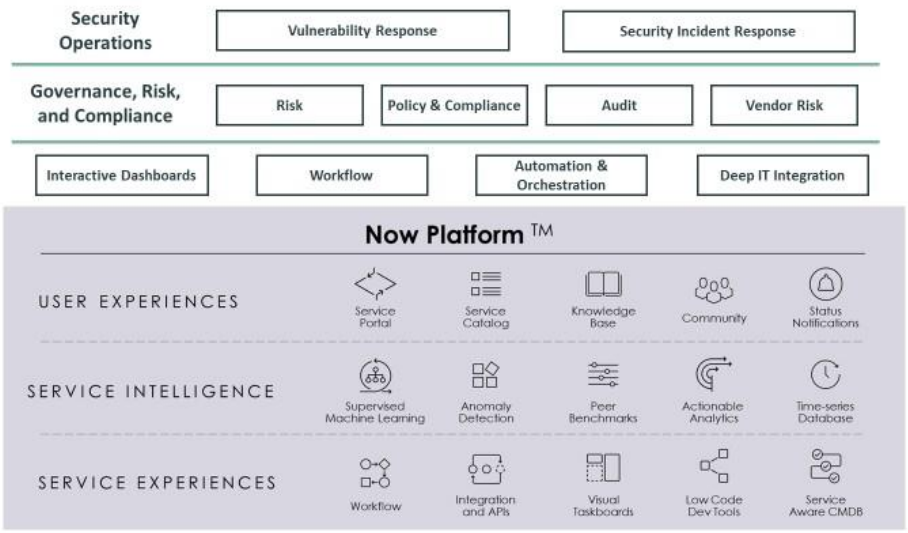
Continuous Risk Monitoring Overview

Enterprise risks proliferate so fast, they can be easy to miss. Minimize data breaches and improve compliance with continuous risk monitoring to better identify issues for analysis and remediation.

ServiceNow Governance, Risk, and Compliance and Security Operations
The enterprise risk landscape is constantly changing. Your cyber security team may be informed of a vulnerability and patch it only to have others quickly emerge. It's an on-going battle to keep up. Plus, enterprises face increasingly more sophisticated threats. Consider the burden of new regulations, the risk posed by a growing number of third parties necessary for digital transformation initiatives, IT changes, applications—and more. By letting these risks fall through the cracks, you are exposing your enterprise to the possibility of costly data breaches and compliance violations.

While any of the risks mentioned above can lead to security breaches, let's focus on vulnerabilities as an example because they are so common. Today, software vulnerabilities, where cyber criminals exploit software coding flaws, are one of the leading causes of data breaches. A study conducted by ServiceNow and the Ponemon Institute* found that nearly 50 percent of organizations surveyed had experienced a breach in the past two years, and for many, the breach was due to a software vulnerability for which a patch existed.



** Ponemon Institute, Costs and Consequences of Gaps in Vulnerability Response, 2019 (https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf)*

So why don't enterprise security teams apply patches more quickly? Too many still depend on slow, manual processes using spreadsheets and e-mail to respond to vulnerabilities. Teams also lack processes to easily track and confirm when a

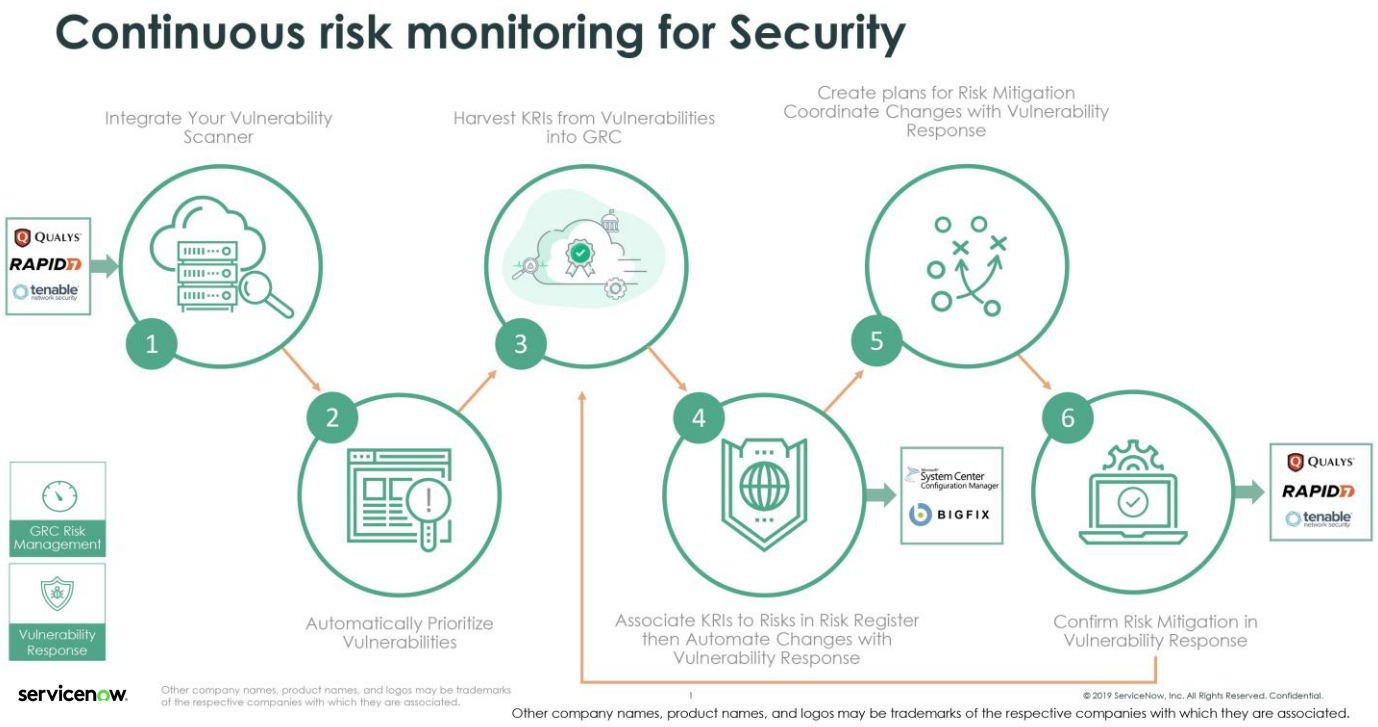
The continuous monitoring perspective

With a common platform running GRC Risk Management and Vulnerability Response and Vulnerability Solution Management, you can achieve a complete continuous monitoring perspective to minimize enterprise risk exposure and be certain that the correct processes are in place to establish an optimal security, risk and compliance posture.

Actions taken within Vulnerability Solution Management to remediate previously unpatched software vulnerabilities are easily viewable within the interactive GRC Risk Management dashboard.

Learn More:
GRC Continuous Risk Monitoring
www.servicenow.com/risk

Security Operations
www.servicenow.com/sec-ops



vulnerability has been closed and remediated to achieve up-to-date visibility into their organization's current risk exposure.

What can you do to more quickly identify and remediate risks like software vulnerabilities to minimize your risk exposure? And how can you more easily ensure that the right processes are in place for your enterprise to achieve an optimal security, risk, and compliance posture?

ServiceNow enables real-time continuous monitoring for risk based on the impact to the business through ServiceNow Governance, Risk and Compliance (GRC) Risk Management with out-of-the-box risk indicator templates and the Security Incident Response and Vulnerability Response applications in ServiceNow Security Operations, all on the Now Platform®. With these tools, your enterprise can efficiently remediate security incidents and unpatched vulnerabilities to ensure compliance.

ServiceNow GRC Risk Management
Ideally all vulnerabilities are addressed in a timely fashion. However, this is rarely the case and that's why continuous monitoring is so important. Using ServiceNow GRC Risk Management, your risk team can say good-bye to the manual processes and significant time required to continually identify, assess, and monitor risks. With the application, security teams can monitor IT controls to ensure proper processes are

A study conducted by ServiceNow and the Ponemon Institute* found that nearly 50 percent of organizations surveyed had experienced a breach in the past two years.

followed for changes or patches to HR or legal processes such as code of conduct, on-boarding, or data privacy. It's also possible to track changes impacting financial processes to ensure compliance to Sarbanes-Oxley and other regulations, to name a few.

If we again focus on our example of mitigating the risk associated with an unpatched software vulnerability, the GRC Risk Management dashboard lets your security team clearly view current enterprise risk exposure levels and drill down to identify risk exposure.

Your security team can easily define and automate the testing of additional controls to help ensure that a failure is not repeated. For example, to mitigate the risk that an unpatched software vulnerability creates (such as loss of confidentiality), the team can design a patch management process.

ServiceNow Vulnerability Response

Using ServiceNow Vulnerability Response, your security and IT teams can work together to respond faster and more efficiently to remediate vulnerabilities, such as our example of an unpatched software vulnerability that was initially identified in the GRC Risk Management dashboard.

ServiceNow Vulnerability Response connects the workflow and automation capabilities of the Now Platform® with vulnerability scan data from leading vendors to give your teams a single platform for response that can be shared between security and IT. The application imports and automatically groups vulnerable items according to group rules, allowing teams to remediate vulnerabilities quickly. Vulnerability data is pulled from internal and external sources, such as the National Vulnerability Database (NVD) or third-party integrations.

Using the Vulnerability Solution Management, which is a feature that is available within the Vulnerability Response application, the system automatically correlates vulnerability exposure with solutions to show the most impactful remediation activities, prioritize them by the greatest reduction in vulnerability risk, and monitor their completion.

So, your security team member can log into your vulnerability management system and see a quick overview of vulnerability issues, including those identified as critical. In the case of a flagged unpatched software vulnerability, the system automatically identifies the best solution, which in this case is the optimal software patch. Once the patch has been successfully deployed, the system automatically records the completion.

Using ServiceNow Vulnerability Response, your security and IT teams can work together to respond faster and more efficiently to remediate vulnerabilities, such as our example of an unpatched software vulnerability that was initially identified in the GRC Risk Management dashboard.

Learn More:
GRC Continuous Risk Monitoring
www.servicenow.com/risk

Security Operations
www.servicenow.com/sec-ops

servicenow.