Life Is On | Schneider Electric

Addressing Cyber Security Concerns of Data Center Remote Monitoring Platforms

White Paper 239

Revision 0

by Torben Karup Nielsen and Patrick Donovan

Executive summary

Digital remote monitoring services provide real-time monitoring and data analytics for data center physical infrastructure systems. These modern cloud-based platforms offer the promise of reduced downtime, reduced mean time to recovery (MTTR), less operations overhead, as well as improved energy efficiency for power and cooling systems. However, with the cost of cyber security crime projected to quadruple over the next few years reaching $2 trillion by 2019[1], there is concern these systems could be a successful avenue of attack for cyber criminals. This paper describes key security aspects of developing and operating digital, cloud-based remote monitoring platforms that keep data private and infrastructure systems secure from attackers. This knowledge of how these platforms should be developed and deployed is helpful when evaluating the merits of remote monitoring vendors and their solutions.

Introduction

Mission-critical information technology (IT) is wholly dependent on the underlying physical infrastructure systems. Not only are these systems fundamental to IT operation, they represent a significant capital and operating expense. This criticality and cost drive a need for monitoring and management of these assets. Data center infrastructure management (DCIM) software tools and remote monitoring services help make IT operations more reliable and efficient by providing proactive notification and a centralized view of all resources, their status, as well as their dependencies on each other.

Remote monitoring services (i.e. monitoring by a 3rd party from outside of the network) have been around for years. Traditionally this service has involved simple intermittent status updates via email broadcasts from the infrastructure systems to those doing the monitoring. These services have evolved into cloud-based, digital (online) services where monitoring is performed in real-time while using IT services such as cloud storage, data analytics, and mobile apps. White Paper 237, *Remote Monitoring and How it Changes Data Center Operations and Maintenance*, further explains this modern type of remote monitoring. These digital monitoring platforms offer the promise of reduced downtime, reduced mean time to recovery (MTTR), less operations overhead, as well as improved energy efficiency for power and cooling systems. Data analytic engines can yield insight not possible with traditional offline monitoring systems. This insight can identify important trends and conditions that can reduce costs and prevent interruptions.

Digital remote monitoring platforms work by having connected data center infrastructure systems send a continuous stream of data about itself to a gateway that forwards it outside the network or to the cloud. This data is then monitored and analyzed by people and data analytic engines. Finally, there is a feedback loop from the monitoring team and systems to the data center operators. The data center operators have access to monitoring dashboards from inside the network via the gateway or to the platform's cloud when outside the network via a mobile app or computer in a remote NOC. **Figure 1** illustrates the basic architecture of a modern digital monitoring platform.

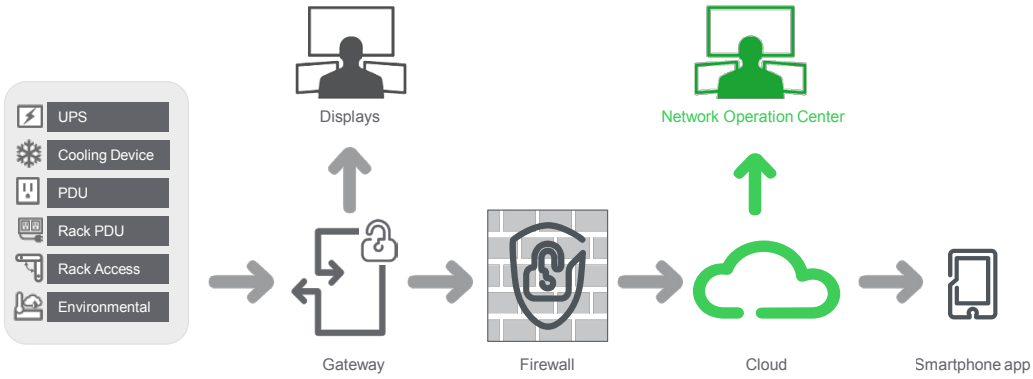

Figure 1
A recommended digital monitoring architecture

With the cost of cyber security crime projected to quadruple over the next few years reaching $2 trillion by 2019[1], there is understandably a concern these externally connected monitoring platforms could be a successful avenue of attack for cyber criminals. Today, cyber security threats are always present and the nature of cyber criminal attacks is constantly evolving. Preventing these attacks from causing theft, loss of data, and system downtime requires a secure monitoring platform and

[1] http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#45018db93bb0

constant vigilance by a dedicated DevOps team. Before selecting and implementing a digital monitoring platform, vendor solutions should be evaluated not just on the basis of features and functions, but also on their ability to protect data and the system from cyber attacks. Knowing how secure a platform is requires an understanding of how it is developed, deployed, and operated. This knowledge will help you evaluate the merits of remote monitoring vendors to better ensure the system and its data is protected once implemented. This paper provides a basic overview of a Secure Development Lifecycle (SDL) process describing how a product should be designed and developed. Additionally, it describes some of the key features and functions specific to digital remote monitoring platforms that help reduce risk of cyber attack. Note that this discussion focuses on the vendor's platform. Equal attention should be paid to the security of the end user's data center and/or its IT network.

Secure Development Life Cycle (SDL)

SDL is a process by which security is considered and evaluated throughout the development lifecycle of products and solutions. It was originally developed and proposed by Microsoft[2]. The use of an SDL process to govern development, deployment, and operation of a monitoring platform is good evidence that the vendor is taking the appropriate measures to ensure security and regulatory compliance. The vendor should be using a process that is consistent with ISO 27034[3].

Figure 2
Key practices of a Secure Development Lifecycle (SDL) process that overlays the software development process

This paper identifies 8 key practices as shown in **Figure 2**. Each is described briefly below. The subsequent sections of this paper highlight specific and key aspects of these practices as it pertains to the development and operation of a digital, cloud-based data center remote monitoring platform.

Train

There should be a continuous training program for employees to design, develop, test, and deploy solutions that are more secure.

Require

The cyber security features and customer security requirements to be included in product development should be enumerated clearly and in detail.

Design

Security architecture documents are produced that follow industry accepted design practices to develop the security features required by the customer. These documents are reviewed and threat models (see **sidebar**[4]) are created to identify, quantify, and address the potential security risks.

Develop

Implementation of the security architecture design into the product follows the detailed design phase and is guided by documentation for best practices and coding standards. A variety of security tools as part of the development process including static, binary, and dynamic analysis of the code should be used.

Threat modeling

The Open Web Application Security Project (OWASP) Foundation describes threat modeling as, "…an approach for analyzing the security of an application. It is a structured approach that enables you to identify, quantify, and address the security risks associated with an application. Threat modeling is not an approach to reviewing code, but it does complement the security code review process. The inclusion of threat modeling in the SDLC can help to ensure that applications are being developed with security built-in from the very beginning. This, combined with the documentation produced as part of the threat modeling process, can give the reviewer a greater understanding of the system. This allows the reviewer to see where the entry points to the application are and the associated threats with each entry point. The concept of threat modeling is not new but there has been a clear mindset change in recent years. Modern threat modeling looks at a system from a potential attacker's perspective, as opposed to a defender's viewpoint. "

[2] https://en.wikipedia.org/wiki/Microsoft_Security_Development_Lifecycle

[3] http://www.iso27001security.com/html/27034.html

[4] https://www.owasp.org/index.php/Application_Threat_Modeling

Verify

Security testing on the product implementation is performed from the perspective of the threat model and ensuring robustness. Regulatory requirements as well as the deployment strategy are included as part of the testing.

Release

Security documentation that defines how to more securely install, commission, maintain, manage, and decommission the product or solutions should be developed. Security artifacts[5] are reviewed against the original requirements and to the security level that was targeted or specified.

Deploy

The project development team or its deployment leader should be available to help train and advise service technicians on how best to install and optimize security features. Service teams should be able to provide help for customers to install, manage, and upgrade products and solutions throughout the life cycle.

Respond

There should be a product "Cyber Emergency Response Team" that manages vulnerabilities and supports customers in the event of a cyber incident. Ideally, this team should be the same group of people that has developed the application. This means that everyone involved knows the product in detail.

Key aspects of secure platform development & deployment

This section describes in more detail some of the key aspects of the SDL practices that are critical for ensuring good cyber security for digital remote monitoring platforms. Understanding if and to what degree a platform embraces these aspects requires discussion with the vendor.

People

A common source or conduit for cyber attack is someone inside the organization or its network. And that person doesn't necessarily have to be a "bad actor". Even a loyal and ethical employee can unwittingly become a conduit for an attack. Since your infrastructure data will be sent to a digital remote monitoring platform, it is important to understand how the vendor handles its staff, both those who develop the platform, as well as those who deploy and operate it. **Table 1** lists key things to look for in terms of how the vendor manages its employees.

[5] Security artifacts are the documented outcomes of the testing performed in the verify phase. Therefore, at this point in the process, you review that your developed application meets the originally required level of security.

Table 1
Conditions and actions to look for in how the vendor manages employees

Vendor Employee Management

Hiring	• Background checks performed on all perspective employees • Ideally, platform operators have data center facility operations experience • Developers have experience with SDL practices
Training & Management	• Mandatory Cyber Security training based on role (developer, operator, field service technician, general employee) • Monitor, track, and report training completion and scoring • On-going, continuous training program to keep up to date • Escalating process for handling security policy violations
IT/Network Access	• Principle of least privilege: users are only given access to IT and network functions/resources needed to perform their job • All users have individually identifiable accounts, which enable full accountability and auditing of system access, use, and changes.

Designing a secure architecture

The digital remote monitoring platform should be designed with cyber security as a top guiding principle. The following points are recommended attributes and best practices for a digital monitoring platform:

Recommended design attributes and best practices for the platform

Outbound connections only	The Gateway that collects customer data within the customer's network should be the only one to initiate connections to the outside: from the gateway to the cloud service. No one outside of the gateway should be able to connect to it first. The gateway cannot be polled without a secure connection first being made by the gateway. Since the gateway does not need to allow inbound connections, this eliminates the gateway as a conduit for attack.
HTTPS	Platform should only use secure Hyper Text Transfer Protocol (HTTPS) to protect the confidentiality and integrity of the data in transit.
Multifactor Authentication	All authentication uses multifactor authentication, e.g. a combination of username/password and a one-time code sent via text message to a verified phone as a second factor, to reduce the risk of stolen credentials being used to access the system. This should also be the case for the vendor's access to the platform, such that a compromise to the vendor's internal network does not allow the attacker to access the remote monitoring platform's data or source code.
Data encryption	Sensitive data should be encrypted while it is at "rest" (i.e., stored on disk or in the cloud) and in motion (e.g., during transmission from the gateway to the cloud service). All user credentials, billing, and order information both at rest and in motion should be encrypted.
Secure source code	Platform's source code should meet current source code compliance standards such as NIST SP 800-53 Rev 4 and DISA STIG 3.9. These standards are endorsed by the U.S. Government at the time of this writing. Compliance is verified using static code (or program) analysis[6]. All code changes should be peer reviewed before being accepted. The process enforces that code cannot be changed without at least two developers accepting the change. Deployment and configuration changes to source code use automation and predefined scripts to reduce the risk of human error.

[6] https://en.wikipedia.org/wiki/Static_program_analysis

Security testing

Security testing is a critical aspect of developing a digital monitoring platform. It is the only way to properly assess the security of the architecture and its design before deployment. Testing begins during the development phase. **Table 2** summarizes the recommended test practices.

Table 2
Security testing for platform development

Recommended testing practices	
Static Code Analysis	Static Code Analysis is a means to identify weaknesses in the source code prior to building and deploying it. All code should be scanned prior to each build to eliminate those issues before the application is developed.
Penetration testing	Penetration testing is a means to discover vulnerabilities by testing the platform and its network just as an attacker would. Testing can be done from the perspective of an external attacker (or Black Box), or from the perspective of an insider (White Box). Test teams should be separate and independent from the development team and specially trained in penetration testing. Sometimes, test providers are external to the company.
Continuous security scans	The platform should be continuously (post deployment) scanned and tested for new vulnerabilities. This should be done using scanning tools that look for publicly known security vulnerabilities.

The role of "DevOps" teams

Remaining vigilant post deployment is important – perhaps even more so than developing a secure product to begin with. Cyber security is a moving target in that the number and type of threats are constantly evolving. In addition to how the platform is designed and developed, the security of a platform is also very dependent on the vendor's ability to detect, react to, and remedy security issues in a timely fashion.

A dedicated DevOps[7] team (see **sidebar**) should be put in place by the vendor that is responsible for maintaining the security of the platform and reacting to any threats once the solution is deployed. This team should have three basic functions:

- **Detect** - The team should perform continuous security scans (as described above) using up-to-date detection tools from reputable vendors. In addition to this, all logs from all system components should be captured and consistently reviewed and monitored for anomalies.
- **React** - DevOps team should offer "24x7" coverage and be capable of being automatically notified of any critical issues by the platform or gateway.
- **Remediation** – With continuous training, monitoring, and testing, including automated tests of functionality and security, DevOps teams should be able to easily and confidently roll out fixes across all environments.

For DevOps, attention is on two key metrics: Mean Time to Detect and Mean Time to Recover, meaning that the team focuses on detecting and subsequently recovering from any issues (security-related or just technical problems) as quickly and efficiently as possible. Note that this is in contrast to a more traditional approach of focusing on Mean Time Between Failures, which is a less helpful metric for a cloud platform, as it says nothing about how quickly issues are resolved. Two areas of

"DevOps"

This term is a shortened compound of "development" and "operations". Wikipedia's definition (see footnote) is, "...a culture, movement or practice that emphasizes the collaboration and communication of both software developers and other information-technology (IT) professionals while automating the process of software delivery and infrastructure changes. It aims at establishing a culture and environment where building, testing, and releasing software, can happen rapidly, frequently, and more reliably." Ideally, in the context of digital remote monitoring platforms, the team should be composed of the platform developers and operators.

[7] https://en.wikipedia.org/wiki/DevOps

focus for DevOps teams influencing these metrics are network security and physical security. Recommended practices are briefly explained.

Network security

DevOps teams need to monitor security for the vendor's platform network at all times. The network of the operating platform needs to be as isolated from the outside world as possible to ensure data is safe and remains private. One effective way to do this is the use of Jump Servers or Hosts. A Jump Server is a hardened and monitored computer that typically includes a local firewall that acts to control access between networks of dissimilar security protocol levels. These hosts are configured with SSH (secure shell), a cryptographic network protocol that protects network data from being intercepted. Using SSL (secure socket layer) certificates ensure that its real owners (i.e., the vendor/owner/provider) of the platform are operating the platform's web pages and dashboards. These certificates will initiate the secure HTTPS internet protocol (described above) using port 443 of the router. This ensures a secure connection between the platform and the user's browser or mobile app. Further, access control lists (ACLs) should be used and kept in the Jump Server to ensure only those who should and need access, have it. In fact, all servers that are part of the cloud platform service should be protected by ACLs. This makes it much more difficult for a potential hacker to use one breached server as a platform to attack others since servers are not "visible" to each other.

Physical security

An important, but often overlooked, element of the DevOps team's responsibility to detect *any* threat, is *physical* security monitoring. Physical security is typically thought of as being the purview of the vendor's facility physical security teams who manage and monitor building access. Some aspects of physical security, however, require management by, or at least cooperation with, IT and the DevOps team. These aspects include people's access to the data center, IT rooms and closets, as well as software development areas. The IT department and DevOps teams also should be responsible for ensuring adversaries are unable to gain access to a computer. To this end, all developers and operators should be required to:

- Secure laptops with disk encryption
- Use a local firewall
- Use a "strong" password
- And enable screen lockouts on a short timeout period

In addition, the vendor's DevOps team should ensure that there are regular, unannounced penetration tests against both the physical and network security of any sites where a cloud platform is developed and operated. And this testing should ideally use third party firms to help ensure unbiased results.

Conclusion

Modern digital monitoring platforms have the great potential to reduce downtime, reduce mean time to recovery (MTTR), ease operations overhead, as well as improve energy efficiency for power and cooling systems. Data analytic engines can yield valuable insight on important trends. However, online, connected monitoring systems could be a potential avenue for attack. With the right development, deployment, and operation practices, however, these cloud-based platforms can be made highly secure. It is important to have in-depth discussions with monitoring vendors to understand if and to what degree these practices are implemented and followed. This knowledge will help make effective sourcing decisions and provide peace of mind once deployed.

About the authors

Torben Karup Nielsen is a Program Manager at Schneider Electric. He has nearly a decade of experience in software development, including several versions of Schneider Electric's award-winning DCIM software suite. During his time at Schneider Electric, Torben has contributed to several white papers, and holds several patents related to software solutions for data center management. Before joining Schneider Electric, Torben comes from a background in theoretical computer science.

Patrick Donovan is a Senior Research Analyst for the Data Center Science Center at Schneider Electric. He has over 20 years of experience developing and supporting critical power and cooling systems for Schneider Electric's IT Business unit including several award-winning power protection, efficiency and availability solutions. An author of numerous white papers, industry articles, and technology assessments, Patrick's research on data center physical infrastructure technologies and markets offers guidance and advice on best practices for planning, designing, and operation of data center facilities.

Resources

Remote Monitoring and How it Changes Data Center Operations and Maintenance
White Paper 233

Browse all
white papers
whitepapers.apc.com

Browse all
TradeOff Tools™
tools.apc.com

Contact us

For feedback and comments about the content of this white paper:

Data Center Science Center
dcsc@schneider-electric.com

If you are a customer and have questions specific to your data center project:

Contact your Schneider Electric representative at
www.apc.com/support/contact/index.cfm