vicarius

CASE STUDIES

EL AL Airlines finds a clear flight path to Patch Compliance with Vicarius

General info

EL AL Airlines, Israel's national carrier operating global 24×6 infrastructure, transformed its patch management by replacing rigid, manual tools with Vicarius. Facing limited visibility, inflexible scheduling, and compliance gaps across 500 Windows and 250 Linux servers, the IT team cut patch planning from a full-time job to a single day. Vicarius provided unified coverage, automation, and real-time compliance visibility, driving 98% monthly server coverage and a 95% reduction in manual effort. Tasks like SSL certificate swaps and reboots are now automated at scale.

INDUSTRY

Airline

COMPANY SIZE

~6000

KEY FEATURE

- Unified Patch Management
- Compliance Visibility & Auditing
- Automated System Actions

SUB-INDUSTRY

- Commercial Aviation

“Within two weeks we decided on Vicarius. Patch scheduling is now a one-day task instead of a full-time job.”
Tal Shachar – Deputy Director, Infrastructure, EL AL Airlines

Challenges

- Rigid SCCM maintenance windows
- No unified solution for 500 Windows and 250 Linux servers across 55 global sites
- Third-party application patches were slow and manual
- Lack of visibility left critical servers unpatched, hurting PCI and NIS2 compliance
- Patch manager spent most of each month wrestling with schedules and reboots

Results With Vicarius

- Robust, flexible patch windows eliminate service disruption during 24×6 operations
- Single console covers Windows, Linux, and soon macOS with full compliance visibility
- Patch compliance measurable and auditing ready → monthly 98 % server coverage
- 95 % reduction in manual effort: one administrator now plans updates in one day
- Script automation enables fleet-wide SSL certificate swaps, reboots, and software removal in minutes

About EL AL

As Israel’s flagship carrier, EL AL operates a complex 24×6 infrastructure supporting ~6,000 employees and customers in 55 locations around the world. Based out of Ben Gurion Airport, the airline's systems must remain operational at all times.

Security and Operations Challenges

Tal Shachar, Deputy Director of Infrastructure at EL AL, leads five key areas: systems (Windows/Linux/cloud), storage and backup, monitoring, DBA, and help desk. When his team received vulnerability assessments from the InfoSec team, they were responsible for executing the patching and remediation an effort that had become increasingly unsustainable.

EL AL relied on SCCM for Windows patching and Satellite for Linux. But these tools were inflexible. The lack of robust scheduling options created could result in a mistimed reboot and could disrupt operational systems.Third-party patching was even worse. There was no centralized mechanism to manage non-Microsoft updates. As Tal described it, “It was causing chaos.”And the biggest issue? Visibility. “We didn’t even know which servers weren’t getting patched,” he explained. “We had no real insight. That hurt our ability to comply with regulations like PCI and NIST 2.”

“Within two weeks we decided on Vicarius. Patch scheduling is now a one-day task instead of a full-time job.”
Tal Shachar – Deputy Director, Infrastructure, EL AL Airlines

Why Vicarius

Tal needed a solution that could cover both Windows and Linux, deliver clear visibility, and respect EL AL’s strict maintenance windows. When Vicarius was introduced via reseller Wise Group, the evaluation moved fast.

> *“It was an easy decision,” Tal said. “Within two weeks, we had the proof we needed. Vicarius gave us full visibility, flexible scheduling, and powerful automation in one platform.”*

From POC to Production

The POC process was simple. Vicarius agents were distributed via SCCM for Windows, and by script for Linux. A proxy server was set up on-prem, so no production servers needed direct internet access. After one week of testing, Tal’s team rolled Vicarius out across the entire infrastructure.

The result? “We used to spend all month planning patches. Now it’s a one-day job.”

Operational Benefits

Visibility that Drives Compliance

For the first time, the infrastructure and InfoSec teams had unified, real-time visibility into patch status. This allowed EL AL to show auditors a clear compliance story critical for maintaining cyber insurance and regulatory certification.

When a new CVE hits, the InfoSec team can immediately assess its relevance. “We used to treat all high CVSS scores as urgent. Now we have context. If it doesn’t impact our systems, we wait for the next window. That’s huge.”

Patching and Beyond

Vicarius brought relief beyond traditional patching. Using Vicarius’s built-in scripting engine, Tal’s team automated the replacement of SSL certificates across 150 servers. “It would have taken days,” Tal said. “We did it in one click.”

Reboots, software uninstalls, mass actions all are now orchestrated centrally, without jumping through SCCM hoops or logging into dozens of machines.

Team Efficiency

Tal estimates a 95% reduction in patch-related overhead. The administrator who once wrestled SCCM full-time now spends a single day scheduling updates and spends the rest of the month on strategic initiatives.

Looking Ahead

EL AL plans to extend Vicarius to its Mac endpoints, and as its security team matures, use features like network scanning and more advanced automation. “It’s not just a patch tool,” Tal said. “It’s a platform.”

Final Thoughts

“Vicarius is simple, powerful, and easy to use,” Tal said. “It gave us back time, visibility, and control.”

Key Takeaways

- **Flexibility safeguards revenue:** precise window patching.
- **Unified coverage:** Windows, Linux, and soon macOS under one roof.
- **Tangible ROI:** 95 % reduction in patching effort and clear compliance reporting.
- **Automation as force multiplier:** scripting turns routine jobs into instant actions.