IBM Intelligent Networking Support for Cisco products

Discovers your Cisco network, collects and analyzes data to help strengthen network security and increase stability.
Technology defines everything, and it’s evolving at a blistering rate, forcing disruption across industries and causing networks to give in unexpectedly under the pressure. Now think about what a network outage can mean for you: how the loss of time, money and resources would impact your profitability and your productivity.

IBM Intelligent Networking Support (IBM INS) is a service feature, built into IBM® Managed Maintenance Solutions for Cisco Products. A state-of-the-art collector technology is used to catalogue all the elements that can affect the availability of your network and the proactive notification component alerts you of newly published security vulnerabilities. The comprehensive approach combines the complementary strengths of IBM and Cisco to enhance the health and security of your network, improving reliability and performance, and identifying potential problems before they occur.

**Automation that matters**

IBM INS for Cisco products is an automated, zero-cost service that verifies whether your network is secure, reliable and functional. It’s backed by powerful Analytics that process and correlate raw data to extract intelligence facilitating the prevention and/or resolution of network-wide problems. This improves your employee productivity and helps you maximize your technology investments.

<table>
<thead>
<tr>
<th>Time savings¹</th>
<th>ROI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>50% - 70%</strong></td>
<td><strong>+368%</strong></td>
</tr>
</tbody>
</table>
**Enhanced network visibility and security**

IBM INS helps you identify various changes that have occurred in your network and offers access to insights on INS indices of exposure over time. It’s easier to avoid issues with a clear, up-to-date record of each device in the environment and through the preemptive identification of network exposures. IBM INS for Cisco products presents in-depth security vulnerability information including remedial actions; visibility over hardware and software lifecycle together with recommended upgrade paths, which enables you to properly plan code upgrades and budget hardware refresh far in advance. Additionally, IBM INS displays support coverage status of the network and flags devices which are uncovered or approaching support renewal.

---

**With IBM INS, we get a list of devices that are running on really old code, or the code they are running has known security or other issues. This allows us to resolve or upgrade to the next recommended code quickly and smartly.**²

Senior Network Engineer

---

**The intelligent dashboard**

The dashboard provides information on support coverage status of the network devices and flags those that are not covered or approaching support renewal.
A simple, complete solution
IBM INS for Cisco products delivers enhanced availability and performance of your network environment with software updates, hardware replacements and around-the-clock break-fix support for your Cisco hardware, applications and operating systems. With IBM, you receive world-class support from a single, trusted service provider and for severe issues, direct access to Cisco product experts for faster issue resolution. As a result, you can take a comprehensive approach to the care and continuous improvement of your network for a single price, with a single point of contact.

For more information
To see how IBM INS for Cisco products can help your enterprise grow, read the Forrester study The Total Economic Impact™ Of IBM Intelligent Networking Support (INS).

Learn more about IBM Intelligent Networking Support →

To get more information please contact your IBM representative.

References
1,2 “The Total Economic Impact™ of IBM Intelligent Networking Support (INS).” Forrester Total Economic Impact™ Study. Published February 2016.

IBM. © Copyright IBM Corporation 2019
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
June 2019

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., other countries, or both. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Check Point Software Technologies cybersecurity solutions are not IBM products or offerings. Check Point Software Technologies cybersecurity solutions are sold or licensed, as the case may be, to users under Check Point Software Technologies terms and conditions, which are provided with the product or offering. Availability, and any and all warranties, services and support for Check Point Software Technologies cybersecurity solutions are the direct responsibility of, and is provided directly to users by, Check Point Software Technologies.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.