Origina

Benefits

Security for any version, even end-of-support software

Proactive risk mitigation

Security services without forced migration

Ultra-responsive security support

Origina Security Services

Origina Security Services provides a proactive and comprehensive approach to securing your IBM, HCL, and VMware software. Origina offers expert support, risk mitigation, and compliance with industry standards. Our services are a viable alternative to the traditional patching approach, focusing on risk management and empowering your team with the tools and knowledge to stay ahead of threats. Origina will enhance your security, reduce costs, and ensure the longevity of your software investments.

Business Challenges

Customers face increasing security challenges, including dealing with vulnerabilities in end-of-support software, managing complex IT environments, and ensuring compliance with regulations like DORA, PCI DSS, and NYDFS. They also need to keep up with the constantly evolving threat landscape, often with limited resources and budget constraints. Unfortunately, relying on software megavendors for security patches can lead to delays and increased risks. Origina addresses these issues by offering proactive risk mitigation, expert support, and tailored security solutions to help organizations manage their software security more effectively.

Origina Solution

Origina provides a premier security service for IBM, HCL, and VMware software, focusing on proactive risk mitigation tailored to each organization's unique environment. Origina employs a proven process for threat assessment and mitigation, which a basic reactive OEM vendor patching-only approach does not provide. By removing dependence on megavendors and enhancing transparency, we help organizations manage security risks. Origina Security Services include a Vulnerability Advisory Portal, which provides curated insights and the ability to customize dashboards for managing risk in your software. With a dedicated team of security experts, Origina ensures that clients not only respond to threats but also anticipate them, securing their software investments.

Origina Maintenance Services

Product Hardening Guides

Origina Product Hardening Guides deliver a targeted approach to enhancing software security and are included as one of Origina's full range of security services. They offer:

- **Product-focused direction:** Tailored to specific IBM, HCL, or VMware software products, these customized recommendations provide specific, actionable steps to strengthen the security posture of each product

- **Risk reduction:** Minimizes security risks by addressing potential vulnerabilities

- **Attack surface reduction:** Delivers strategies to eliminate potential attack vectors

- **Defense against security vulnerabilities:** Maintained by curated threat intelligence from over 28 trusted sources

- **Proactive approach:** Part of Origina's comprehensive strategy to anticipate and prevent security issues

> "
>
> You guys have been phenomenal, very accommodating, and very accepting of our requests following Origina's proactive support in the mitigation of a major security vulnerability.
>
> — Operations Manager, Global Telecommunications Company

Origina Software Security

Vulnerability Advisory Portal 2.0

Origina's Vulnerability Advisory Portal 2.0 offers proactive insights into software vulnerabilities, allowing teams to stay ahead of threats including:

- **Curated insights:** Up-to-date information on software vulnerabilities as they emerge

- **Customizable dashboards:** Tailored view of your security risk for products under support

- **Automated alerts:** Prompt notification about new threats or vulnerabilities

- **Detailed mitigation advice:** Specific guidance on how to address identified vulnerabilities

- **Resource prioritization:** Better allocation of resources by highlighting critical assets that need immediate attention

Origina Independent Solutions

Origina's independent security solutions offer a comprehensive approach addressing software vulnerabilities without relying on OEM vendor patches and can include:

- **Tailored solutions:** Addresses specific weaknesses in software products
- **Configuration adjustments:** Implements changes to software settings to enhance security
- **Feature management:** Disables unused features to reduce potential attack surfaces
- **Environmental modifications:** Adjusts periphery environments to improve overall security
- **Independent code-based patches:** Develops custom patches to fix security issues including open-source components that are typically not addressed by vendor patches

- **Virtual patching:** Creates a security shield around applications, including zero-day attacks without modifying the software code
- **Rapid development:** Virtual patches can be created in hours, compared to traditional patches that may take weeks
- **No downtime required:** Can be implemented while systems remain online, avoiding costly business interruptions
- **Flexible deployment:** Offers two implementation methods — embedded mode or reverse-proxy mode
- **Any version:** Works with older end-of-support software

Origina Maintenance and Support

Ultra-responsive software support: Origina offers 24/7/365 global support from IBM, HCL, and VMware experts, ensuring rapid response and resolution times. Response times for critical issues are as fast as 30 minutes or less.

800+ supported products: Origina supports over 800 IBM, HCL, and VMware products, including applications on Z mainframes and end-of-support software.

Software security: Origina's multilayered, in-depth, proactive approach to threats and vulnerabilities will often deliver better protection than an OEM passive single-layered patch approach.

Guidance on licensing: Keeping track of software license usage is essential to prevent unexpected audit issues. Origina gathers data on usage to reduce risk before audits occur.

Meet the Experts workshops: Origina includes quarterly workshops where you can benefit from the extensive technical knowledge of Origina's software and licensing specialists.

Customer advocacy: Assigned technical account managers and customer success managers provide escalation for complex issues and act as liaisons for compatibility concerns.