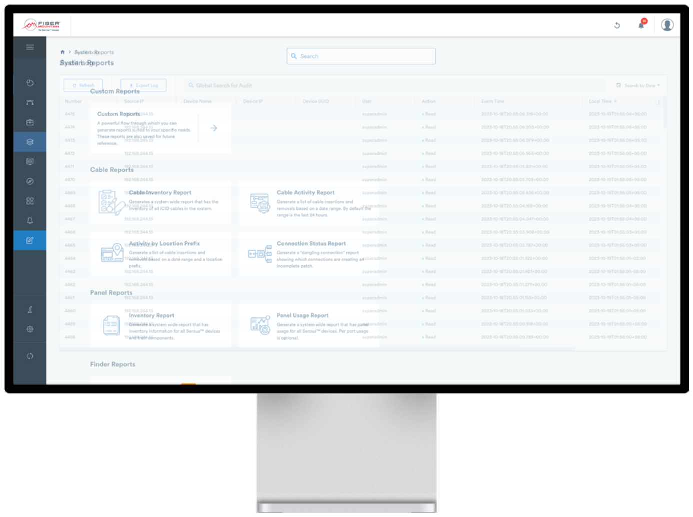
Number	Source IP	Device Name	Device IP	Device UUID	User	Action	Event Time	Local Time
4475	192.168.244.13				superadmin	• Read	2023-10-18T20:55:06.319+00:00	2023-10-19T01:55:06+05:00
4474	192.168.244.13				superadmin	• Read	2023-10-18T20:55:06.203+00:00	2023-10-19T01:55:06+05:00
4473	192.168.244.13				superadmin	• Read	2023-10-18T20:55:06.079+00:00	2023-10-19T01:55:06+05:00
4472	192.168.244.13				superadmin	• Read	2023-10-18T20:55:05.955+00:00	2023-10-19T01:55:05+05:00
4471	192.168.244.13				superadmin	• Read	2023-10-18T20:55:05.831+00:00	2023-10-19T01:55:05+05:00
4470	192.168.244.13				superadmin	• Read	2023-10-18T20:55:05.709+00:00	2023-10-19T01:55:05+05:00
4469	192.168.244.13				superadmin	• Read	2023-10-18T20:55:05.636+00:00	2023-10-19T01:55:05+05:00
4468	192.168.244.13				superadmin	• Read	2023-10-18T20:55:04.168+00:00	2023-10-19T01:55:04+05:00
4467	192.168.244.13				superadmin	• Read	2023-10-18T20:55:04.047+00:00	2023-10-19T01:55:04+05:00
4466	192.168.244.13				superadmin	• Read	2023-10-18T20:55:03.908+00:00	2023-10-19T01:55:03+05:00
4465	192.168.244.13				superadmin	• Read	2023-10-18T20:55:03.787+00:00	2023-10-19T01:55:03+05:00
4464	192.168.244.13				superadmin	• Read	2023-10-18T20:55:01.522+00:00	2023-10-19T01:55:01+05:00
4463	192.168.244.13				superadmin	• Read	2023-10-18T20:55:01.401+00:00	2023-10-19T01:55:01+05:00
4462	192.168.244.13				superadmin	• Read	2023-10-18T20:55:01.277+00:00	2023-10-19T01:55:01+05:00
4461	192.168.244.13				superadmin	• Read	2023-10-18T20:55:01.155+00:00	2023-10-19T01:55:01+05:00
4460	192.168.244.13				superadmin	• Read	2023-10-18T20:55:01.033+00:00	2023-10-19T01:55:01+05:00
4459	192.168.244.13				superadmin	• Read	2023-10-18T20:55:00.918+00:00	2023-10-19T01:55:00+05:00
4458	192.168.244.13				superadmin	• Read	2023-10-18T20:55:00.789+00:00	2023-10-19T01:55:00+05:00

The Audit Trail starts recording from the moment Fiber Mountain solutions are activated on the network, and the records can be exported for further preservation, analysis, or presentation. By preserving all events that occur in the data center, the Audit Trail provides a comprehensive historical view of the network's activity, helping to identify areas for improvement and increase overall network security.

System Reports

The System Reports feature provides data center network administrators with a powerful tool for generating detailed and customizable reports on cable and panel activity and inventory. By utilizing this feature, administrators gain a comprehensive understanding of the network's current condition, enabling them to identify areas for improvement and take proactive measures to maintain optimal network performance.

These reports can include a wide range of data, such as cable usage, patch panel connections, device inventory, and more, providing a complete view of the network's physical infrastructure. The reports can be generated on a regular basis or as needed, providing network administrators with the flexibility to obtain real-time insights into network activity.



System Reports

System Reports

Custom Reports

Custom Reports

A powerful flow through which you can generate reports suited to your specific needs. These reports are also saved for future reference.

Cable Reports

Cable Inventory Report

Generates a system wide report that has the inventory of all ICID cables in the system.

Cable Activity Report

Generate a list of cable insertions and removals based on a date range. By default the range is the last 24 hours.

Activity by Location Prefix

Generate a list of cable insertions and removals based on a date range and a location prefix.

Connection Status Report

Generate a "dangling connection" report showing which connections are creating an incomplete patch.

Panel Reports

Inventory Report

Generate a system wide report that has inventory information for all Sensus™ devices and their components.

Panel Usage Report

Generate a system wide report that has panel usage for all Sensus™ devices. Per port usage is optional.

Finder Reports

For more information, visit:
www.fibermountain.com

System Reports feature is a crucial component of data center network management, enabling administrators to stay fully aware of the network's condition and take proactive measures to ensure optimal performance. The feature provides a comprehensive view of network activity and inventory, ensuring that network administrators are fully equipped to identify and address any issues that may arise.

Conclusion

Fiber Mountain focuses on the importance of physical layer security in data centers and proposes a redesign of the physical layer that integrates security and intelligence features. The solution provides real-time documentation, comprehensive event logs, automated responses, and a zero-trust policy to ensure network security. It also offers automated documentation, alarms, audit trails, and system reports to achieve the necessary visibility and agility to address physical changes promptly. These features streamline and accelerate the troubleshooting and correction process, ensuring the continuity and security of data center operations. Overall, the solution offers robust protection for any data center, enabling network administrators to maintain a secure and agile network infrastructure.