



Predict | Protect | Prevent



Security Compliance Management

Centralized Engine | Risk Assessment and Controls | Risk Mitigation

ARCON | Security Compliance Management (SCM) solution enables organizations to identify compliance irregularities by assessing the systems against the organization-specific information security and configuration baseline policies resulting in identifying the possible risks. The solution enhances visibility towards the information security posture of an organization for disparate technology platforms. ARCON | SCM is a robust technology that enables enterprises to adhere to various IT security standards for compliance purposes.

Overview

Information Technology is the driving force behind the success and growth of businesses. As a result, risks and vulnerabilities become an unavoidable part of the organization's information security culture and must be addressed promptly.

However, the scale of today's enterprise IT infrastructure demands a sophisticated toolset to address information security risks, including regulatory compliance needs of the organization. The organization's ever-expanding IT infrastructure, due to changing IT dynamics, demands robust organization wide information security compliance assessment mechanism.

It is critical to have a full-system information security compliance assessment to identify the possible security blind spots that remain undetected due to the lack of essential safeguards.

Further, in the current digital era, organizations must audit and review their techno-business processes to enhance IT Security efficiency.

ARCON | Security Compliance Management: A robust centralized engine for IT controls, risk assessment, and risk mitigation to secure Information assets

ARCON | Security Compliance Management (SCM) enables an organization to identify, assess and mitigate risks in the enterprise network. The solution helps to enforce a comprehensive IT risk management framework. It acts as a unified engine to report all IT risks at different layers for IT infrastructure for effective risk mitigation. Additionally, the solution provides comprehensive audit reports enabling an organization to build a robust security posture to ensure compliance.

The ARCON | SCM framework offers a highly scalable and customizable architecture, which provides web-based user interfaces. Its powerful agentless architecture works across technologies including operating systems, middleware, databases, and network, security devices.

ARCON | SCM

Key Features



Risk Review and Control

Risk Control within ARCON | Security Compliance Management (SCM) encompasses a powerful array of features and functionalities specifically designed to manage and mitigate risks identified during the compliance assessment process. It goes beyond mere identification by implementing measures to tackle non-compliance issues, thereby fortifying the organization's security stance. ARCON offers an extensive range of capabilities to bolster risk control, including remediation actions, establishment of standardized workflows, and ongoing monitoring to gauge the effectiveness of implemented controls. By maintaining thorough audit trails, the platform enhances transparency, accountability, and regulatory compliance. By generating detailed reports ARCON | SCM empowers organizations to preemptively minimize potential risks, elevate their security infrastructure, and highlight unwavering adherence to industry standards and regulations.

Automatic Risk Review

Automatic Risk Review in ARCON | Security Compliance Management (SCM) is a cutting-edge capability. By autonomously scanning and assessing various risk factors, due to non-compliance issues, the platform swiftly identifies and alerts the organization to potential risks. This automated process eliminates the need for laborious manual reviews, enabling prompt risk identification and response. Automatic Risk Review streamlines the overall risk assessment process, providing organizations with comprehensive insights into their security posture. It effectively pinpoints critical areas that require attention and facilitates prioritization of remediation efforts. With its automated nature, this feature enhances efficiency, accuracy, and consistency in risk evaluation, empowering organizations to proactively address compliance irregularities and uphold a robust security stance.



Exception Management

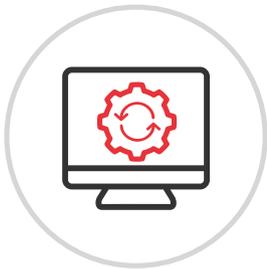
Exception Management in ARCON | Security Compliance Management (SCM) serves as a critical element, enabling organizations to handle deviations from established security policies efficiently. This feature empowers organizations to effectively manage and document authorized deviations to the established security policies, providing a systematic approach to review, approve, and track them. By leveraging a centralized platform, security administrators can meticulously store and maintain comprehensive information about each exception, including its rationale, duration, and associated risks. Exception Management within ARCON | SCM utilizes the exception handling process of an organization by allowing workflow implementation.

Policy Manager

The Policy Manager within ARCON | Security Compliance Management (SCM) serves as a dynamic and robust tool for establishing and enforcing standardized security policies throughout an organization's IT infrastructure. It empowers organizations to define security configurations and policies that align with industry best practices and regulatory requirements. With the Policy Manager, security administrators have the flexibility to create and personalize security baselines that cater to the specific needs of their organization, ensuring consistent and uniform security settings. This feature provides a centralized platform to efficiently manage and distribute these baselines to various assets and systems within the organization. By utilizing Policy Manager, IT administrators can effortlessly monitor compliance status, track deviations, and ensure policy adherence. This



streamlined approach simplifies the implementation and maintenance of a robust security posture, effectively reducing the risk of non-compliance and security risk. Leveraging the Policy Manager in ARCON | SCM empowers organizations to establish and manage standardized security policies, fortifying their overall security framework.



Workflow Management

Workflow Management in ARCON | Security Compliance Management (SCM) encompasses a powerful suite of capabilities that harmonize and optimize the management of security-related tasks, approvals, and collaboration across an organization. By providing a centralized platform, security administrators gain the ability to establish, automate, and enforce standardized workflows for diverse compliance activities and security operations. Workflow Management empowers organizations to precisely define task sequences, assign responsibilities, and establish approval mechanisms. This ensures consistent and efficient execution of security processes. It fosters seamless coordination and collaboration among stakeholders engaged in compliance and security endeavors, enabling smooth information flow and timely decision-making. Leveraging Workflow Management in ARCON | SCM unlocks the potential to enhance operational efficiency, bolster compliance adherence, and uphold a structured and auditable approach to security management.

Dashboard & Reports

The Live Dashboard in ARCON | Security Compliance Management (SCM) serves as an immersive and dynamic visualization tool, providing a holistic view of an organization's security compliance landscape in real time. With its centralized interface, the Live Dashboard offers a comprehensive display of key metrics, status updates, and critical information pertaining compliance measures, and risk assessments. Through visually captivating charts, graphs, and data summaries, it delivers a concise and easily digestible snapshot of the organization's security performance. Security administrators can effectively monitor and track the status of security controls, promptly identify potential risk or non-compliance issues, and make well-informed decisions based on up-to-the-minute insights.



The Live Dashboard empowers organizations to swiftly detect emerging risks, facilitate proactive responses, and foster strategic decision-making, fortifying their security framework. By harnessing the power of the Live Dashboard in ARCON | SCM, organizations can uphold a vigilant and responsive approach to managing security compliance.



Compliance Management

Compliance Management in ARCON | Security Compliance Management (SCM) encompasses an extensive array of tools, processes, and capabilities meticulously crafted to ensure unwavering adherence to an organization's security policies as well as regulatory requirements. This comprehensive solution provides a centralized platform where adept security administrators can flawlessly define, implement, and monitor compliance controls and measures throughout the IT infrastructure. Compliance Management empowers organizations with remarkable features including policy management according to the compliance requirements based on the organization's need. It proficiently identifies compliance gaps, empowers proactive implementation of remediation actions, and diligently tracks progress towards fulfilling regulatory obligations. By harnessing the power of Compliance Management within ARCON | SCM, organizations successfully streamline their compliance efforts, effectively mitigate risks, and showcase an unwavering commitment to upholding a formidable security posture. It empowers organizations to adeptly manage compliance, mitigate risk, and safeguard sensitive information, thereby nurturing trust with esteemed customers, valued partners, and regulatory authorities.

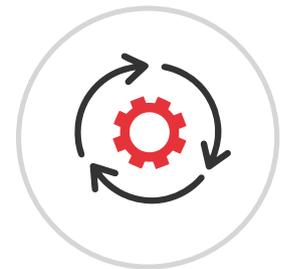


Security & Configuration Drift Management

Security & Configuration Drift Management (SCDR) in ARCON | Security Compliance Management (SCM) embodies a crucial process that revolves around the vigilant monitoring and control of configuration differences within an organization's IT infrastructure. Configuration drift occurs when unauthorized alterations or deviations arise between the configurations and settings of the Disaster Recovery (DR) and production environments. Drift Management diligently preserves the desired state of security controls by continuously comparing the present configuration of systems against the sanctioned baseline. This proactive approach effectively identifies any discrepancies or variances, empowering security administrators to expeditiously investigate and rectify them. Through the systematic management of drift, organizations uphold compliance with security policies, industry standards, and regulatory mandates, by mitigating the risk of non-compliance and potential security risk. SCDR in ARCON | SCM plays a pivotal role in cultivating and preserving a resilient and secure IT environment.

Remediation Management

ARCON | Security Compliance Management (SCM) provides an innovative capability that empowers organizations to resolve security risk due effortlessly and expeditiously to non-compliances detected during assessments. By harnessing the power of predefined rules, policies, and remediation actions. Remediation seamlessly applies corrective measures, harmonizing systems, and configurations as per compliance standards. This pivotal feature allows to maintain security posture of the datacenter, reducing the window of potential threats, empowering organizations to proactively secure their Information security landscape. Remediation within ARCON | Security Compliance Management (SCM) amplifies operational efficiency by bolstering information security and engendering a proactive ethos within security management endeavors.



Server Hardening

Server Hardening within ARCON | Security Compliance Management (SCM) entails implementing rigorous security measures and configurations to fortify servers against potential risks in the organizations' policies. This process involves adjustment of server settings and operating system configurations to minimize security risks. Server Hardening ensures servers are fortified against prevalent attack vectors and comply with regulatory standards. ARCON | SCM streamlines the Server Hardening process, enabling organizations to efficiently implement standardized security controls throughout their server infrastructure. Leveraging Server Hardening in ARCON | SCM empowers organizations to elevate their server security posture, significantly mitigate the risk of unauthorized access or data breaches and uphold a resilient and safeguarded IT environment.

ARCON | SCM

Benefits at a glance

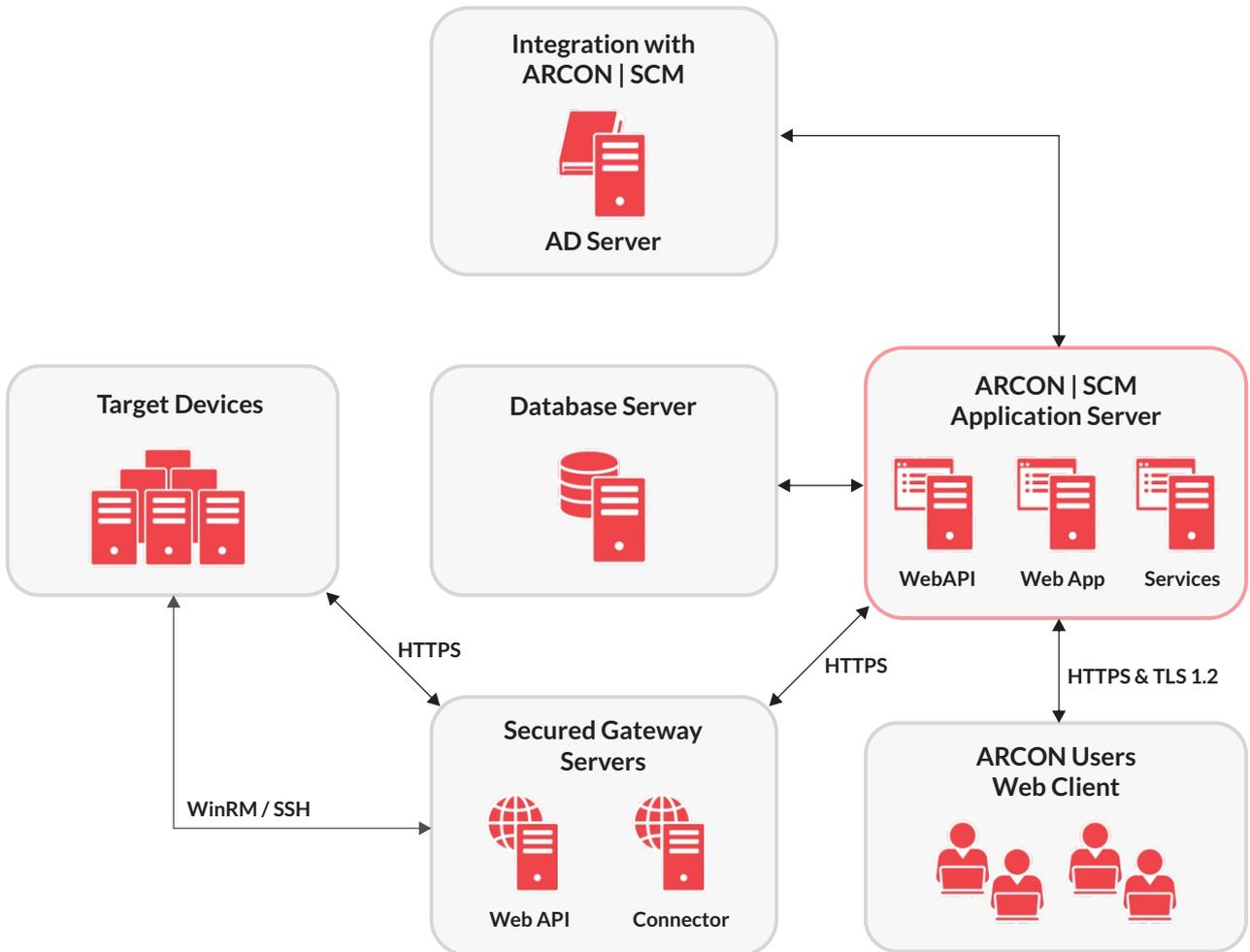
Enables prioritization of security & compliance efforts based on risk level, enterprise wide.

Allows to perform continuous risk assessment for technology platforms.

Governs, assesses, and allows optimization of Information Risk Management posture of an organization.

Provides centralized risk control framework over the IT assets.

Architecture Overview



About ARCON



ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.

All rights reserved by ARCON

This document or any part of the document may not be reproduced, distributed or published in any form without the written consent of the copyright owner under any circumstances. Any kind of infringement in the owner's exclusive rights will be considered unlawful and might be subject to penalties.