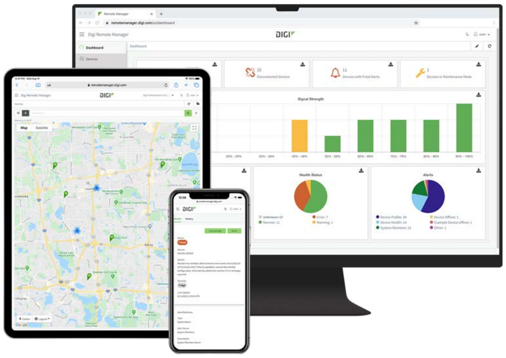
Digi Remote Manager: Security and Compliance Technical Brief

Abstract

Historically, security has oftentimes been an afterthought or a bolt-on to any engineering product. In today's markets, however, security is taking a firm front seat in engineering solution design. Digi International recognizes the crucial nature of security components in our products and services, including Digi Remote Manager® (Digi RM). Indeed, security is at the core of Digi RM and regarded as a critical component to be passed to our customers.

This whitepaper will discuss the standards and controls put in place by Digi's DevSecOps (Development, Security and Operations) team, and answer common security questions. Digi's DevSecOps policies are designed to support customer security frameworks, enabling solutions that meet specific corporate or standard security requirements.



Overview

Security is firmly at the core of every feature developed and every decision that is made regarding Digi Remote Manager. The Digi DevSecOps team fiercely protects the confidentiality, integrity and availability of the Digi RM Service. The extensive Digi RM ecosystem has over 100 different security and operational controls in place that take into account security frameworks, including but not limited to ISO27002's ISMS, NERC CIP (critical infrastructure protection) guidance, Payment Card Industry PCI-DSS v2, the Cloud Security Alliance (CSA) Cloud Controls Matrix, SOC 2 Type 2 as well as relevant HIPAA and NIST standards. Digi RM customers are assured that there is no safer place for their data.

Certifications

Our systems are located in SSAE-16 (SAS-70 Type II) and ISO27001 certified facilities. Digi RM enables you to meet your security compliance targets by providing to your field devices the following security functions: Centralized Device Patching, Capacity Planning, Centralized Logging, Compliance Scanning, Compliance Reporting, Change Control, Backup/Disaster Recovery, Intrusion Detection and Asset Management.

HIPAA/PCI Compliance

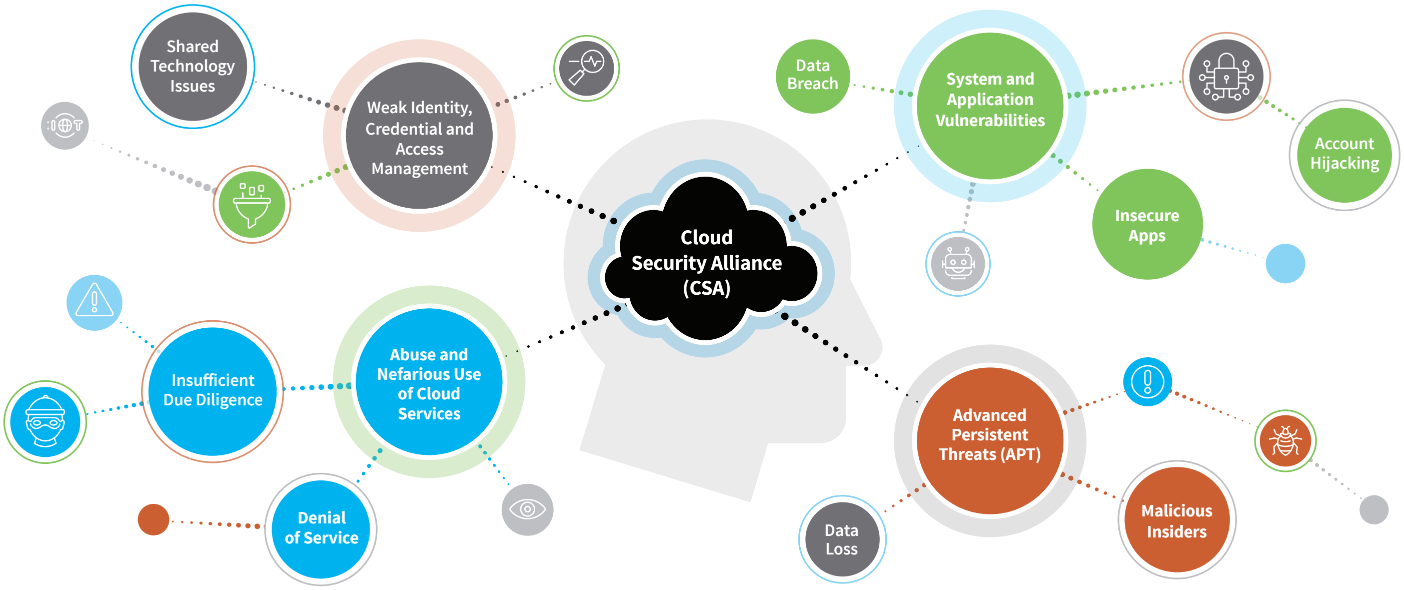
Digi RM is a powerful IoT network management tool that can help organizations achieve compliance with PCI and HIPAA regulations. While Digi RM does not provide direct monitoring of stored data or data encryption, it provides centralized device management and monitoring that can enable organizations to better secure their Digi devices and data. Digi RM can help organizations monitor the status of their Digi devices, apply firmware updates, and ensure that only authorized personnel have access to sensitive data, helping to meet PCI and HIPAA regulations. Digi RM can also integrate with other encryption tools and solutions to further enhance security for IoT devices and data. By providing a comprehensive platform for managing and monitoring Digi devices, Digi RM can help organizations achieve compliance with PCI and HIPAA regulations.

For more information, visit:

www.digi.com

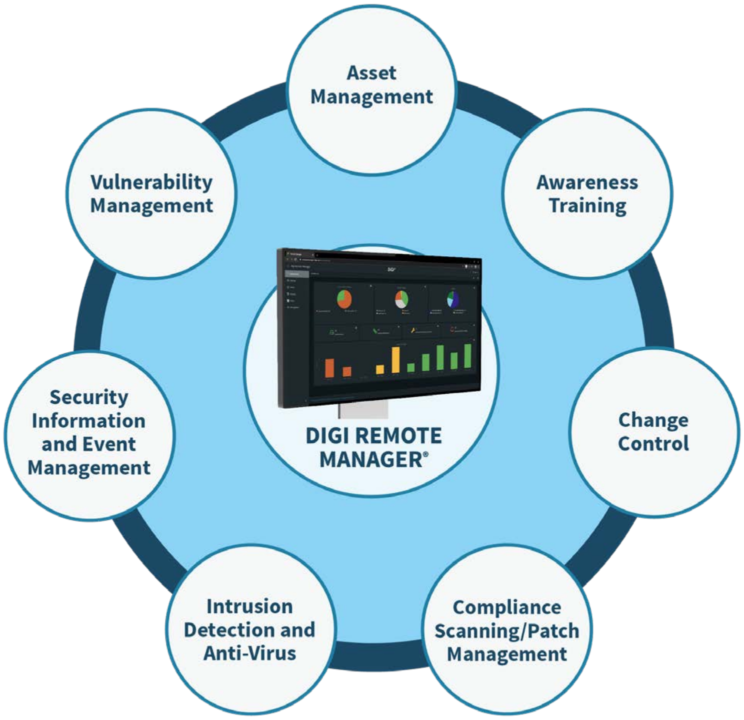
877-912-3444 I 952-912-3444

© 2023 Digi International Inc. All rights reserved.


Shared Technology Issues
Weak Identity, Credential and Access Management
Data Breach
System and Application Vulnerabilities
Account Hijacking
Insecure Apps
Cloud Security Alliance (CSA)
Insufficient Due Diligence
Abuse and Nefarious Use of Cloud Services
Denial of Service
Advanced Persistent Threats (APT)
Malicious Insiders
Data Loss

Digi Remote Manager Security Office Functions

The Digi DevSecOps embraces a continuous improvement program for each security function:


Asset Management
Awareness Training
Change Control
Compliance Scanning/Patch Management
Intrusion Detection and Anti-Virus
Security Information and Event Management
Vulnerability Management
DIGI REMOTE MANAGER®

Security Governance and Compliance

This bi-annual process is conducted to allow verification of compliance with all Digi Remote Manager security policies. This includes such audit checks as user access attestations, as well as contract review processes.

1. Asset Management

To properly identify our scope of controls and configuration compliance, and to understand which function one of our servers does and which data it holds, we track this information with security information and event managers and various state management and detection tools.

2. Awareness Training

All employees and anyone who interacts with Digi Remote Manager undergoes mandatory annual compliance training. The core DevSecOps team that maintains Digi Remote Manager holds daily and weekly meetings to ensure we are trained in every core aspect of the application. The security team holds monthly security guild calls with the whole business to ensure continued awareness and discussions about securing Digi and its product and services.

3. Change Control

All Digi Remote Manager code deployments follow a strict process of change control, where quality assurance processes are validated, and all proper change control functions are tested prior to deployment to production, in order to minimize outages.

4. Compliance Scanning/Patch Management

Digi Remote Manager uses a next-generation software composition analysis tool to ensure continued patch management occurs with every build. In order to stay compliant with our own internal acceptance criteria, our builds will fail upon having detections that reach severity levels that are not acceptable by our DevSecOps team. We use controls to monitor the state of our cloud environment to ensure our environment doesn't deviate from our desired baseline.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

© 2023 Digi International Inc. All rights reserved.

5. Intrusion Detection and Anti-Virus

Digi uses a top-tier product for network intrusion detection and prevention. In conjunction, Digi implements a host-based intrusion detection/prevention system for further detection of security events. This solution is centrally managed and any alerts are centrally alerted via our SIEM solution and investigated.

6. Security Information and Event Management

Logs are collected from the entire Digi Remote Manager infrastructure to include the operating system, firewalls, and intrusion detection systems, as well as the Digi Remote Manager core and applications. This data is centrally fed to a secure SIEM server and saved minimally for one year. An extensive list of active alarms for specific log messages, along with tools to review correlated events between different equipment looking for security attacks on Digi Remote Manager infrastructure and applications ensures peace of mind.

7. Vulnerability Management

Digi RM follows an intensive vulnerability management program. This includes many vendors and layers of testing. Below are the different methodologies of testing and frequency followed. Findings are recorded in a bug tracking system for further review and resolution.

External Infrastructure Yearly Pen Test (Outside Organization)

Digi contracts with a leading vendor to conduct a yearly pen test on Digi Remote Manager systems. All services are tested, along with any common standard protocols for all publically known weaknesses. Web applications and web services for common application weaknesses also use this.

External Application Authenticated Access Continuous Testing (Outside Organization)

Digi contracts with a leading application vulnerability scanning service. This service runs continuously with a credentialed access looking for web application weaknesses in Digi Remote Manager code. Many parts of the automated scan are reviewed and further tested by professional pen testers to validate false positives. This service alerts Digi RM to any immediate vulnerabilities.

Internal Infrastructure Automated Scanning Testing (Internal)

Digi RM uses vulnerability scanners to look for and detect open ports, and other services that may be vulnerable to attack. This scan runs on a weekly basis.

Internal Infrastructure Pen Test (Internal)

Digi RM uses dynamic API testers and fuzzers and other tools that are commonly contained on the Kali Linux distributions for internal pen testing. This testing occurs during the QA process for major releases, as well as on an ad-hoc basis.

Code Reviews

All developers for Digi RM code have a peer review process that allows them to validate each other's work. The code for all of Digi RM is run through static, dynamic, and software composition tools that work in conjunction with the NIST vulnerability database.

Start your **90-DAY FREE TRIAL**
of Digi Remote Manager **PREMIER** Edition

Connect with Digi

- Contact us to talk to a Digi expert.
- Sign up for our newsletter to learn about emerging trends and new solutions.
- Shop for solutions from Digi and our partners.

For more information, visit:
www.digi.com
877-912-3444 | 952-912-3444

© 2023 Digi International Inc. All rights reserved.