INNOVATE
TRANSFORM
Adapt to the new business reality.
SUCCEED

Technology Strategy and Operations
- Cybersecurity and Privacy
- Cloud Solutions
- Software Services

SAP Solutions
- Enterprise Application Solutions
- Enterprise Data and Analytics
- Emerging Technology Solutions
How well is your organization adapting to the ever-changing demands of today’s marketplace? Implementing the right mix of technology and programs to innovate, protect margins and build shareholder value while keeping your data assets safe requires a partner that can help you succeed. Trust Protiviti. We’ll help you find the right solutions to make your business excel.
Yesterday’s innovation is today’s status quo, and any business that doesn’t stay ahead of the curve falls behind. But technology is rarely the sole solution to business challenges. Understanding the business process you want to enable, the customer experience you want to create or the critical information you need to protect is a necessary first step in making technology work for you.

We leverage emerging technologies and methodologies to innovate, while helping organizations transform and succeed by focusing on business value.

Our advanced Technology Consulting solutions range from strategy development through design, implementation and managed services. We are also experts in operational resilience, data and analytics, cybersecurity and privacy, cloud, application implementation, artificial intelligence and robotic process automation.

See why Protiviti is the right choice to innovate, transform and succeed.
Cybersecurity continues to be a top concern for boards and enterprise risk management functions. Organizations must respond to manage this important risk while not draining resources that drive growth and innovation.

Security is, and will continue to be, a key factor in the digital transformation process for regulated data, internal control, critical operations and intellectual property protection spanning public cloud, SaaS and the use of Internet of Things (IoT) devices.

The industry will need to implement innovative solutions, both to overcome the severe cyber talent shortage and to keep up with the threat actors that are improving capabilities at an astonishing rate.

As a stopgap, CISOs are adapting short-term skills management practices by outsourcing security functions to managed security service providers (MSSPs).

By 2021, cybercrime is likely to cost the world $6 trillion annually — more than the combined GDP of the UK and France.*

The rapid speed of disruptive innovations enabled by new and emerging technologies (e.g., artificial intelligence, robotics, machine learning, hyperscalable platforms) and/or other market forces may outpace an organization’s ability to compete and/or manage the risk appropriately, without making significant changes to the business model.**

Ensuring privacy and identity management and information security or system protection may require significant resources.**

Organizations may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage their brand.**


**Executive Perspectives on Top Risks 2020, Protiviti and North Carolina State University’s ERM Initiative, December 2019.
WE UNDERSTAND THE CLIENT’S PERSPECTIVE
AND DELIVER A CUSTOMIZED STRATEGIC SOLUTION

Each client brings a unique set of challenges to be solved and strategic opportunities to seize. Organizations are almost universally reevaluating their business models and platforms to stay relevant and achieve success in this digital era. Similarly, they are continually modifying their security defenses to address new threats. Invoking meaningful transformative change is both rewarding and elusive. Ideas, initiatives and a wide range of priorities compete for limited people and dollars to bring them to fruition. At Protiviti, we take the time to fully understand the particular needs our clients bring to the table and then partner to customize solutions for powerful insights and proven delivery.

<table>
<thead>
<tr>
<th>THE CHALLENGES CLIENTS BRING</th>
<th>THE ANSWERS CLIENTS ARE LOOKING FOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automate, mature and manage new digital security challenges</td>
<td>Implementation and management of new cyber capabilities and technologies across domains of Identify, Protect, Detect, Respond and Recover, leveraging new technologies (e.g., AIML)</td>
</tr>
<tr>
<td>Privacy pressures from increased regulation (GDPR, CCPA, etc.) and scope of compliance</td>
<td>Implementation of regulatory compliance, privacy and third-party risk management programs</td>
</tr>
<tr>
<td>Resource shortages and skills for cybersecurity and privacy needs</td>
<td>Deep subject matter expertise with a flexible delivery model, including bringing in the right partners</td>
</tr>
<tr>
<td>Securing the journey to the cloud and new technologies</td>
<td>Efficient and effective transition to, compliance with and management of the cloud</td>
</tr>
<tr>
<td>Respond, recover and build resilience in the face of an adverse event (e.g., data breach)</td>
<td>Design and implementation of resilience solutions and processes to withstand disruptive events</td>
</tr>
</tbody>
</table>
WE’RE ONE OF A KIND
FLEXIBLE SOLUTIONS THAT ADJUST TO YOUR NEEDS

We are the only organization that provides flexible delivery models to help you address short-term skill gaps, deliver projects or transform your organization by creating the right team that can scale up or down, quickly and cost-efficiently.

We have flexibility to tailor our delivery models to meet your organizational needs:

<table>
<thead>
<tr>
<th>BLENDED DELIVERY</th>
<th>ONSHORE DELIVERY</th>
<th>OFFSHORE DELIVERY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FLEXIBLE RESOURCES</strong></td>
<td><strong>MANAGED SOLUTIONS</strong></td>
<td><strong>CONSULTING</strong></td>
</tr>
<tr>
<td>• Project leadership delivered in collaboration with skilled resources</td>
<td>• Delivered in collaboration with our consulting solution centers</td>
<td>• Delivered in collaboration with our offshore solution centers</td>
</tr>
<tr>
<td>• Local, specialized talent with option to convert to permanent</td>
<td>• Access to Robert Half’s 24x7 Service Center with Tier 1 and 2 technical and operational support staff</td>
<td>• Greater concentration of resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reliable, optimized source of talent</td>
</tr>
</tbody>
</table>

More than 2.7 million experienced professionals at Robert Half support Protiviti’s core team of consultants, operating from over 400 offices across 25 countries. We provide the specialized skills you need fast and with minimal to no travel costs. It also means we can ramp up or down depending on your needs.
MANAGED SOLUTIONS: OUR VALUE PROPOSITION
POWERED BY ROBERT HALF

OUR MANAGED SOLUTIONS PROVIDE YOU WITH

- Cost reductions by avoiding overhiring
- Bandwidth to prevent burdening full-time employees to deliver on projects
- Ability to scale up or down as needed
- Experienced subject matter experts, on demand, for unique and complex issues

MANAGED SOLUTIONS VALUE

ADVISORY
Identify, anticipate and solve problems through transformation and implementation
- Solving complex programs with Agile methodologies and design thinking while managing deliverables, milestones and outcomes
- Technology enablement through artificial intelligence, machine learning, process mining and robotic process automation

THE RIGHT TEAM
Address skillset gaps and hiring challenges
- Maintaining control and oversight of the resources
- Access to specific, specialized skills and expertise that cannot be found on your internal team
- Time saved to upskill your existing team

SEAMLESS OPERATION
Manage or fix functions, processes or data to free up your team to work on what matters
- Cost efficiencies: Flexibility to scale up or down with the right resources at the right time (onshore or offshore)
- Reduced risk: Performance, productivity and service levels are our responsibility
WHERE WE EXCEL

CYBERSECURITY AND PRIVACY

Transforming business happens one step at a time.

Attention to detail, respect for the process and a commitment to excellence set Protiviti apart.

<table>
<thead>
<tr>
<th>ENVISION VALUE</th>
<th>REALIZE VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SECURITY PROGRAM AND STRATEGY</strong></td>
<td><strong>CLOUD SECURITY</strong></td>
</tr>
<tr>
<td>Risk Assessment and Analysis</td>
<td>Strategy, Architecture and Implementation</td>
</tr>
<tr>
<td>Program Design, Benchmarking and Metrics</td>
<td>Cloud Security Assessment</td>
</tr>
<tr>
<td>Policy Design and Development</td>
<td>DevSecOps</td>
</tr>
<tr>
<td>Security Strategy and Governance</td>
<td>Cloud Vulnerability Management</td>
</tr>
<tr>
<td>Board/C-Suite Cybersecurity Communication and Reporting</td>
<td></td>
</tr>
<tr>
<td>Cyber Program Office</td>
<td></td>
</tr>
<tr>
<td><strong>DATA PRIVACY</strong></td>
<td><strong>DIGITAL IDENTITY</strong></td>
</tr>
<tr>
<td>Privacy Program Assessments</td>
<td>IAM Program and Strategy</td>
</tr>
<tr>
<td>Privacy Program Development</td>
<td>Role-Based Access Control</td>
</tr>
<tr>
<td>Managed Privacy Services</td>
<td>Identity Governance and Administration</td>
</tr>
<tr>
<td></td>
<td>Privileged Access Management</td>
</tr>
<tr>
<td><strong>DATA SECURITY</strong></td>
<td><strong>ATTACK AND PENETRATION</strong></td>
</tr>
<tr>
<td>Data Classification, Protection and Governance</td>
<td>Application Security Testing</td>
</tr>
<tr>
<td>Cyber Defense</td>
<td>Network Security Testing</td>
</tr>
<tr>
<td>Compliance (e.g., PCI, HITRUST, FFIEC)</td>
<td>Red Team</td>
</tr>
<tr>
<td>Vendor/Third-Party Risk Management</td>
<td>Social Engineering</td>
</tr>
<tr>
<td></td>
<td>DevSecOps/SSDLC</td>
</tr>
<tr>
<td></td>
<td>Source Code Review</td>
</tr>
<tr>
<td></td>
<td>Hardware, IoT and Medical Device Testing</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Management</td>
</tr>
</tbody>
</table>
With our ability to function at both the strategic and tactical levels, we combine deep technical security competence with executive-level communication and management. Our holistic approach starts by understanding what is most important to organizations, then structuring and supporting programs so your business is engineered to grow securely.

<table>
<thead>
<tr>
<th>PROTECT VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MANAGED SECURITY SERVICES</strong></td>
</tr>
<tr>
<td>Managed Detect and Respond</td>
</tr>
<tr>
<td>Threat Exposure Management</td>
</tr>
<tr>
<td>Data Protection Management</td>
</tr>
<tr>
<td>Third-Party Risk</td>
</tr>
<tr>
<td>Cloud Security Sustainment</td>
</tr>
<tr>
<td>Digital Identity Management</td>
</tr>
<tr>
<td>Managed Privacy Services</td>
</tr>
<tr>
<td>Supply Chain Security Management</td>
</tr>
<tr>
<td>Security Operations</td>
</tr>
<tr>
<td><strong>OPERATIONAL RESILIENCE</strong></td>
</tr>
<tr>
<td>Enterprise Resilience Programs</td>
</tr>
<tr>
<td>Formalizing Business Services</td>
</tr>
<tr>
<td>Cyber Resilience</td>
</tr>
<tr>
<td>Technology Resilience</td>
</tr>
<tr>
<td>Business Resilience</td>
</tr>
<tr>
<td>Third-Party Resilience</td>
</tr>
<tr>
<td>Resilience Testing and Assurance</td>
</tr>
<tr>
<td><strong>INCIDENT RESPONSE AND CYBER RESILIENCE</strong></td>
</tr>
<tr>
<td>Strategy and Planning</td>
</tr>
<tr>
<td>Tabletop Exercises</td>
</tr>
<tr>
<td>Emergency Breach Response</td>
</tr>
<tr>
<td>Cyber Forensics and Litigation Support</td>
</tr>
<tr>
<td>Compromise Assessments</td>
</tr>
<tr>
<td>Cyber Threat Hunting</td>
</tr>
<tr>
<td>Business Continuity/Business Resiliency</td>
</tr>
<tr>
<td>Post-Event Review/Facilitated Lessons Learned</td>
</tr>
</tbody>
</table>
SECURITY PROGRAM AND STRATEGY

CLIENT PROBLEMS WE SOLVE

Gaining clarity on ever-increasing information security-related risks and their impact to the organization; quantifying and defining the risk tolerance and developing/refining strategies and controls to address those risks

The challenge to build and operate an infrastructure that preserves the integrity and confidentiality of the organization’s data assets and intellectual property

Communication effectiveness to a variety of stakeholders, from operational management to C-suite leadership and boards of directors

Insufficient skills or operational resources to manage and deliver security program initiatives

BUSINESS OUTCOME

ENVISION
Understand information security threats and current capabilities to deal with them, and design necessary improvements

REALIZE
Set a strategic course and implement the designed architecture, leveraging strong program/project management and quantifying risk to articulate the benefit of doing so

PROTECT
Meaningful communication of progress and results to stakeholders that matter most — the board, employees, partners and customers — and driving continuous improvement

OUR STEPS TO SUCCESS

1. Drive clarity on information security and privacy strategies, quantify and align them with business objectives

2. Establish the cybersecurity program office’s foundation and strategy; manage work streams and improve security programs

3. Implement security program design, benchmarking, strategy, architecture, policies, metrics and awareness of program objectives

4. Ensure board/C-suite cybersecurity communication and reporting, training and awareness
Our Security Program and Strategy services are designed to assist clients with understanding the information security and privacy risks they face and determining their readiness to address them. Our offerings help companies take a holistic business and technology view of their risk environment, use industry-accepted information security frameworks to evaluate their control environment, and develop/refine information security and privacy strategies, practices and technology architectures to reduce their exposures. In addition, we assist clients in designing metrics of merit for security and privacy, and develop effective communication to their stakeholders — from operational management to C-suite leadership and boards of directors.

CLIENT CHALLENGE

A global life insurance company sought assistance in building a cloud platform with appropriate controls to provide high-availability (HA) applications for their clients. Specifically, the client wanted to develop a target control structure and framework for a cloud platform.

SOLUTION DELIVERED

Evaluated maturity of the risk management organization, including target capabilities and new areas of focus

Analyzed existing Agile delivery and continuous integration models; defined and implemented key security controls for a DevSecOps pipeline

Identified opportunities for organizational and procedural change supporting cloud integrations

Developed prioritized security reference architecture patterns to establish repeatable guidelines for cloud initiatives

Provided assessment of existing capabilities and new requirements necessary for cloud transformation

Created roadmap for DevSecOps integration with existing Agile environment

Provided expertise on existing process changes required to support cloud integrations

Created sustainable cloud security architecture for repeatable processes

BUSINESS RESULTS
DATA PRIVACY

Our national and global clients are experiencing an unprecedented change in the data privacy landscape. Numerous new and changing U.S. state and federal regulations, as well as global regulations, are forcing business, technical and legal operational changes on a nearly weekly basis. These changes are not necessarily exclusive of one another and often overlap, resulting in highly complex legal and regulatory scenarios.

Protiviti supports our clients by helping them establish effective privacy compliance programs that cross the legal, technical, business and compliance groups. Our approach ensures that clients’ privacy programs meet or exceed their legal data privacy obligations in an efficient and cost-effective manner.

ENVISION
Understanding data collection, processing and applications in scope; identification of regulatory compliance gaps and remediation steps to quickly achieve compliance

REALIZE
Implementation of an effective and flexible data privacy program that meets not only today’s obligations, but those of tomorrow as well

MANAGE
Support client data privacy obligations by providing a managed services/outsourced option to the GC and CIO groups

OUR STEPS TO SUCCESS

1. Establish a formal inventory of data processing operations and supporting systems that collect, process and store personal data
2. Perform a current-state analysis against the requirements to identify gaps and develop a roadmap to achieve compliance
3. Implement appropriate solutions to remediate gaps and achieve compliance. Establish all components of data privacy compliance program
4. Conduct ongoing monitoring of compliance data, privacy protection and changes to legal obligations
Our Data Privacy team understands the inherent risks clients face and the challenges they encounter in developing and maintaining effective privacy programs. Drawing on our skills and experience in regulatory compliance, business processes, technology, information security and communications, we assist our clients in building and sustaining privacy programs that address both regulatory requirements and industry best practices.

A global insurance company with operations, customers and employees in 23 countries needed to create an effective data privacy program that addressed not only U.S. data privacy regulations, but global regulations as well. Trying to meet the individual regulations using a “one-off” approach was not only legally risky, but also inordinately expensive.

The nature of data processed globally by the organization, along with the complex, overlapping legal jurisdictions (e.g. CCPA, FCRA, GDPR, etc.) that they fell within, required a common, comprehensive and flexible data privacy compliance approach. In addition, the company needed global training and communications, governance and strategic support.

Developed an executive report summarizing the organization’s privacy requirements and potential risks, educating leadership on an effective path to compliance

Produced a detailed analysis addressing key privacy compliance gaps and root causes, along with a remediation plan

Implemented a common and flexible data privacy compliance program globally

Introduced a vendor-contract review program, including a standardized assessment template and DPIA template framework and approach

Created a managed services model to support customer requests

Issued detailed and executive data privacy regulatory assessment reports

Increased enterprise data privacy awareness across the organization using state-of-the-art organizational change management techniques

Implemented effective and flexible data privacy compliance program globally

Established a managed services/outsourcing model that moved data subject requests processing to Protiviti

BUSINESS RESULTS
DATA SECURITY

CLIENT PROBLEMS WE SOLVE

Design, implement, operationalize and validate data security technology and programs supporting PCI, HIPAA, GLBA and FTC compliance requirements

Implement data governance and protection

Design and implement security architecture, including physical and cloud firewalls, security engineering and zero-trust network design

BUSINESS OUTCOME

ENVISION
Understanding of data collection, processing and applications in scope; identification of compliance gaps and remediation steps to achieve compliance

REALIZE
Implementation of improvements and solutions to protect data

PROTECT
Data protection controls embedded throughout the organization

OUR STEPS TO SUCCESS

1. Determine security goals and objectives and translate them to technical requirements

2. Determine gaps between current processes, tools, architecture and desired outcome

3. Architect a technical solution including sourcing third-party products

4. Implement and test the technical solution
Our Data Security services help companies preserve business value by protecting sensitive data and ensuring compliance with respective regulations. Our offerings address the design, implementation and assessment of technical and procedural controls focused on identification, classification, protection and compliance for sensitive data. We bring expertise in security and privacy regulations as well as innovative approaches for reducing compliance obligations and risk.

**CLIENT CHALLENGE**

A global technology company was unable to address the totality of their security compliance requirements. The company lacked both the knowledge and the headcount necessary to address its customers’ vast and disparate compliance requirements, which included FedRAMP, PCI, SOC 1 & 2, HITRUST, ISO 270001, alignment with FFIEC, and several others. This, combined with strong growth projections for the organization, required the company to expand its current team and also consider how to respond to future compliance maintenance necessities without constantly having to add headcount.

**SOLUTION DELIVERED**

Fielded a team of Protiviti professionals qualified to support the required security standards

Facilitated interactions between the client process and control owners and third-party certification/attestation bodies

Developed standardized reporting and communication protocols for tracking compliance status, ensuring leadership is made aware of progress and potential roadblocks

Analyzed repeatable compliance processes that could be standardized and offshored

**BUSINESS RESULTS**

Key security compliance deadlines were met

Increased support for control and process owners, allowing them to focus on their own operational goals and objectives

Client’s customers were able to place more reliance on the organization’s control environment
CLOUD SECURITY

CLIENT PROBLEMS WE SOLVE

The proliferation of services and features available on cloud platforms, coupled with underinvestment in training on how to protect specific use cases, leads to unmanaged complexity.

Lack of visibility into the type of information being processed in the cloud and which users have control to manipulate data, services and infrastructure results in poorly governed cloud footprints.

Organizations are not taking advantage of the efficiency and effectiveness opportunities that exist through automation and orchestration, and the outcome is manual, people-dependent processes that do not scale.

BUSINESS OUTCOME

ENVISION
Improved confidentiality, effective controls over information access, and compliance with legal and regulatory mandates.

REALIZE
Reduced risk of data and system compromise; greater confidence in security effectiveness due to automation and coverage of security controls.

PROTECT
Business-critical information assets are operating in a secure environment.

OUR STEPS TO SUCCESS

1. Design secure architecture for cloud services, focusing on customized global standards for systematic identification, prevention, detection and recovery of threats.

2. Assess, design and implement security solutions to ensure confidentiality, accessibility and integrity of data and information on cloud.

3. Make software security a core path of the software delivery process, ensuring security controls are implemented during the software development lifecycle.

4. Utilize distinct processes to identify, create and maintain the ability to quickly and efficiently react to vulnerabilities while accomplishing business goals.
Cloud security expands beyond the technology. Cloud security is about designing and implementing a collection of deterrent, preventive, detective and corrective security controls that help to protect the cloud ecosystems and its services (SaaS, PaaS and IaaS) from being exploited by attackers. Our Cloud Security services help clients understand, address and actively manage the risks they face to successfully operate their business in a secure cloud. We assess, design and implement security solutions to reduce exposure and communicate effectiveness to stakeholders at the management and executive levels.

**CLIENT CHALLENGE**

A global consumer goods conglomerate was advancing the execution of its digitization strategy (which included defaulting to SaaS, PaaS and IaaS options for new IT projects). However, this organization had not designed or implemented protection, secure provisioning and governance frameworks to align with the speed of deployment and to guard against business disruption. As a result, the organization was seeking a partner to develop control governance framework and a technical cloud security reference architecture to support their “cloud first” digital strategy.

**SOLUTION DELIVERED**

Developed foundational cloud security controls for SaaS, PaaS and IaaS cloud computing categories

Designed identity, information protection and operations security reference architectures to meet security requirements and incorporate budgetary and risk-based decision criteria

Analyzed and documented use of "sanctioned" versus "unsanctioned" applications to ensure compliance with internal and regulatory requirements

Developed standardized reference architectures to provide stakeholders with security principles that can drive self-service assessments

**BUSINESS RESULTS**

Accelerated decision making for product teams and stakeholders, thus eliminating the cybersecurity team as a bottleneck for innovation

Created detailed roadmap to support ongoing journey to maturity of the cloud security program and reduce probability of noncompliance with HIPAA, PCI and GDPR

Documented security capabilities for SaaS, IaaS and PaaS platforms to enable benefits of modern technologies without diminishing security of customer information

Developed common language for executives and business stakeholder to discuss governance of their digital transformation initiatives
DIGITAL IDENTITY

CLIENT PROBLEMS WE SOLVE

Effective management or reporting of user access, access privileges, audit trails, and when or how privileged accounts are being used, including by third parties hosting client servers or applications

Remediation of audit or regulatory requirements for controlled access or least privileged

Changes in security management due to mergers, acquisitions or divestiture of business entities

BUSINESS OUTCOME

ENVISION
Assess and baseline current environment to identify gaps; develop IAM program strategy with a centralized onboarding approach and control framework

REALIZE
Reduced risk of data breach with an improved security posture, including efficiencies on the organization’s access lifecycle; reduced reliance on manual controls

PROTECT
Establish single view of user’s access catalog; implement automated solutions to manage access

OUR STEPS TO SUCCESS

1. Define IAM strategy and roadmap
2. Develop IAM operating model
3. Implement IAM and PAM solutions; remediate compliance issues
4. Establish governance model to support business objectives
Our Digital Identity services include best practices, frameworks and tools to maintain identity, privileges and assets that are essential to protecting sensitive data and secure information in a compliant and cost-effective manner while providing adequate protection and an optimal user experience on a variety of applications and tools, whether on premise, in the cloud, via mobile or on their own devices.

CLIENT CHALLENGE

This global specialty hospital corporation had recently been spun off from its parent and had two years to implement its own IAM program, systems and processes. Although the client had its own subdomain, many of its systems and users were joined to the parent’s corporate domain; identity governance technologies and IAM processes were owned and operated by the parent company.

SOLUTION DELIVERED

Selected and implemented IAM solution for provisioning for Active Directory and 110 business applications and systems

Supported the migration of Active Directory domains

Implemented IAM governance model and reporting to monitor access

Timely migration to new domain and implementation of provisioning solution

Creation and implementation of “run books” to standardize the migration of users, computers and applications to the new domain

Automated provisioning for distribution lists and shared drives

BUSINESS RESULTS
ATTACK AND PENETRATION

CLIENT PROBLEMS WE SOLVE

Help organizations gain an understanding of their specific threat landscape, including security vulnerabilities, root causes and remediation options

Protect sensitive data and systems to avoid costly breaches, loss of intellectual property, business disruption and reputation damage

BUSINESS OUTCOME

ENVISION
Understanding of security vulnerabilities and specific threat landscape, including how potential issues may impact businesses

REALIZE
Remediation of security vulnerabilities and threats in the environment

PROTECT
Reduced risk of data breaches

OUR STEPS TO SUCCESS

1. Periodic internal and external vulnerability assessments or manual penetration tests of the environment

2. Consistent, on-demand security testing across networks, applications, IoT, hardware and more

3. A managed, risk-based testing program with remediation oversight to maximize ROI
Our Attack and Penetration team helps companies protect their critical assets and data by identifying vulnerabilities and providing actionable remediation guidance. Applications, services, databases, the Internet of Things (IoT) and mobile devices, whether on-premise or in the cloud, are safer with Protiviti.

**CLIENT CHALLENGE**

A global supermarket chain was undergoing significant technology change which required a number of investments and updates to applications, systems and networks. The Security team was tasked with deploying a method to ensure that the new technologies were being implemented in a secure manner that prevented unauthorized access. However, the team was not able to quickly source or train the talent needed to perform these technical reviews on such a wide array of technologies. The client needed an “on-demand” solution that would allow it to quickly spin up testing and meet dynamic business deadlines.

**SOLUTION DELIVERED**

Developed penetration testing-as-a-service solutions that allowed the client to respond to changing needs

Deployed red and purple teams to aggressively challenge plans, policies, systems and assumptions while verifying the technologies’ capabilities

Developed network-level testing and static web application assessments

Implemented wireless reviews for various stakeholders within the client organization

**BUSINESS RESULTS**

A defined process for business and IT leaders to assess new technologies before implementation to better understand risk and impact of potential vulnerabilities

Significant reduction in the organization’s overall security risk through the identification of hundreds of critical network, system and application vulnerabilities which might have allowed attackers access to sensitive systems and data if left undiscovered or unfixed

A more thorough understanding of potential business impact (data loss, significant system downtime, etc.) for known/accepted issues in the environment

In many cases, confirmation that technologies have been designed, configured and deployed in a secure manner
MANAGED SECURITY SERVICES

CLIENT PROBLEMS WE SOLVE

Keeping pace with changing business demands
Limited market availability of qualified resources; staff retention challenges
Rapid responses necessary to satisfy critical functions, including critical security incidents and IT risk management and controls
Immediate demand for solutions to secure and protect assets and data

BUSINESS OUTCOME

ENVISION
Scalable, contractual teams and services in simple solution frameworks with skilled resources

REALIZE
Optimize the delivery of repeatable processes, emerging compliance changes and transformative business process changes

PROTECT
Optimize compliance activities by successfully achieving business strategies and objectives

OUR STEPS TO SUCCESS

1. Scan digital technology infrastructures for existing vulnerabilities and remediate cyber threats
2. Build a unified security program that increases visibility, automates threat detection and response, and delivers actionable metrics for continued improvement
3. Monitor cloud resources to continuously assess and measure data, applications and infrastructure behaviors for potential security threats
Our Managed Security Services are scalable, contractual services which provide for a reduction in complexity and increased access to deeply skilled resources, while being delivered at a significantly reduced and predictable annual fee. Protiviti uses market-leading analytics, metrics and techniques to embed risk and compliance controls with business objectives. This allows for better response to dynamic business process changes that are continually monitored, ensuring correct controls exist to mitigate risks. Protiviti helps clients respond to dynamic compliance and business process changes, as well as optimize their compliance activities to successfully achieve their business strategies and objectives.

**CLIENT CHALLENGE**

Improving overall enterprise resiliency and providing additional capabilities for the client’s current security operations center (SOC) to accelerate identification and remediation of its critical Tier 3 security events.

Engagement is technically complex within the customer outsourcing network infrastructure, with two outsourced network service providers providing critical services.

**SOLUTION DELIVERED**

Developed incident identification and incident response playbooks

Implemented tools in third-party SIEM platform

 Developed procedures for Tier 3 event ID and response

Managed response execution by setting up a scalable onshore/offshore response capability

Performed threat hunting within the internal network

**BUSINESS RESULTS**

Provided a unique Managed Detection and Response (MDR) offering, leveraging onshore and offshore capabilities

Adjusted delivery model and team composition as MDR services scaled up

Embedded scaling factors based on number and complexity of client MDR requirements

Expanded vendor partnership
INCIDENT RESPONSE AND CYBER RESILIENCE

CLIENT PROBLEMS WE SOLVE

- Uncertain organizational response to handling security incidents and related outages
- Unseen threat actors may have bypassed traditional defenses and detection
- Complex security incidents requiring specialized skills, tools and knowledge
- Rigid incident response programs are unable to counter dynamic threats
- Lack of business continuity and/or resiliency strategies, documentation and response plans

BUSINESS OUTCOME

- ENVISION
  Discover and respond to otherwise unseen cyber attacks and related outages
- REALIZE
  Effective strategies for detecting and responding to threat actors; coordinating the entire organization’s reaction to security incidents, from initial discovery through reporting to the Board; ensuring continuity and resiliency plans are well designed, documented and tested
- PROTECT
  Enhance confidence in the business by offering strategic planning, meaningful practice, detection of unseen attacks through compromise assessments, and comprehensive response to actualized threats, while ensuring continuity and resiliency plans are in place to protect the enterprise

OUR STEPS TO SUCCESS

1. Incident response strategy and planning; business continuity and resiliency planning
2. Compromise assessment; tabletop and breach response; cyber threat hunting
3. Forensic discovery and analysis; post-event review and facilitated lessons learned
4. Documented and tested business continuity and resiliency plans
Our Incident Response and Recovery services help companies prepare for, respond to and recover from security incidents. When bad things happen, a trusted partner like Protiviti guides organizations through the process to help avoid costly pitfalls and recover as quickly as possible.

**CLIENT CHALLENGE**

A global e-commerce provider was approached by acquiring banks about common point-of-purchase correlations, indicating that the provider may be compromised. The client needed to:

- Identify PCI gaps and deliver remediation as a demonstrable act of diligence
- Develop and implement a global strategy to identify the alleged breach
- Gather information for external counsel to use in formulating a regulatory response
- Preserve evidence under the direction of counsel for anticipated litigation
- Develop strategic guidance in conjunction with counsel during an independent PFI investigation

**SOLUTION DELIVERED**

Provided on-site team in forensic/incident response and PFI investigations to build a response strategy

Gathered global evidence preservation and tracking for regulatory, PCI and potential litigation strategies

Delivered a security remediation program to establish diligence in response

Provided articulation and support for key elements of external counsel’s strategy for answering requests from privacy regulators

Provided interpretation and articulation of cyber threat intelligence used to identify the true source of the CPP data, establishing that client systems were not breached

**BUSINESS RESULTS**

Privacy regulators accepted the assertion that global systems were not the source of data exposure

Avoided millions of dollars in potential PCI fines by making timely and accurate disclosures

Presented an accurate narrative of events that was legally defensible, and defused negative publicity

External counsel received demonstrably accurate answers to questions during the formation of strategy
OPERATIONAL RESILIENCE

CLIENT PROBLEMS WE SOLVE

The ability to detect, respond to, manage and recover from a disruptive event, whether initiated from cyber, natural disasters, technology or human error

Aligning with new and evolving regulations with regard to operational resilience

Taking advantage of opportunities to increase resilience of business services through trusted approaches and innovative solutions

Integrated testing efforts, which allows firms to demonstrate their ability to recover from events and improve upon weaknesses in current processes and services

ENVISION
Assess current practices around operational resilience, including assessment of foundational elements

REALIZE
Analyze existing business services to determine criticality, establish initial impact tolerance methodology, and create economic impact scenarios
Design and implement a resilience program with a focus on governance and alignment
Address cyber resilience and third-party deficiencies

PROTECT
Conduct testing to simulate “extreme but plausible” scenarios impacting critical business services; in partnership with executive leadership, integrate resilience standards into all standard business and IT audits and foundational audits (e.g., cybersecurity, third-party)

OUR STEPS TO SUCCESS

1. Establish a clear understanding of critical business services, including a clear front-to-back mapping of processes, third parties, and systems that support the service

2. Take advantage of and adapt to existing programs and initiatives to better integrate resilience into the environment

3. Build resilience by designing and implementing essential programs to withstand adverse changes

4. Orchestrate across the enterprise on operational resilience. Break down silos that exist across business and technology functions
Facing a complex, dynamic system, our Operational Resilience services help leaders confidently prepare for and respond to known and unknown futures through an iterative process that improves an organization’s ability to proactively withstand adverse change.

**CLIENT CHALLENGE**

This global and systemically important financial institution had been given a regulatory mandate to address the operational resilience of their organization. This mandate, driven by the first line, included assessing planned initiatives against leading practices and enhancing plans where necessary; helping to draft regulatory responses; developing a go-forward strategy for the first line, including criticality framework, resilience operating model and testing approach; and working with the second line to develop appropriate metrics to monitor resilience and challenge first-line efforts.

**SOLUTION DELIVERED**

- Performed a current state assessment of operational resilience efforts, benchmarking against regulatory expectations and leading practices
- Created a go-forward plan that accounted for work efforts to date and organizational/system limitations to address resilience concerns
- Embedded Protiviti consultants and subject matter experts across the delivery workstreams, aligning the client’s efforts with operational resilience leading practices and regulatory expectations from a global set of regulators
- Aligned regulatory response with pragmatic go-forward efforts, ensuring plans exceeded regulatory demands

**BUSINESS RESULTS**

- Created a global resilience strategy and operating model to align the organization with pending regulator demands
- Provided guiding principles, frameworks and industry/regulatory insights to allow for advancement of resilience efforts and enhanced board/management reporting
- Created a framework to address and validate the organization’s critical business services
- Developed a customized strategy and approach for resilience capability testing
OUR KEY PARTNERS

Gold Microsoft Partner

paloalto®

SailPoint

OneTrust
Privacy Management Software

RELIQUEST

netskope®
ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Through its network of more than 85 offices in over 25 countries, Protiviti and its independent and locally owned Member Firms provide clients with consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of Fortune 1000® and 35% of Fortune Global 500® companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.