Raritan®
A brand of legrand®

Physical Security and Compliance at the Rack Level

FIVE WAYS TO FULFILL TOUGHER REQUIREMENTS WITH LIMITED RESOURCES

A White Paper from Raritan

INTRODUCTION

If you are a data center manager, you face escalating security and compliance requirements in the white space and at the rack level. No longer is it sufficient to merely safeguard your data center or facility with secure, auditable access control just at entrances or building grounds. Increasingly, regulators also demand that you diligently restrict and audit access to specific data infrastructure, which contains digital assets such as customers' financial records and patients' healthcare data. Since the server rack is the final point of data vulnerability in the data center, where this data infrastructure is powered, it makes sense to consider implementing the same level of sophisticated physical security and access control monitoring at the rack that is already established at every other level of entry in the data center.

Unfortunately, you most likely don't have unlimited resources to fulfill these increasingly stringent rack-level access control requirements. Your capital budget, available cash, staff time, and tolerance for complexity are all finite. And because of this, you must evolve your rack-level access controls aggressively and efficiently.

To fulfill your rack-level compliance requirements with the utmost confidence and efficiency, you need to make some smart decisions for both the near and long term. In particular, implementing control and audit solutions that readily fit into your existing DCIM technology that leverage your current security systems. Over time, you can cost-effectively add new and required rack-level control and monitoring capabilities without adding counter-productive friction to your staff's daily tasks.

RAISING THE BAR AT THE RACK

At one time, it was sufficient to merely regulate access to the data center's entry points. If you could ensure that no unauthorized person had access to your sensitive digital infrastructure — and if you could prove those reasonable measures to auditors — you would be OK.

Times have changed. Escalating regulatory requirements across industries now require sensitive systems and data to be subject to specific protections. It's no longer enough to ensure that only authorized staff enters the data center. You must now track and monitor each person's access to specific sensitive systems and ensure they are properly authorized for a particular area. And you must be able to provide an extensive audit trail regarding who touched those systems when — and what they did each time.

In other words, rack-level physical security and compliance are necessary.

Of course, the particulars of compliance vary from industry to industry. The mandates outlined by HIPAA (Health Insurance Portability and Accountability Act) are not precisely the same as those in SOX (Sarbanes-Oxley Act). And the requirements of PCI DSS (Payment Card Industry Data Security Standard) are not the same as those in SSAE (Statement on Standards for Attestation Engagements).

But regardless of these particulars, the primary goal of compliance standards across industries is similar: Ensure that your most sensitive systems and data are especially protected against inappropriate access — and that your compliance with regulatory mandates is accurately documented.

Critical considerations for physical rack-level security and compliance may include:

- Enclosure locks can be remotely administered so that appropriate permissions can be mapped between the right people and the right systems using enterprise security policy and/or ad hoc administration.
- Proximity card authentication makes it easy for authorized personnel to quickly gain access to the enclosures for which they are authorized.
- Single-factor, dual-factor, or multi-factor authentication refers to the number of unique keys required to access a particular area or enclosure.
- Door sensors monitor the door's position, either opened or closed to connect seamlessly, power, operate, and manage electronic handles.
- In-rack cameras capture live video and photos that are automatically tagged with relevant data (time, date, user ID, system data, actions, etc.) for audit documentation and forensics.
- Integration with DCIM or other access control systems to facilitate a single point-of-control and easy consolidation of all security/compliance-related audit trails.
- Encryption and detection safeguards to ensure the integrity of rack-level security protections and audit systems.
- Real-time alerting and alarming that notifies appropriate parties of problematic events requiring immediate attention.
- Implementing incident management processes and procedures including specifying courses of action, procedures for notification, escalation, mitigation, and documentation.
- Rack PDU integration to ensure continuity of security and compliance even in a power outage.

It's worth noting that rack-level compliance requirements will continue to evolve as customers and regulators alike become increasingly concerned about the potential social and economic impact of data breaches. It's wise to take a long-term view of your rack-level physical security needs — rather than focusing only on what current regulations require.

OBSTACLES TO RACK-LEVEL SUCCESS

While the above security and compliance goals may seem straightforward, several obstacles can stand between you and rack-level success. These obstacles include:

TOTAL COST OF OWNERSHIP

If you're like most data center managers, your capital budget and headcount are already spread thin. When determining how to fulfill your rack-level compliance requirements, you must factor in the total cost of ownership (TCO).

The upfront capital cost of purchasing and installing any new equipment and software is just one part of this TCO. It is crucial to consider the possible effects of rack-level implementation on resource efficiency — including how it will add to your ongoing administrative burdens or valuable staff productivity lost due to chronic failures with proper rack access.

PROCESS INTEGRITY AND CONFIDENCE

It's also important to recognize that your rack-level controls don't exist in a vacuum. They are a critical part of your data center infrastructure management workflows. They feed into your SIEM (Security Information and Event Management) analytics and forensics. They support the delivery of compliance documentation to your organization's internal and external auditors. They can even play a role in processes you haven't considered — such as the capture and analysis of activity-based data center costs.

For your rack-level tools to effectively function in all these contexts, they must integrate well with a wide range of associated hardware and software. And the diverse stakeholders in rack-level management — from your front-line tech staff to outside regulators — must have a high level of confidence in the data and controls you provide through those integrations. In addition to effectively integrating rack-level tools into your broader security and compliance processes from a technical perspective, you must also ensure that both technical and non-technical stakeholders understand how those integrations help them do their respective jobs.

THRESHOLDS OF COMPLEXITY

A third factor that can undermine your rack-level success is complexity. When you implement rack-level controls, you're adding locks, card readers, network connections, video cameras, logging software, and other elements to your environment. That means you're making your environment inherently more complex. This added complexity can be challenging in and of itself — but when piled on top of all the increased complexity occurring in your environment, it can push you past a reasonable threshold.

This complexity can be especially problematic for colocation managers, cloud service providers, and other third-party infrastructure aggregators who must be particularly diligent about segmenting DCIM and related security/compliance activities by client account, and by application or data types. That's why both enterprise and service provider data center managers need to minimize the complexity — as well as the raw cost — of rack-level access control.

FIVE BEST PRACTICES FOR DATA CENTER MANAGERS

Given these obstacles — and the evolving requirements for rack-level control — here are five best practices to consider as you plan your physical security and compliance strategy:

1. MAKE SURE THE HARDWARE AND SOFTWARE YOU IMPLEMENT PROVIDE ALL NECESSARY INTEGRATIONS.

Installation of your new cabinet controls should ideally retrofit easily with existing locks and be plug-and-play with existing rack infrastructure such as rack PDUs. You'll also want support for whatever type of proximity card reading you require (iClass®, MIFARE®, DESFire®, HID® Prox, etc.). And, of course, you'll need software that works with your existing DCIM applications, asset tracking systems, LDAP/AD directory services, etc.

2. APPROPRIATELY WEIGH THE EASE AND FLEXIBILITY OF ADMINISTRATION IN YOUR BUYING CRITERIA.

Given budget pressures, it's easy to be short-sighted about cost — and to, therefore, seek out bargain prices for rack-level equipment, especially in large facilities. That's a mistake. Over the long term, far more of your costs will come from time-consuming, unwieldy administration. Make sure you can streamline that administration with rules-based automation. One suggestion is to use "virtual caging" that allows you to flexibly define groups of racks by attribute, and other time-saving functions. Also, it's recommended to ensure connectivity back to your rack PDU infrastructure to deliver dual networking and power redundancy options without requiring added infrastructure wiring.

3. KEEP IT SIMPLE.

Complexity remains one of the data center manager's most fearsome enemies. And things aren't likely to get any simpler as applications multiply, demand variability increases, and security threats intensify. Do whatever you can to keep things simple. For example, you may want to avoid sourcing parts from multiple vendors. Instead, you may wish to source a complete solution from one of your incumbent vendors to avoid managing yet another supplier relationship.

4. KEEP IT SAFE.

You and your stakeholders need to have the utmost confidence in both the security of rack access controls and the reliability of the compliance-related audit data they capture. Make sure that communication between rack devices and your DCIM console is appropriately protected with AES-256-bit encryption. Also, make sure that your rack controls can continue operating even in the event of a power failure—and that they can generate real-time alerts if someone attempts to tamper with them.

5. AIM FORWARD.

As noted earlier, it's a mistake to take a short-term view of rack-level compliance mandates. Multiple regulatory agencies are addressing a broad range of issues of personal data security and sovereignty. If you only view your objective as checking off an itemized list of current regulatory specs, you're just setting yourself up for more work and spending more down the road. The wiser approach is to build on your existing DCIM foundation to implement technology that empowers you to incrementally increase the granularity of your security and compliance controls over time in response to ever-evolving requirements.

One more tip: You don't have to engage in a complete overhaul of your data center enclosures to start on the road to better rack-level control and audit. A good pilot program on select enclosures can give you the hands-on insight you need to ensure your success when you're ready to execute a complete roll-out.

That's why it's a good idea to start your pilot sooner rather than later. Rack-level access and control will be a requirement. It's simply the next step in the responsible governance of your organization's critical digital infrastructure.

ABOUT RARITAN

Raritan began developing KVM switches for IT professionals to manage servers remotely in 1985. Today, as a brand of Legrand, we are a leading provider of intelligent rack PDUs. Our solutions increase the reliability and intelligence of data centers in the top 10 Fortune 500 technology companies. Learn more at Raritan.com