Innovating Data Center Security with CyberSecure IPS

Executive White Paper

January 2019

*Corporate security **isn't** getting better **fast enough**, critical infrastructure security hangs in the balance, and state-backed hackers from around the world are getting bolder and more sophisticated.*

Wired Magazine

Executive Summary

With more companies and government agencies adopting Cloud and 3rd Party Hosting services, Data Center security is at the forefront on the minds of today's CIOs and CISOs. More than ever, traditional methods of security cannot keep up with the growing landscape of new and dangerous threats.

CyberSecure IPS Data Center Protection Suite offers an array of innovative security solutions to an area that is often overlooked—Physical Infrastructure and Layer 1 security

Using our patented software and sensing solutions, we provide a granular level of security that transcends traditional Data Center security products on the market today. Our 10-Layer Data Center Protection approach can be customized to any Data Center environment. Customers can choose to alarm cabinet doors, cage walls, and even individual floor tiles using our array of zero-power fiber optic sensors. This white paper will seek to communicate a major security issue facing every organization, but that has particular ramifications to Data Center and Cloud providers, as well as the following:

1) Why one of the largest Cloud providers globally has adopted our security solution.

2) How Data Center and Cloud providers can truly differentiate themselves in the crowded Hosting market by incorporating our solution into their offerings while increasing revenue at the same time.

Introduction

With the news of more Fortune 100 companies being hacked in today's headlines, there is tremendous pressure and scrutiny on Data Center providers and Cloud companies. No one is immune from the news of attacks on Target, Wells Fargo, Equifax, and most recently Facebook. The cyber security industry is crowded with companies and solutions that address the application layer, data layer, network layer, session layer and combinations thereof. But even with these sophisticated and often expensive tools in place, companies are still forced to come to the realization that they have been hacked with sensitive customer data being compromised. In most cases, companies are not aware until months after the data leakage or exfiltration has taken place that customer data has been stolen. These companies are then faced with the fallout with damage to their reputation whilst dealing with the financial penalties and reparations that persist long after the security issues have been addressed.

What many in the security industry has known for years is that most of the successful hacks into these large companies are the result of an inside job with someone who is ***supposed*** to have access or network permissions. The focal point for these attacks is the Data Center where all the critical data assets, be it structured or unstructured data, are stored. The physical fiber network infrastructure (or Layer 1) is a vulnerable aspect of security within and around the data center where the magnitude of threat can compound easily to those on the inside. This includes the fiber pathways and conduits that can be accessed through maintenance holes directly outside the facility and communication lines throughout the inside of the Data Center. This executive white paper presents the often-overlooked problem facing Data Center and Cloud providers today and presents the solution to monitor and mitigate against it.

The Insider Threat

Combatting the *Insider Threat* is not only elusive but without using the right set of tools, it can also be a costly endeavor. Often, these inside jobs are perpetrated by disgruntled employees or those that are under financial duress. In fact, these are the very types of people that hackers target and recruit to be their vectors into an organization's network. Social Engineering now combined with Social Media has made the work of hacking via an insider much easier and faster.

When it comes to physical Data Center security, we have found most providers and vendors have excellent safeguards to keep the "bad" actors from entering their premises. Traditional security measures such as automatic gates, Anti-Pass Back & Man Traps, 24/7 manned CCTV, and Biometric Access all keep the people who shouldn't be in the Data Center on the outside. But what about those that have access? These are typically the employees of the Data Center, maintenance contractors, or in a Colo scenario—the system administrators of customers leasing Colo space. In many cases 3rd party IT contractors are also prevalent. With this many people moving in and out of these Data Center facilities, the need to ensure that no one is accessing an area or data center cage that are off limits or trying to tap or manipulate a fiber cable traversing an aggregation point or cable tray is extremely important. Though recruiting best practices rightfully seek to weed out individuals who could potentially be a vector for malicious behavior, there is no guarantee and certainly no assurance that can be provided to end customers.

The CyberSecure IPS Solution

To address the ever-present insider threat, **CyberSecure IPS** utilizes their DoD-grade fiber sensing technology for the Data Center industry to create the Data Center Protection Suite.

Figure 1: Data Center Protection Suite

With our Data Center Protection Suite, customers can choose which features they wish to employ to ensure the level of protection they need as demonstrated in the scenario below.

Regardless of which features are deployed, the entire solution is monitored and managed by the **CyberSecure IMS** software. This user-friendly dashboard and console includes Real-time Alerts, Case Management, Event Logging, Visual Mapping, and API Integration. Key to our software is the patented Fiber Forensics capability which performs analysis and correlation of the sensor data to quickly determine actual intrusions versus false alarms. Furthermore, CyberSecure IMS can Integrate to existing security systems and be configured to send Email, SMS Text, and other forms of communication to immediately alert the appropriate personnel.

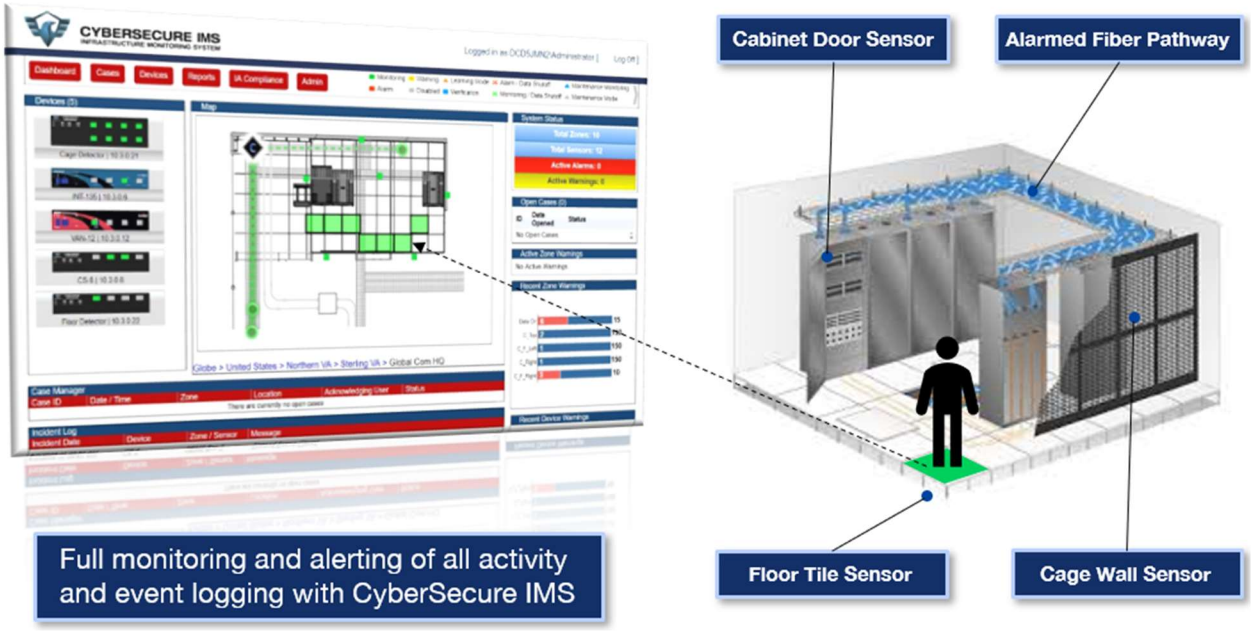


Figure 2: Customized Scenario

Our proprietary sensors require zero power and come in a variety of form factors to ensure it can be installed in various spaces and conditions. These ruggedized sensors can measure pressure, strain, dB loss, and even temperature. As shown in the diagram above, with our fiber-based sensors, we can detect where a person is standing in the cage, when a cabinet door is open or closed, if someone is trying to climb over the cage wall, and whether someone is trying to tap the fiber pathway specific to a cage. No other solution provides this level of situational awareness in the Data Center. In addition, our solution is one of the first to have received an accreditation for Risk Management Framework (RMF) from the Defense Information Systems Agency (DISA). Having gone through this level of scrutiny ensures that the CyberSecure IPS Data Center Protection solution will help any Data Center or Cloud provider meet the most stringent compliance and regulatory requirements.

- ✓ Centrally Managed Solution with installations spanning the globe
- ✓ Integrates into Existing Alarm Management Systems
- ✓ Integrated Standard Operating Procedures
- ✓ Patented Fiber Forensics™ Technology and Optical Warning System

Case Study

A Global Titan uses CyberSecure IPS

One of the largest Cloud providers and a ubiquitous player in the online consumer industry uses our security solution today in all their colocation data centers worldwide. This comprises data centers across 27 countries and 5 continents. This customer approached us after seeing a demo of our solution to address a single vulnerability that if exploited could be disastrous to their customers, most notably in the Government space.

Inside Plant Pathways (ISP) can hold thousands of strands of fiber and are commonly aggregated in Data Center facilities for efficiency and to conserve space. These run along conduits near the ceilings above or in meet me rooms throughout the facility. These bundled cables are then distributed to other parts of the Data Center holding critical customer shared infrastructure or to individual cages leased by Colo customers.

Figure 3: ISP Pathways

In order to mitigate this vulnerability and to monitor and detect any insider from potentially accessing or tapping a fiber cable, this Data Center company leverages our ISP Pathway protection solution from the Data Center Protection Suite. Using a patented fiber sensing solution, we monitor the fiber pathway using spare strands of fiber within the optical cables of the network infrastructure. This 24/7/365 monitoring allows the system to immediately detect and report the most subtle tampering or sophisticated intrusion attempts on the network. With the ISP Pathway protection, this Cloud provider is now able to ensure their customers enjoy the added assurance of knowing that their fiber cable feeding into their cage has not been tampered

Multiple Layers of Protection:

- ✓ Perimeter fences
- ✓ Maintenance Holes
- ✓ OSP Pathways and Conduits
- ✓ Utility Pathways
- ✓ Raised Floor
- ✓ Cage Perimeter
- ✓ Cage Door
- ✓ Ladder Rack
- ✓ Cabinet Door
- ✓ ISP Pathways and Conduits Monitoring

with and is under constant supervision using our CyberSecure IMS software.

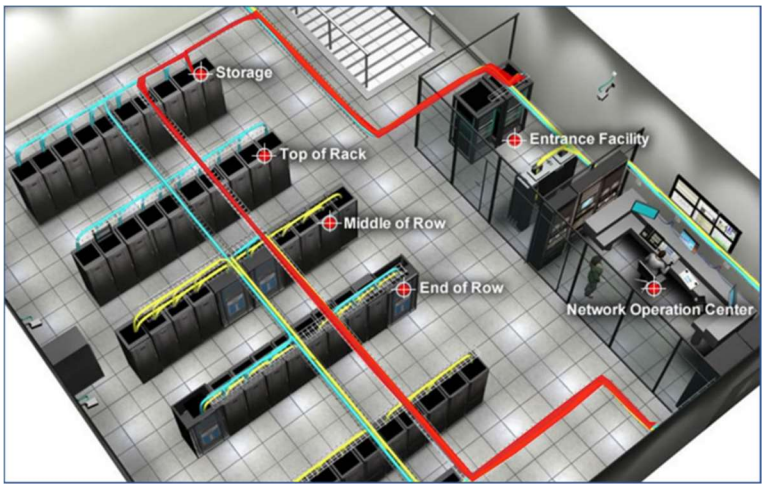


Figure 4: Alarmed Pathway Zones

It is important to note that while protecting your ISP pathways are important, it is just as important to ensure that your OSP (Outside Plant) pathway is protected as well. Another globally known Data Center customer is doing just that by using both the ISP and OSP protection features from our Data Center protection suite. More often today, global Data Center providers who service US Government agencies are being required to take additional security measures when hosting customers from countries such as Russia and China. By using our fiber optic sensors, our solution ensures that no one from a neighboring cage can enter or tamper with an alarmed data center asset without being detected.

Integration with Existing Security Systems

Having the ability to integrate with existing monitoring and security systems is key to any new solution that is acquired and deployed. The global Data Center provider in this case study required integration with their onsite Lenel Security system used by their NOC security staff. Our CyberSecure IMS software was integrated with their Lenel OnGuard system with standard REST API integration and now provides actionable intelligence to the appropriate security personnel.

Our software integration capability extends far beyond IDS Alarm systems to any monitoring software capable of using SNMP traps. Whether it's COTs software such as WhatsUpGold and Nagios, or to highly customized Government systems such as Vindicator, CyberSecure IMS has dynamic API capability to ensure seamless integration. Furthermore, our team of expert developers can provide the required support to help customers ensure integration with our software is fast and painless.

Financial Potential for Data Center Operators

Although this white paper has provided numerous compelling reasons for Data Center and Cloud providers to leverage our Data Center Protection solution, there is even more to consider with the financial potential that exists in leveraging our solution as a mechanism for added revenue. With our security technology in place, Data Center providers can advertise additional security features such as ISP Pathway monitoring, Cabinet Door monitoring, and Floor Tile monitoring as premium services. These added security features can be imbedded into existing service models and priced as a distinctive capability. With this in place, the data center pricing strategy can include these capabilities within a 'premium' a la carte plan for those customers that are hyper-sensitive to security concerns. Pricing can be modular with a cost associated to each type of protection or included as a bundled price for all 10 layers of security.

The added revenue stream this provides for Data Center and Cloud providers can be extremely lucrative in a multitenant environment where our solution is setup for a particular cage or container within the Data Center that is reserved for customers willing to pay for the added security benefits of our solution. Applying such a pricing model where customers pay per server in a virtual server environment could prove to be quite significant for data center vendors when considering deployments of virtual infrastructure can scale to the thousands.

External revenue streams aside, there are also operational cost benefits that can be derived from our solution that will significantly impact the bottom line for Data Center and Cloud providers. Our solution can be used to minimize the time to troubleshoot an issue causing downtime due to a fiber cable being cut or conduit being damaged. Our monitoring solution will immediately alert the appropriate personnel to the area or affected zone where the fiber cable damage has occurred. When seconds in down time equate to millions of dollars in lost revenue, any additional intel on identifying the problem area and being able to troubleshoot the root cause is critical. Reduced down-time will help meet SLAs and also keep the Data Center & Cloud provider from incurring stiff financial penalties.

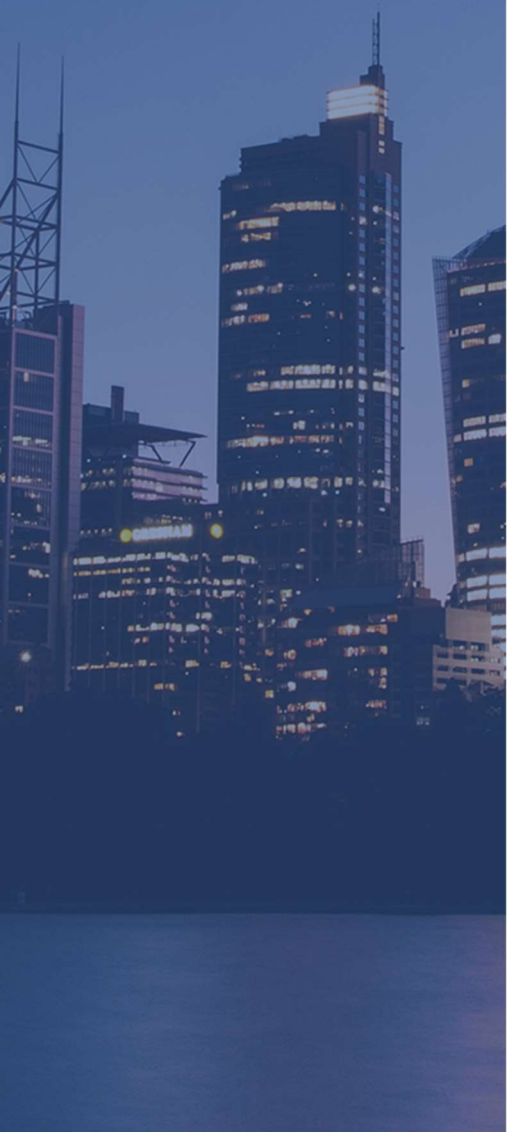
Interested in learning more?

Contact us at

1-844-653-1018

sales@cybersecureips.com

www.cybersecureips.com



Conclusion

Trying to prepare for an unknown future is challenging. Yet some clear trends are emerging in the rapidly growing and changing Data Center industry. The convergence of IoT, Smart Cities, and mobile data transactions correlate to the creation of new frontiers in Data Science (ML/AI) which will continue to add demand for bandwidth and capacity making way for innovations such as Edge Computing. With continued construction of new Data Centers and Edge Computing facilities to meet this demand, physical infrastructure vulnerability will continue to expand in kind. As the physical footprint of these Data Centers grow, more resources will be required to counter threats on multiple levels within the data center.

As a category-defining leader, **CyberSecure IPS** knows and understands the threat against the physical Layer 1 infrastructure. Born from the standards of DoD-grade requirements, our solutions are uniquely positioned to ensure the right kinds of security measures are in place to protect a commercial Data Center's weakest link—the Insider Threat. Our Data Center security solutions will help the providers and customers sleep well at night knowing that their most critical data assets are being monitored and protected.