A Secure Partner for the Connected World

Built-in Security for Branch, Mobile & IoT Networks

Overview

Network security is a top business imperative today. Companies need to connect more people, places, and things than ever before, and users need to be able to access critical data and applications from anywhere. Many enterprises are turning to cloud-delivered networks and best-in-breed threat management solutions. However, there are serious security implications associated with choosing network and cloud solutions that are either lacking in security maturity or overexposed to vulnerabilities.

Third-party security questionnaires and vendor security checklists can be effective tools to vet potential solutions providers. These questionnaires often focus on the following factors:

- Industry certifications and compliance
- Existing, known vulnerabilities
- Third-party security analysis and penetration testing
- Authentication and encryption practices

This white paper explains Cradlepoint's security posture and offers an overview of the security processes built into the solution development process. It also demonstrates why Cradlepoint's security culture and maturity level make it a trusted partner for thousands of organizations across the globe whose IT teams are charged with deploying LTE-enabled networks that will stay online and secure now and into the future.

Foundational Security: Secure Coding & Development

Security is at the foundation of Cradlepoint's solutions — it's not an afterthought to developing better features or scaling our business. Instead, it informs the development process from the beginning. Cradlepoint also utilizes frameworks that ensure full evaluation of potential security risk and exposure at every stage of solution development. The ethos guiding the Cradlepoint development process dictates that security maturity should outpace the company's scale and our solutions' potential exposures.

Security-Focused Developers

Cradlepoint consciously chooses to recruit developers who are particularly well versed in hacking techniques like cross-site scripting, cross-site requested forgery, and SQL injection. They have expertise in reverse engineering memory scraping and other Point-of-Sale-focused malware. Of course, Cradlepoint developers utilize static and dynamic analysis and code reviews during the development process.

Independent, Third-Party Evaluation

Cradlepoint validates all development with independent, third party vulnerability assessment and conduct manual pen testing on devices, firmware, NetCloud Manager, and NetCloud Perimeter annually.

While no code can be 100 percent perfect, approaching coding with a security-first mindset is critical in today's computing and networking environment.

Cradlepoint Security Philosophy:

Maturity should outpace scale and potential exposures.

Building a More Secure World

cloud CSA security alliance®

Cradlepoint is a proud member of the Cloud Security Alliance, investing in helping shape the future of IT and in making the cloud safer. Cradlepoint has implemented the CSA Cloud Control Matrix as a framework for cloud security.

- Cloud Security Alliance Membership
- PCI Security Standards Council Participating Organizations
- No open vulnerabilities, no public exploits

"Cradlepoint's uses of the Cloud Control Matrix as a framework ensures customers and partners that Cradlepoint solutions are secure and aligned with the industry's most current standards."

Jim Reavis,
CEO, Cloud Service

Incident Response: Security Culture in Action

At Cradlepoint, actions speak louder than words. While the Heartbleed vulnerability was discovered in 2014 and is now firmly in most organizations' rearview mirror, it's one of the most memorable SSL exposures ever. Cradlepoint's response to the discovery shows what sets the company apart when it comes to prioritizing customers and their security.

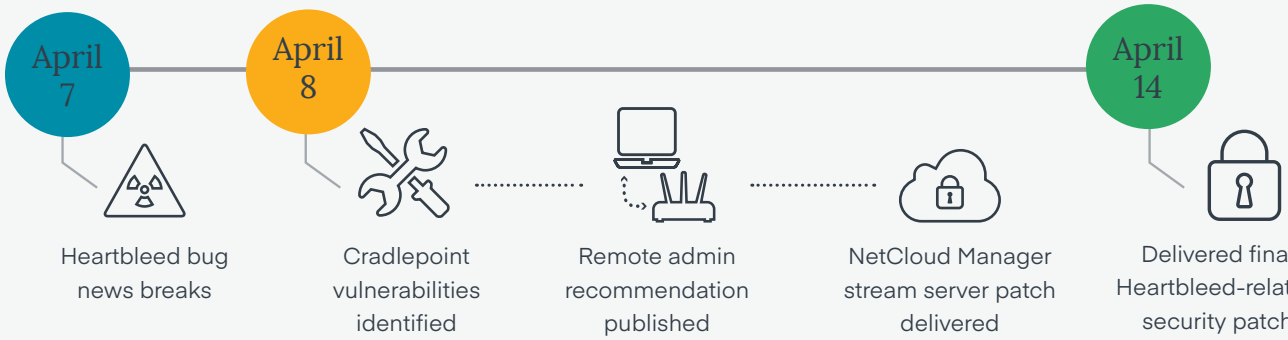
When news of the Heartbleed bug broke — and as it became apparent how serious and widespread the problem was—Cradlepoint's response team immediately started the process of finding and resolving any correlated vulnerabilities in Cradlepoint solutions. The abundance of national headlines about Heartbleed meant Cradlepoint needed to reassure its customers.

With that in mind, the response team moved quickly and thoroughly to evaluate Cradlepoint solutions, pulling developers off of new product enhancements and version upgrades, fully utilizing internal resources to address the exposure. The evaluation revealed an exposure risk under a certain combination of conditions. Cradlepoint moved quickly to publish a KnowledgeBase article on the vulnerability the next day, suggesting that users disable remote admin capabilities while a firmware update was in development. The response team also developed a patch for NetCloud Manager stream servers that same day.

By day seven, the response team delivered an update for the remote admin issue, made possible both by the secure foundation of Cradlepoint solutions and the development team's dedication to protecting customers as quickly as possible. This is compared to the month or longer that it took a number of other solution providers to deliver updates.

Perhaps most importantly, Cradlepoint saw a high uptake of the Heartbleed patch among customers, made possible by the ease with which Cradlepoint's NetCloud platform allows remotely deployed routers to be updated. NetCloud Manager eliminates the need to access and update each router individually; IT admins can group routers together and remotely execute firmware upgrades across every router in the group at once. During this period, Cradlepoint made NetCloud Manager free for 30 days so all customers could update their devices as quickly as possible.

Timeline of incident response



Internal Security Controls

Helping customers stay secure starts with upholding the highest levels of corporate security.

Encryption

Internally, Cradlepoint uses AES 256 to encrypt Cloud Administrator passwords. AES 256 is the worldwide standard in encryption for software, firmware, and hardware, specified and recommended by the National Institute of Science and Technology (NIST). With AES, no password or login IDs are delivered as clear text. All customer data is encrypted at rest.

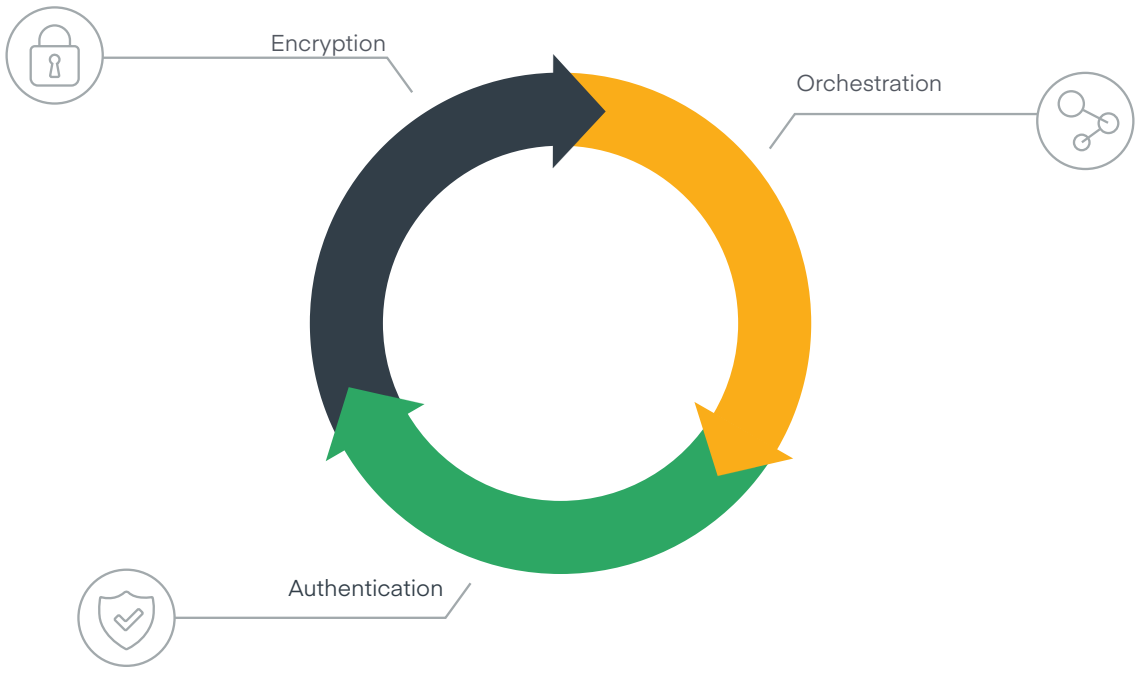
Orchestration

Cradlepoint utilizes Amazon AWS cloud facilities for auditing and orchestration in order to standardize platform configuration.

Authentication

Remote access to the AWS console requires multi-factor authentication.

Access to production infrastructure is limited to DevOps engineers from the Cradlepoint network. Systems are automatically monitored every 15 minutes to ensure the secure configuration is maintained. In the event the configuration has changed, the system automatically reverts back to the desired secure state.



Cradlepoint's Security Vulnerabilities Policy

Cradlepoint recognizes the importance of security and privacy for our customers, partners, and employees, and takes security issues very seriously. As such, we are committed to reporting and addressing security issues in a timely and proactive manner in order to offer the greatest level of protection. Whether you're a user of Cradlepoint solutions, a Cradlepoint employee, a software developer or a security specialist, you're an important part of this process. Cradlepoint is committed to a transparent process in how it reacts to potential vulnerabilities.

The Cradlepoint vulnerability process flow includes these key points:

- Cradlepoint is committed to communicating and working in a timely manner for any reported security vulnerability from an employee, customer, partner, or outside party.
- Cradlepoint recommends submitters of vulnerabilities to follow our responsible disclosure process to minimize the risk to all customers and users of our technology.
- To submit a vulnerability send an email to security@cradlepoint.com with the following information:

    1. Product & NCOS versions
    2. Steps taken to expose vulnerability
    3. Contact information & preferences
    4. Copies of screen shots, code snippets, and/or logs that might be helpful

- Cradlepoint follows a responsible disclosure process for communicating vulnerabilities. As such, we will first privately notify customers and partners before any public disclosure in order to minimize risk to customers from exploitation of vulnerabilities. The private disclosure includes details for the risk, severity, remediation steps, and/or fixes.
- The method for publicly disclosing vulnerabilities may vary, but it will include a post to the Cradlepoint Trust Page and may include email or in-product alerts to affected users.
- Questions about Cradlepoint's vulnerability notification policy as well as other security related issues can be sent to security@cradlepoint.com.

About Cradlepoint

Cradlepoint is the global leader in cloud-delivered wireless edge solutions for branch, mobile, and IoT networks. The Cradlepoint Elastic Edge™ vision—powered by NetCloud services—provides a blueprint for agile, pervasive, and software-driven wireless WANs that leverage 4G and 5G services to connect people, places, and things everywhere with resiliency, security, and control.

More than 27,000 enterprise and government organizations around the world, including 75 percent of the world's top retailers, 50 percent of the Fortune 100, and first responders in 10 of the largest U.S. cities, rely on Cradlepoint to keep critical branches, points of commerce, field forces, vehicles, and IoT devices always connected and protected. Major service providers use Cradlepoint wireless solutions as the foundation for innovative managed network services. Founded in 2006, Cradlepoint is a privately held company headquartered in Boise, Idaho, with a development center in Silicon Valley and international offices in the UK and Australia.

To learn more visit cradlepoint.com.