COVID-19 has changed healthcare forever. The pandemic has forced the healthcare industry to accelerate their path to digital transformation from years to weeks. Seemingly overnight, member needs shifted to limited-touch access for virtual care, benefits, and health plans. The changes in today’s market reinforce the need to deliver reliable services, maintain data privacy, adhere to new regulatory requirements, and protect member information. As a result, healthcare organizations continue to invest significantly in security to protect medical information from malicious attacks, drive continuous scanning of IT infrastructure for vulnerabilities, and automatically identify software upgrades and patches that are needed to keep ahead of a growing range of cyber threats.

To better understand the benefits, costs, and risks associated with ServiceNow Security Operations, ServiceNow commissioned Forrester Consulting to interview one customer and conduct a Total Economic Impact™ (TEI) study.  

The interviewee’s organization has the following characteristics:

- A healthcare company with multiple offerings ranging from pharmacy services to clinical and specialty programs/solutions.
- More than 3,000 employees with operations across the United States.

ServiceNow Security Operations includes ServiceNow Security Incident Response and ServiceNow Vulnerability Response. Security Incident Response is a security orchestration, automation, and response (SOAR) solution that integrates with other security tools to consolidate all security incidents in one place and orchestrate investigations and response. Access to business and threat context allows security analysts to quickly triage incidents and prioritize the most critical issues.

ServiceNow Vulnerability Response provides risk-based vulnerability management (RBVM) to help organizations respond faster and more efficiently to vulnerabilities, connect security and IT teams, provide real-time visibility, and prioritize assets based on value and exploitation status. Vulnerability Response provides a comprehensive view of all vulnerabilities affecting a given asset or service through integration with ServiceNow Configuration Management Database (CMDB), as well as the current state of all vulnerabilities affecting the organization.
INVESTMENT DRIVERS
Decision-makers with the healthcare organization wanted to replace legacy manual processes that made it increasingly difficult for their organization to keep up with the rate and volume of vulnerabilities and security incidents. They looked for a solution that could help them eliminate vulnerabilities faster, provide a more timely and efficient response to security incidents, and fuel digital transformation.

- **Manual processes hindered security incident and vulnerability response times.** The healthcare organization’s security team was inundated with alerts and information from multiple tools. Each incident required manual effort to determine the risk level, business context, and priority. Once the team established the criticality and priority of a security incident or vulnerability, coordinating a response across IT and security, and tracking it to resolution involved inefficient manual processes. This hindered the organization’s ability to accelerate digital engagements with customers.

- **There was limited visibility into security posture.** Decision-makers relied on spreadsheets and emails to manage the remediation of vulnerabilities and security incidents. It was overly complex to monitor and build alerts for potential security threats and risks. Security analysts struggled to consolidate data and metrics across multiple formats to provide the management team with real-time visibility into the security posture and response performance of the organization.

- **The costs associated with manual security response were high.** Decision-makers previously spent days assessing each security incident or vulnerability and then coordinating a remediation plan. In addition, frontline security analysts were burdened with working on incidents that could easily be addressed through automation.

SECURITY OPERATIONS FEATURES
The healthcare organization’s decision-makers looked for a solution that could:

- **Significantly improve the security of mission-critical assets.**
- **Facilitate a highly structured, efficient, and repeatable process.**
- **Provide intelligence of where each vulnerability stands and what action IT is taking to fix it.**
- **Prioritize vulnerabilities that affect sensitive medical and financial data.**
- **Improve security incident response times.** The healthcare organization’s goal was to increase the efficiency with which IT and security professionals manage both tier 1 security incidents and the more complex tier 2 and higher security incidents.
- **Improve vulnerability management process.** Decision-makers wanted to automatically pull data from vulnerability scans into ServiceNow Vulnerability Response, group vulnerabilities by criticality, and automatically link vulnerabilities to organization assets.
- **Offer intuitive dashboards and reporting to deliver real-time visibility into the organization’s security posture.** All levels of employees within the organization can then track the status of a security incident or vulnerability, and the risk profile at any time.
- **Increase communication and coordination between IT, security, and risk teams.** Decision-makers wanted a single platform that enables teams to communicate, track, and coordinate security incident and vulnerability response efforts more effectively.
- **Increase automation.** The healthcare organization needed to automate basic tasks and
route incidents and vulnerabilities to appropriate resources, to improve security operations productivity.

KEY RESULTS
By leveraging the ServiceNow Security Operations capabilities, the healthcare organization experienced the following risk-adjusted present value (PV) quantified benefits over three years:

- **Increased efficiency of prioritization and resolution of security incidents, resulting in $1,683,678 in benefits.** The healthcare organization realized a 30% improvement in the efficiency of frontline security analysts handling tier 1 or less complex security incidents. It also achieved a 50% efficiency increase related to managing tier 2 or higher security incidents that require coordination across multiple IT and security resources. The organization gained these efficiencies by automating workflows that span security and IT, prioritizing security incidents based on business criticality, and tracking incidents and assigning tasks using a single platform.

“We are very happy with our investment in ServiceNow Security Operations. I would highly recommend the vulnerability integration with a vulnerability management tool because it not only provides increased visibility, but it has great assignment rules that ensure timely and effective remediation.”

Manager of information security, healthcare

- **Improved vulnerability management and response times, resulting in $353,947 in benefits.** The healthcare organization is now equipped to manage the outputs of weekly scans – identifying, classifying, and prioritizing vulnerabilities in its environments. On average, teams identify 10,000 vulnerabilities each week. Previously, IT teams resorted to manually intensive processes (e.g., spreadsheets, emails) to categorize vulnerabilities and have security teams analyze them. ServiceNow Vulnerability Response allows the organization to automatically pull all the data from a vulnerability scan into the solution and then apply rules and logic to identify critical vulnerabilities that need immediate action. For example, decision-makers can map vulnerabilities and prioritize them based on risk scores and eliminate manual tasks or disjointed processes with automated workflows. They can also link these vulnerabilities to existing assets to determine business relevance and impact. The healthcare organization now sees a 70% improvement in identifying and prioritizing vulnerabilities and can quickly assess the impact to existing assets. In addition, it realizes a 50% improvement in vulnerability response times by speeding the application of patches and other remediation efforts with automated workflows.

- **Improved security governance with real-time visibility and reporting, resulting in $287,242 in benefits.** The healthcare organization realizes labor and time savings with unified dashboards, workflow automation, and easy reporting. These dashboards help security and IT teams respond faster and more efficiently to incidents and vulnerabilities and to make better use of their time driving improvements and innovation. The healthcare organization would have needed to add one FTE to produce real-time reports with the manually driven legacy environment to match the reporting and visualization capabilities of ServiceNow.

Realized opex savings by eliminating legacy manual processes or tools, resulting in $70,999 in benefits. Decision-makers were able to discontinue licenses and support contracts for legacy tools the organization previously used to manage security incident response processes. Forrester estimates legacy approaches and tools previously cost the organization $50,000 each year, and that implementing ServiceNow allowed decision-makers to discontinue these tools and realize those savings beginning in Year 2.
TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full report “The Total Economic Impact™ of ServiceNow Security Operations,” commissioned by ServiceNow and delivered by Forrester Consulting.

STUDY FINDINGS

Forrester interviewed one decision-maker from a healthcare organization with experience using ServiceNow Security Operations and combined the results into a three-year financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- $1,683,678 gain from increased efficiency of prioritization and resolution of security incidents.
- $353,947 savings from improved vulnerability management and response times.
- $287,242 savings from improved security governance with real-time visibility and reporting.
- $70,999 opex savings by eliminating legacy manual processes or tools.

Appendix A: Endnotes

1 Total Economic Impact is a methodology developed by Forrester Research that enhances a company’s technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

DISCLOSURES

The reader should be aware of the following:

- The study is commissioned by ServiceNow and delivered by Forrester Consulting. It is not meant to be a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in ServiceNow Security Operations.
- ServiceNow reviewed and provided feedback to Forrester. Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester’s findings or obscure the meaning.
- ServiceNow provided the customer names for the interview but did not participate in the interviews.

ABOUT TEI

Total Economic Impact™ (TEI) is a methodology developed by Forrester Research that enhances a company’s technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders. The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility.