HostedNetwork

ProjectGuardian Use Cases

Helping MSPs Safeguard Networks and Strengthen Client Trust

Project Guardian is an innovative, free vulnerability notification tool built specifically for MSPs by Hosted Network. It empowers you to stay ahead of potential risks by detecting vulnerabilities, open ports, and high-risk services in your clients' systems.

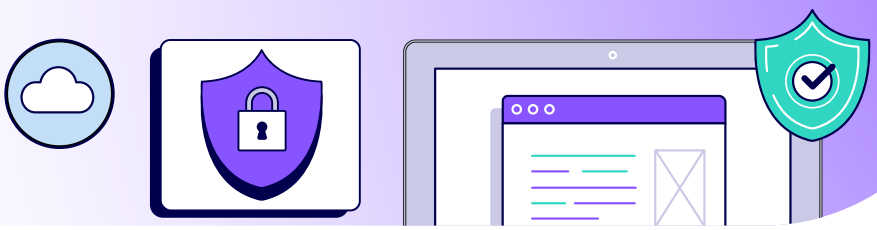
With real-time alerts, expert remediation recommendations, and detailed compliance logs, Project Guardian streamlines your ability to identify and resolve issues efficiently—helping you maintain trust, meet compliance requirements, and position your MSP as a proactive, security-first partner.

The real world examples covered in this Use Case include:

- **Unmonitored devices**
- **Outdated software configurations**
- **Decommissioned servers left active**

How Project Guardian helps MSPs

Fortinet Firewall Oversight: Saving Clients from Security Blind Spots



The Challenge

An MSP specialising in Fortinet solutions faced a serious oversight that could have led to a catastrophic outcome. During a routine audit, it was discovered that two devices had been excluded from their centralised management system due to a human error. These devices, connected to the network but unmonitored, created blind spots that could be exploited by attackers. This issue was especially concerning as the MSP's clients included major brands with high compliance and security expectations.

The Solution

Project Guardian stepped in to provide a lifeline to the MSP. The tool proactively scanned the network and flagged the overlooked devices, identifying the specific vulnerabilities and their severity. Armed with detailed, actionable insights from Project Guardian, the MSP quickly implemented patches and re-integrated the devices into their centralised system. Hosted Network's expert team supported the MSP throughout the process, ensuring the solutions were deployed efficiently without any disruption to the client's operations.

The Impact

By resolving the vulnerabilities in time, the MSP was able to avoid potentially devastating security breaches that could have cost their major brand clients both money and reputation. The proactive detection ensured that their clients' trust in their services remained intact, while the MSP showcased its ability to manage complex IT environments effectively. Thanks to Project Guardian, the MSP turned a potentially damaging oversight into an opportunity to reinforce its position as a security-first provider.

Third-Party CCTV Risk: Securing a Dental Practice's Network

The Challenge

A dental practice managed by another MSP was unknowingly exposed to a serious security threat. The issue stemmed from a third-party CCTV system installed at the practice, which contained vulnerabilities that left the entire network open to potential attacks. The system, managed independently by the CCTV provider, had outdated configurations that the MSP wasn't initially aware of, putting patient data and operational continuity at risk.

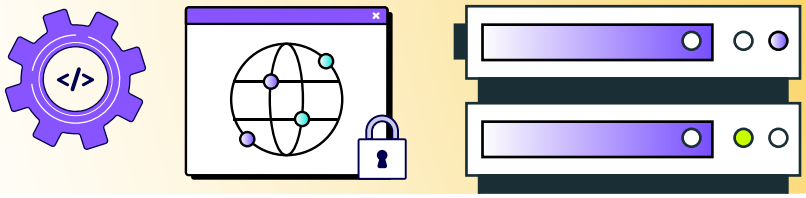
The Solution

Using Project Guardian, the MSP conducted a thorough analysis of the network and quickly detected the vulnerabilities in the CCTV system. The tool identified specific weak points, such as open ports and a lack of access controls, which were flagged as high-risk areas. Guided by Project Guardian's insights, the MSP implemented Unified Threat Management (UTM) policies, restricting access to the CCTV system via a whitelist of approved IP addresses. Hosted Network also provided additional support to ensure the changes didn't impact the dental practice's daily operations.

The Impact

The swift action taken by the MSP eliminated the network vulnerabilities before they could be exploited. The dental practice's network was secured, patient data was protected, and the risk of reputational damage was averted. Moreover, the MSP strengthened its relationship with the client, demonstrating its ability to go above and beyond to ensure security. This incident also highlighted the importance of Project Guardian as a proactive tool that could identify issues even in third-party systems, giving MSPs a competitive edge by enabling them to deliver enhanced protection for their clients.

Undecommissioned Exchange Server: Preventing a Major Security Breach



The Challenge

An MSP faced a hidden threat when an old on-premises Exchange server was accidentally left active after a client migrated to Microsoft 365. This decommissioned server continued forwarding ports, creating a significant vulnerability that exposed the client's network to potential attacks. Since the server was no longer in regular use, the issue had gone unnoticed, leaving the client's data and systems at risk. As the client depended on uninterrupted network operations for critical business processes, resolving the issue before it escalated was crucial to prevent financial and reputational damage.

The Solution

Project Guardian identified the vulnerability during a routine network scan and flagged the issue for immediate attention. The tool provided detailed information about the exposed server, including the specific ports that were still open and the associated risks. Armed with this data, the MSP moved swiftly to deactivate the server, close the open ports, and ensure the network was no longer exposed. Hosted Network's team worked closely with the MSP to validate the solution, providing additional peace of mind that the problem had been fully resolved.

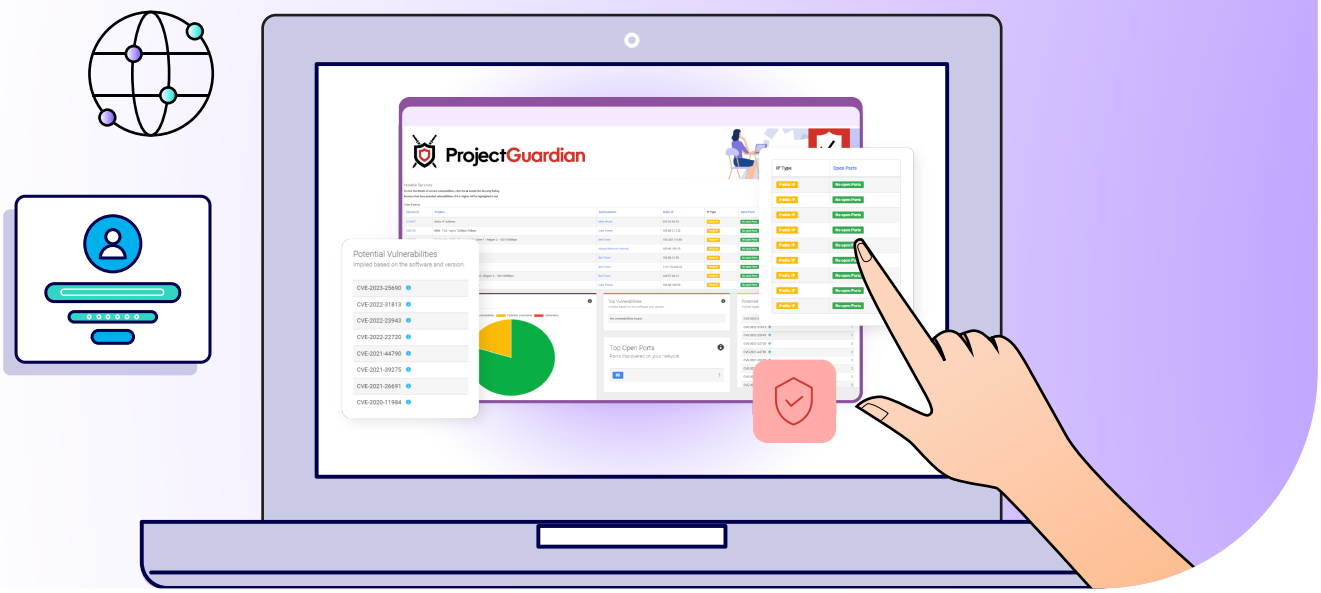
The Impact

The timely detection and resolution of the issue prevented what could have been a costly and damaging breach for the client. By addressing the vulnerability before any harm was done, the MSP not only protected the client's data and operations but also reinforced its reputation as a proactive and reliable service provider. The incident showcased the value of Project Guardian as a tool that could identify hidden risks and prevent them from becoming serious problems. For the client, the experience reinforced their trust in the MSP's ability to deliver exceptional security and IT management services.

Why Choose Hosted Network and Project Guardian?

At Hosted Network, we're dedicated to empowering MSPs with tools that make a real difference. Project Guardian gives you clear insights into system vulnerabilities at no additional cost, saving you time through automated notifications and expert guidance. By helping you address issues proactively, it strengthens your reputation as a trusted partner for your clients.

Designed specifically for MSPs, Project Guardian simplifies risk management and ensures you deliver exceptional service every step of the way.



Ready to take the next step in your MSP's cyber security journey?

To learn more about Project Guardian and Hosted Network, get in touch with us via phone at **1300 781 148** or email us at **sales@hostednetwork.com.au**