Raritan®
A brand of legrand®

Rack-Level Security and Compliance

Five Ways to Fulfill Tougher Requirements with Limited Resources

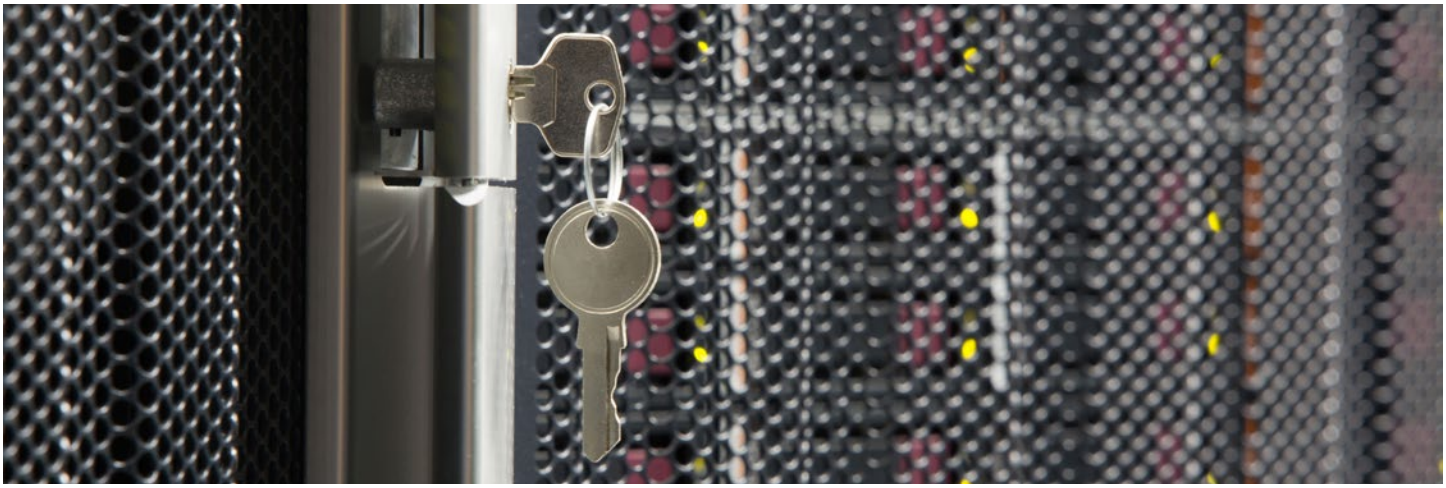
A White Paper from Raritan

Introduction

If you manage an enterprise data center, you face intensifying security and compliance requirements at the rack level. No longer is it sufficient to merely safeguard your data center as a whole with secure, auditable access control at the entrance. 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.

Unfortunately, you don't have unlimited resources with which to fulfill these increasingly stringent rack-level access control requirements. Your capital budget, available cash, staff time, and tolerance for complexity are all finite. So you have to 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, you need control and audit solutions that readily fit into your existing DCIM technology that can leverage your current security. That way, you can cost-effectively add new control and monitoring capabilities at the rack level as required over time — without adding counter-productive friction to the tasks your staff performs every day.



Raising the Bar at the Rack

Once upon a time, it was sufficient to regulate access to the data center as a whole. As long as you could reasonably ensure that no unauthorized personnel had access to your sensitive digital infrastructure — and as long as you could provide proof of those reasonable measures to auditors — you'd be OK.

Times sure have changed. Escalating regulatory requirements across industries now require that sensitive systems and data be subject to their own specific protections. So, as a data center manager, it's no longer enough to ensure that only authorized IT staff enters the data center. You must track and monitor their access to specific sensitive systems and ensure they have the correct rights to 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 is a must.

Of course, the particulars of compliance vary from industry to industry. The mandates outlined by HIPAA are not precisely the same as those in SOX. And the requirements of PCI DSS 3.2 are not precisely the same as those in SSAE 16.

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 can be accurately documented.

Key considerations for rack-level security and compliance may include:

- Enclosure locks that 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 that makes it easy for authorized personnel to quickly gain access to any and all enclosures for which they are authorized.
- In-rack cameras that capture live video and photos automatically tagged with relevant data (time, date, user ID, system data, actions, etc.) for audit documentation and forensics.
- Integration with DCIM and/or other access control systems to facilitate 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/alarming that notifies appropriate parties of problematic events requiring immediate attention.
- PDU integration to ensure continuity of security and compliance even in the event of 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. So it's wise to take a long-term view of your rack-level 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. So when determining how to fulfill your rack-level compliance requirements, you must factor in 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. You also have to consider other factors that will impact how your rack-level implementation will impact your resource-efficiency — including how it will add to your ongoing administrative burdens, whether chronic failures to give the right person access to the right racks at the right time will cost you valuable staff productivity, etc.

Process integrity and confidence

It's also important to recognize that your rack-level controls don't exist in a vacuum. They are part of your data center infrastructure management workflows. They feed into your SIEM analytics and forensics. They support delivery of compliance documentation to your organization's internal and external auditors. They can even play a role in processes you haven't considered yet — 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. So 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 data center managers at colos, 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, as well as by application and/or data types. That's why it's important for both enterprise and service provider data center managers to minimize the complexity — as well as the raw cost — of rack-level access control.

Five Best Practices for Data Center Managers

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

1. Make sure the hardware and software you implement provides 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 PDUs. You'll also want support for whatever type of proximity card reading you require (MiFare®, DESFire®, Tag-it®, Legic®, My-d®, 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 weight 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 cost will come from time-consuming, unwieldy administration. So make sure you can streamline that administration with rules-based automation, "virtual caging" that allows you to flexibly define groups of racks by attribute, and other time-saving functions.

3. Keep it simple.

Complexity continues to be one of the data center manager's most fearsome enemies. And things aren't likely to get any simpler as application multiply, demand variability increases, and security threats intensify. So do whatever you can to keep things simple. For example, you may want to avoid sourcing piece-parts from multiple vendors. You may even want to source a complete solution from one of your incumbent vendors in order to avoid having to manage 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. So make sure that communication between rack devices and your DCIM console are appropriately protected with AES-128 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 big 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. So if you only view your objective as checking off an itemized list of current regulatory specs, you're probably just setting yourself up for more work and more spending further down the road. The wiser approach is to build on your current 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 "boil the ocean" 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 more complete roll-out.

That's why it's a good idea to start your pilot sooner, rather than later. Ultimately, rack-level access and control will be a requirement — not an option — for everyone. 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 9 of the top 10 Fortune 500 technology companies. Learn more at Raritan.com