ZPE Systems

The Nodegrid OS and ZPE Cloud achieve the industry's highest security level with Black Duck

Company Overview

ZPE Systems, a leader in the critical infrastructure automation industry, delivers out-of-band management and automation infrastructure with the highest level of security. Six of the ten top global tech giants trust ZPE Systems' hardware and software infrastructure for management, remote access, and automation of critical systems, from data center to edge.

Its high standards have led ZPE Systems to partner with Black Duck to ensure the highest level of code quality and security by following software development life cycle (SDLC) best practices using Black Duck application security testing (AST) solutions that include Coverity® Static Analysis, Black Duck Binary Analysis, Black Duck SCA, and Black Duck Continuous Dynamic.

The challenge: Addressing security across the software development life cycle

"Security is the cornerstone of ZPE's infrastructure management solutions," said Koroush Saraf, vice president of product management and marketing at ZPE Systems. "Our automation platform touches every aspect of our customers critical infrastructure, from networking and firewall gear to servers, smart PDUs, and everything else in their production network. The ZPE portfolio is architected with the strongest security and implemented with the same level of scrutiny."

Given the critical nature of enterprise networking, security is paramount to ZPE customers.

"The average time taken to apply patches and fix vulnerabilities can be more than 205 days," said Saraf. "This is due to many reasons: limited resources and time, concerns that something may break, or in some cases, admins don't even know that a critical patch is available. That's why ZPE takes on the responsibility for customers. They're assured that the systems running their infrastructure are running the latest, most secure software. And if a patch fails, our built-in undo button reverts to a safe configuration before any damage can be done."

Saraf added, "Like with all modern organizations, ZPE uses a complex mix of proprietary, open source, and third-party software obtained through a variety of sources from the software supply chain. Think third-party libraries, packaged software from ISVs, IoT and embedded firmware, and especially open source components. In fact, studies show that over three-quarters of the code in any given application is likely to be open source."

"Most third parties won't provide the source code behind their software," noted Saraf. "But the question remains whether that supplier is as security-conscious as ZPE. Again, we found the solution with Black Duck, which gives us insight into any third-party software we include without requiring access to the source code."

The solution: Building comprehensive security testing with Black Duck AST

As Saraf noted, different security solutions focus on different aspects of vulnerability detection and risk mitigation. By layering multiple solutions such as static analysis, dynamic analysis, and software composition analysis, ZPE covers a wide range of potential vulnerabilities, ensuring that code quality and security issues are identified at various stages during the software development life cycle and across different types of code.

Coverity provides the speed, ease of use, accuracy, industry standards compliance, and scalability to develop high-quality, secure applications. Coverity identifies critical quality defects and security vulnerabilities as code is written, early in ZPE's development process when they are easiest to fix. Coverity seamlessly integrates automated security testing into CI/CD pipelines, supports existing development tools and workflows, and can be deployed either on-premises or in the cloud.

Continuous Dynamic is a software-as-a-service dynamic application security testing solution that allows businesses to quickly deploy a scalable web security program. No matter how many websites or how often they change, Continuous Dynamic can scale to meet any demand. It provides security and development teams with fast, accurate, and continuous vulnerability assessments of applications in QA and production, applying the same techniques hackers use to find weaknesses This enables ZPE to streamline the remediation process, prioritize vulnerabilities based on severity and threat, and focus on remediation and its overall security posture.

Black Duck helps ZPE identify supply chain security and license risks even when it doesn't have access to the underlying software's code. This is a critical security tool for the modern software supply chain. Black Duck Binary Analysis can scan virtually any software, including desktop and mobile applications, third-party libraries, packaged software, and embedded system firmware. It quickly generates a complete Software Bill of Materials (SBOM), which tracks third-party and open source components, and identifies known security vulnerabilities, associated licenses, and code quality risks.

The result: A notable reduction of CVEs

"One of the outcomes from taking a comprehensive, layered approach to security testing has been a notable reduction in CVEs on the systems we deploy," said Saraf.

"I think a lot of industry players don't give enough attention to patching CVEs. They wait until after a security incident, or until a customer specifically asks. Unfortunately, it's normal to see unpatched, outdated software running on critical infrastructure. The Equifax breach of 2017 is just one example that exposed the personal data of millions. It's a particular problem with IoT and embedded devices—many of those systems get installed and forgotten. But it's another attack surface, especially if you use the equipment for critical infrastructure automation."

"ZPE's goal is to reduce the attack surface of our systems to as close to zero as possible, either by making sure that software vulnerabilities are identified and addressed, and that our software is running the most secure and up to date versions. It's an ongoing process—what is vulnerability-free today won't necessarily be so tomorrow—which is why ZPE always stays security-conscious. I think the company's commitment to security has positioned ZPE as a trusted partner for enterprises seeking secure automation solutions for their critical infrastructure needs."

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.