Customer Case Study

Telecom Service Provider Chooses Vdoo to Assess Security of Edge Devices

The Need

For an industry leading communications service provider (CSP) with cutting-edge network infrastructure and a strong cybersecurity mindset, the ability to see and manage security risks affecting its network, including vulnerabilities in its software supply chain, is of paramount importance.

The service provider's investment in advancing its infrastructure and service offerings continually introduces new challenges in ensuring service performance and resilience, and new sources of cybersecurity risk. Notably, with 5G mobile networking as one of its key strategic initiatives, enabling machine-to-machine communications and IoT implementations at enterprise scale, the service provider needs to facilitate secure connectivity between a far greater volume and diversity of devices at the network edge.

Enhancing Third-Party Product Security Validation

The service provider acquires many edge devices, such as cellular modems, routers, set-top boxes, and smart home appliances from third-party OEM vendors. Validating the security of these devices is critical for the service provider's customers' security, as they enable access to the customer's home or business network and a plethora of sensitive data. The CSP's own network security posture is also at stake - an attacker can potentially exploit a vulnerable device to penetrate the core network and impact network stability and performance, causing severe financial and brand reputation damage.

Before externally sourced devices are connected to the service provider's network and in customer's premises, an internal security team is charged with performing thorough product security reviews to validate that those devices are secure. The team uses a mix of automated analysis tools and manual testing methods to independently gain a comprehensive view of device cybersecurity issues, and works with the OEM vendors to ensure the needed fixes are implemented.

About the Customer

- Tier- 1 telecommunications service provider
- Serves millions of consumers and business customers
- Delivers fixed and mobile voice, internet, TV and additional value-added services
- Faces increasing cybersecurity risk as their network infrastructure expands with more edge and IoT devices

To achieve high security at scale, the security team was seeking to streamline product security practices to effectively uncover, communicate, prioritize and address security issues that lead to actual risk. They have been on the lookout for technology solutions that provide:

- **Accurate and comprehensive** security findings
- **High manageability** with user-friendly reporting and interfaces
- **Fast and efficient** security issue discovery and resolution
- **Full lifecycle** product security capabilities including post-deployment monitoring

The Challenges

The service provider works with multiple OEM vendors to acquire a broad range of edge and IoT devices. While the security team routinely demands static code analysis reports from their vendors prior to deployment, which gives some assurance as to the products' security posture, they have also been expending significant effort vetting their software supply chain security by performing their own analysis of device firmware images they get from vendors as binaries. They employ a combination of internal analysis using multiple tools and work with external testing labs to validate compliance with their security requirements. These difficult and resource-intensive processes have made it hard to consistently enforce their security standards at scale across hundreds of externally sourced products.

Beyond identifying security gaps, the team has also been consuming a great deal of time and resources processing and responding to the findings. Complex tasks include investigating results from multiple sources to pinpoint true security risks and weed out false positives, and preparing relevant information to communicate with other groups internally such as engineering, compliance, and management, as well as externally with their OEM vendors.

Lastly, to maintain the company's strong security posture and reduce risk, the team has been proactively seeking methods to expand their coverage of potential threats in the most effective manner. This has required continual efforts to keep up with evolving attack methods and new vulnerabilities originating from third-party products that connect to the service provider's network, both before and after they are deployed.

Streamlining and Automating Security Validation with Vdoo

Looking for ways to improve the efficiency and coverage of their product security validation methods, their security team decided to start using the Vdoo automated product security platform. The customer has recently started using the platform and so far analyzed the software images of over 80 products supplied by more than 30 vendors.

Vdoo delivers an out-of-the-box SaaS platform that requires no setup, so the team immediately started running automated analysis scans of their binary artifacts. They analyzed varied device software images and obtained comprehensive results within minutes, including a detailed software bill-of-materials (SBOM), CVEs, zero-day vulnerabilities, configuration issues, security malpractices, malicious files, and more.

Comparing the information provided by Vdoo with their existing tools, they found that Vdoo produced higher accuracy and coverage of security issues. In addition, Vdoo provided more thorough and meaningful prioritization, resolution, and standards compliance guidance, enabling efficient handling of the issues that have actual security and risk impact.

In addition to quickly uncovering security gaps, the team appreciated the intuitive interface and the ability to easily share information with OEM vendors through the platform's web-based interface, to facilitate fast resolution of their high-priority issues. Information shared includes details on the issues found and easy-to-follow remediation and mitigation guidance. This enabled the service provider to both build more transparent relationships with suppliers and streamline enforcement of their product security requirements. Soon after the service provider started sending the security results and guidance, a number of OEMs have approached Vdoo in order to integrate the platform into their SDLC and release processes so that they can proactively align with the security standards and testing applied by the CSP pre-deployment.

Finally, Vdoo provides the security team additional capabilities to support their product security management efforts post-deployment, facilitating fast detection and response to new threats. Beyond point-in-time automated security analysis, the team receives continuous alerts on new vulnerabilities and threats affecting previously scanned artifacts, as well as the option to create automatically tailored agents that enable alerting on product security events and active prevention of suspicious activities.

Benefits Gained from Using the Vdoo Platform

Supply chain security at scale

The ability to automatically analyze software images in binary form without access to source code provides the security team independent vetting capability they can easily implement as part of their product security management processes. This capability can be scaled to hundreds of devices, delivering high-quality results without manual effort or expensive external testing services.

Improved efficiency and speed

The security team obtains fast access to highly accurate and relevant findings, including the prioritization and mitigation guidance needed to efficiently address the issues that have actual risk impact, as well as the ability to easily share results with vendors for fast resolution.

Reduced risk

Leveraging rich domain expertise in embedded software security, Vdoo provides deep visibility into third-party product security issues including CVEs, zero-days, malware, and configuration and hardening issues, as well as continuous security capabilities to protect against new vulnerabilities and attack attempts post-deployment, reducing the risk of software supply chain attacks on the service provider's network.

About Vdoo

Vdoo is a global leader in the complex and increasingly-critical product security space. With Vdoo, organizations can identify, prioritize, and mitigate a vast range of security issues. As the only automated platform that provides end-to-end product security, Vdoo helps development and security teams reduce time and effort while ensuring optimal product security. The platform addresses a diverse variety of security risks including supply chain threats, configuration risks, standard compliance, zero-day vulnerabilities, and more. Founded in 2017 by a team of seasoned cybersecurity entrepreneurs and product security experts, Vdoo is now a global company with offices in Israel, US, Germany, Singapore, Japan, and dozens of Fortune 500 customers representing the most security-diligent companies from various industries.

For additional information, please contact us at info@vdoo.com or visit our website at vdoo.com

vdoo