Continuous monitoring

Automate monitoring, manage risk more effectively and get the most out of existing security tools

The rapidly evolving threat landscape and increasingly sophisticated attacks mean all organizations are at risk of assaults on their business, personal, financial and proprietary data. Adversaries are highly motivated and well-funded — often supported by crime syndicates and nation states.

Continuous monitoring of these assets is becoming a mandate in many countries. For example, under NISTIR 8011, the U.S. Department of Homeland Security requires federal agencies and contractors to integrate continuous monitoring into their environments. Similarly, as of 2018 the General Data Protection Regulation (GDPR) requires 72-hour notification of authorities for breaches of personal information affecting citizens in the European Union.

Public sector organizations with a high risk profile need to know and control what is on their network, as well as how to get the most out of their security tools and staffs.

Continually manage your risk

Perspecta continuous monitoring, an intelligent security operations solution used by U.S. federal agencies, provides operations and management teams with continuously updated information on the network environment through an at-a-glance dashboard, helping organizations automate processes and achieve operational excellence.
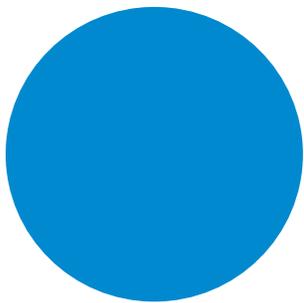
Continuous monitoring helps customers improve operations as well as enterprise governance, risk management and compliance (eGRC) functions while getting more capability out of their existing investment in security tools. Continuous monitoring includes continual assessment of hardware, software, configuration and vulnerabilities to identify and prioritize security issues through a tiered dashboard.
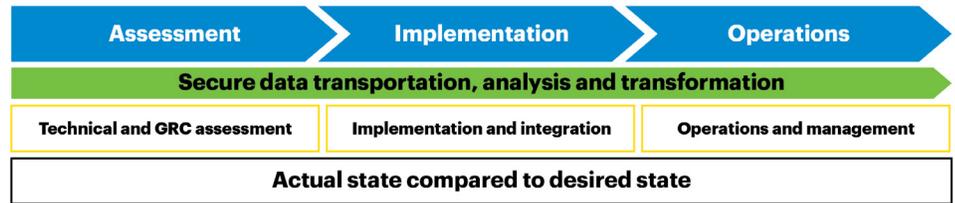
Experienced Perspecta security experts provide technical and eGRC assessments to identify gaps, understand processes and ensure you get the most out of your monitoring program. This solution addresses technical gaps and integration within your environment, allowing data from security sensors to feed and continuously update points of remediation against your desired state.

Reduce risk, increase consistency

Continuous monitoring provides immediate benefits to your operations:

- **Automate and improve security processes:** To address the severe shortage of experienced security specialists industry-wide, continuous monitoring helps your organization automate data gathering, analysis, prioritization and workflow management

- **Quickly identify issues:** Ensure a proven approach to monitoring your assets. The U.S. Department of Homeland Security (DHS), for example, found that public sector agencies on average discovered 44 percent more assets than they were aware of. With Perspecta's solution, you can identify all of the assets on your network, know if they are running approved applications, understand any new configuration issues, and have a consolidated and prioritized list of outstanding vulnerabilities enterprise-wide

- **Gain valuable insights and situational awareness:** Provide ongoing, valuable information about the devices on your network with prioritized risk information

perspecta™

Assessment	Implementation	Operations
Secure data transportation, analysis and transformation		
Technical and GRC assessment	Implementation and integration	Operations and management
Actual state compared to desired state		

Benefits

- Quickly identify security issues with at-a-glance dashboard
- Automate monitoring and improve security processes
- Gain valuable insights and situational awareness
- Free up security staff

- **Maximize the value of existing tools:** Increase the value you derive from existing security tools and gain scalability to minimize the risk of data loss

- **Effectively manage risk:** By comparing the actual to desired state of hardware, software vulnerability and configuration of assets, you can manage risk more effectively

Gain the benefits of a proven solution

- **Industry-leading approach:** Our solution is based on CAESARS FE standards for Continuous Asset Evaluation, Situational Awareness and Risk Scoring – Framework Extension – NISTIR 7756 with recommended enterprise service bus architecture and dashboard integration

- **Flexibility:** An enterprise service bus provides a low-risk, low-cost, scalable option to take advantage of your current security investment without adding disproportionate complexity as you upgrade, so you can easily change and grow with the environment

- **Comprehensive solution:** Our intelligent end-to-end approach includes expertise, management, hardware and software, as well as infrastructure options, to help your security environment become mature

- **Safe pair of hands:** Beyond an industry-leading technical approach, our security consultants provide a maturity assessment and gap analysis, project and administrative management, testing, and a rapid deployment tool to greatly shorten deployment

Meet your security needs

Built to meet DHS requirements for continuous diagnostics and mitigation, our continuous monitoring solution meets required government standards and provides a multi-tiered dashboard to deliver an operational, management and strategic view of enterprise risk. It is designed to minimize implementation and operational risk and is currently running in six U.S. public sector agencies.

Our installed security sensors can grow with changes and upgrades to your security sensor environment, and can be a base for additional functionality, including integration of identity and access management and further situational awareness. Our solution provides flexible functionality to meet your current and future needs.

Rely on our comprehensive program

Continuous monitoring helps meet the risk management and cybersecurity frameworks as well as automate appropriate portions of ongoing assessment requirements outlined in the NIST Interagency Report (NISTIR) 8011, Automation Support for Security Control Assessments. It provides all of the benefits of the first phase of the DHS Continuous Diagnostics and Mitigation program, covering hardware, software, vulnerability and configuration management.

Our program management approach, which includes accelerated delivery planning, helps to identify, manage and eliminate implementation risk, while our robust architecture provides low-risk technical agility to quickly integrate into your current and future environments. Our advisory assessment can give you a complete picture of the products and services required to deploy continuous monitoring.