

STRENGTHENING CYBERSECURITY WITH DEVOLUTIONS: Essential 8 Compliance



In today's landscape of increasingly sophisticated cyber threats, organizations must adopt concrete measures to protect their data, systems, and users. The Essential 8 framework, developed by the Australian Cyber Security Centre (ACSC), outlines eight prioritized mitigation strategies aimed at reducing the attack surface and improving operational resilience.

The Essential 8 focuses on practical and effective security controls that are widely applicable across industries. These include patching applications and operating systems, enforcing multi-factor authentication, restricting administrative privileges, controlling applications, limiting macro use in Microsoft Office, hardening user applications, and implementing regular data backups. Together, these measures provide a strong foundation for cybersecurity maturity and risk reduction, helping organizations prevent, limit, and recover from cyber incidents.

At Devolutions, we not only apply the Essential 8 recommendations within our own operational practices but also design products that enable our clients to meet these standards.

HOW DEVOLUTIONS MEETS THE REQUIREMENTS OF THE ESSENTIAL 8

As an organization, Devolutions adopts a proactive cybersecurity posture that is fully aligned with the eight mitigation strategies of the Essential 8 framework. Here's how we meet each requirement:

1. Patch Applications

Devolutions has a comprehensive set of security policies that encompasses best patching practices for its software and infrastructure. Devolutions uses patch management software to ensure that all critical applications are regularly updated and patched against known vulnerabilities.

2. Patch Operating Systems

All operating systems used by Devolutions are kept up to date and officially supported. A vulnerability management program is in place, supported by regular scans and patch management solutions.

3. Multi-Factor Authentication

A strict Identity and Access Management (IAM) policy is enforced, requiring the use of multi-factor authentication for all platforms handling sensitive data.

4. Restrict Administrative Privileges

Administrative privileges are granted only to authorized personnel, following clearly defined access policies and enforced through strict access controls within our IAM framework.

5. Application Control

Devolutions' cybersecurity team uses a comprehensive set of internal tools to enforce and manage application control policies across the organization and to define, monitor, and restrict application usage based on pre-established security criteria.

6. Restrict Microsoft Office Macros

Devolutions follows Microsoft's recommendations to disable or restrict Office macros, thus minimizing attack vectors associated with document-based malware.

7. User Application Hardening

Devolutions has a dedicated security team that monitors security events and applies an incident response plan to strengthen the protection of user-facing applications.

8. Regular Backups

Devolutions has a comprehensive Business Continuity Management System (BCMS) that includes clearly defined backup procedures and policies, as well as specific Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) to ensure the continuity of critical business operations and services, thus minimizing potential impact on clients in the event of an incident or disruption.

HOW DEVOLUTIONS PRODUCTS HELP ORGANIZATION ACHIEVE ESSENTIAL 8 COMPLIANCE

Patch Operating System

Devolutions products are designed to run only on actively maintained and officially supported operating systems, ensuring optimal security, stability, and compatibility.

Multi-Factor Authentication

Devolutions products support Multi-Factor Authentication (MFA) methods, including Google Authenticator, YubiKey, Duo, email, SMS, and Radius-based authentication, providing an additional layer of security for privileged access. MFA can be enforced organization-wide or at the user level.

Restrict Administrative Privileges

Devolutions' Privileged Access Management (PAM) features empower organizations to tightly manage and secure privileged access. A standout capability is time-based access control, which allows temporary access to critical resources based on specific time windows. This ensures that users only have elevated privileges for as long as needed, significantly reducing the risk of privilege misuse, unauthorized access, or the persistence of unnecessary permissions.

Privilege Access Logs

Devolutions products allow organizations to maintain detailed logs of privileged access and actions, ensuring thorough auditability, traceability and accountability.

Regular Backups

To ensure the protection and availability of customer data, Devolutions has implemented comprehensive backup policies and procedures for its cloud-based solutions. Regular, automated backups are performed to safeguard customer data, ensuring it is securely stored and can be quickly recovered in the event of data loss or system failure.

ABOUT DEVOLUTIONS' PRODUCT SUITE

Devolutions offers a suite of products which, whether used alone or in combination, are designed to enhance IT management and security:



Remote Desktop Manager

Remote Desktop Manager: Centralizes remote connections, credentials, and tools into a unified platform, supporting over 150 connection types to streamline access and boost productivity.

<https://devolutions.net/remote-desktop-manager/>



Devolutions Server

Devolutions Server: A self-hosted solution providing secure management of shared accounts and passwords, with optional privileged access components, tailored for small and medium-sized businesses.

<https://devolutions.net/server/>



Devolutions Hub

Devolutions Hub: A cloud-based password manager enabling teams to securely store and manage business-user passwords and sensitive information through an intuitive web interface.

<https://devolutions.net/password-hub/>



Devolutions PAM

Devolutions PAM: An affordable and robust privileged access management solution that balances security with productivity, offering features like role-based access control and detailed logging.

<https://devolutions.net/privileged-access-management/>



Devolutions Gateway

Devolutions Gateway: Facilitates authorized just-in-time access to resources within segmented networks, eliminating the need for traditional VPN setups.

<https://devolutions.net/gateway/>



CONTACT DEVOLUTIONS

Based in Lavaltrie, Québec, Canada, Devolutions delivers productivity and security solutions to more than 800,000 IT professionals and business end users in over 140 countries worldwide. Please direct your inquiries and free trial requests to us via the following:

Email: service@devolutions.net

Phone: +1 844 463.0419

Live Chat via our Website: <https://devolutions.net/>