Spotlight on Security

A Modern Approach to Threat Protection, Detection, and Reaction

1.800.800.0019
www.govconnection.com

GovConnection™
A PC CONNECTION COMPANY
we solve IT™

Why Choose PC Connection, Inc. Security Solutions and Services?

With the continuous state of change in the global threat landscape, organizations face cyber attacks and security breaches that are growing in frequency and sophistication every day. PC Connection, Inc.'s Security Practice offers solutions and services to counteract increased risk proliferation. Our team of experts has designed industry-leading assessments, analysis, technology planning and integration that focus on a unified and centralized solutions approach, risk management guidance and oversight, including managed security services to combat attacks and prepare for the unknown.

As a trusted partner with more than 30 years of experience, we can help you identify vulnerabilities in your environment and determine which ones are exploitable and dangerous. Then we can proactively develop a prioritized action plan to support your organization's ability to define, document, and manage acceptable risk requirements.

Based on your organization's needs, environment, business process, and security goals, our experts will provide insights to help you implement the right solutions to address your critical risks and protect your operations. As an extension of your IT team, we're committed to keeping your organization operating safely and securely.

PC Connection, Inc.™
we solve IT™

Customized technology solutions and services
are available through the PC Connection, Inc. family of companies.

PC Connection™ GovConnection™ MoreDirect™

Managing the Complete Threat Lifecycle

A comprehensive approach to security requires solutions and services that ensure the safety and security of your data, infrastructure, and user experience throughout the complete threat lifecycle. We can help you manage those threats with the three pillars of security management: Protect, Detect, and React. Gone are the days when a single layer of defense was enough to keep intruders out of your data. Together, these three pillars form a cohesive, interdependent approach to information security, ensuring that you don't just deploy technology to address security-point issues, but manage your technology to prevent a security event from becoming a security epidemic.

The 3 Pillars of Security Management

PROTECT—Our security experts identify, document, and analyze your security risks—and define the people, processes, and technologies necessary to bring that risk into the acceptable range with a suitable protection strategy. We focus on a unified security stack approach with technology that integrates, communicates, and correlates critical security information and events to keep your data safe.

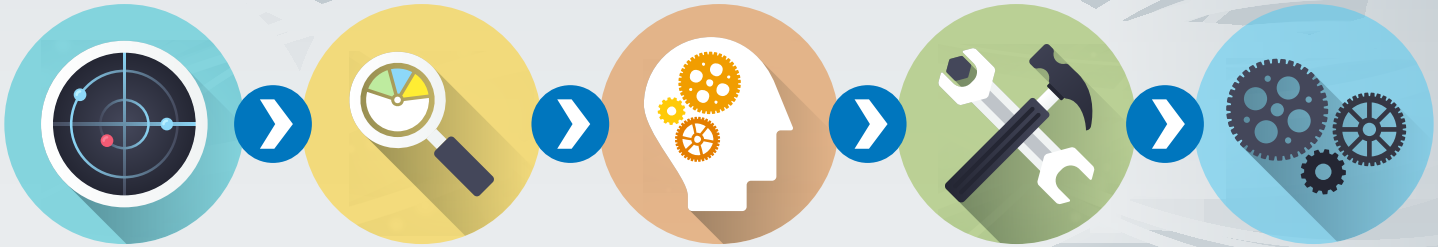
DETECT—Simply protecting your critical assets and data is no longer an adequate plan to protect your organization from today's evolving threats. You must also implement the appropriate solutions to detect when security events or breaches occur. This involves people, process, and technology all unified under one common process to keep your risk at an acceptable level.

REACT—It's no longer a matter of if a breach will occur, it is only when. You must create your security program to expect that breaches will happen, and when they do, you must be prepared to react quickly and decisively to lock the breach down and prevent compromise of critical systems or data. Keep a "security event" from becoming a "security epidemic". PC Connection's Security Assessment, unified security stack, and program services empower your organization with effective strategies and services to manage your risk 24×7×365.

5 Steps to Success

PC Connection addresses your full security risk lifecycle through a five-step process:

Discover, Assess, Remediate, Implement, and Manage



1. DISCOVER—Our experts work with you to conduct a security penetration test and vulnerability risk analysis to determine what vulnerabilities exist across your organization—external, internal, and wireless—and then determine what active exploits are available against those vulnerabilities. In short, how does the cybercriminal get past your defenses?

2. ASSESS—Next, we help you assess risk liability by prioritizing vulnerabilities based on ease of exploitation and exposure to critical systems or data. In other words, which risks need to be addressed immediately?

3. REMEDIATE—With agreed upon priorities, we build a remediation plan to address those risks with appropriate mitigation strategies. This plan is then circulated for approvals to ensure all stakeholders are also in agreement. In addition, we are ready to assist you with remediation execution as necessary.

4. IMPLEMENT—Our experts work with your team to implement solutions that bring risk to an acceptable range, based on the approved plan, in lockstep with your organization's policies and controls.

5. MANAGE—With a security solution in place, we facilitate the final—and most critical—step in your security strategy. Our industry-leading Managed Security Services reduce the burden of ongoing protection, empowering you to manage your risk, day over day, month over month, and year over year. In contrast to quarterly threat scans and annual audits—which are merely reactive ways to provide your organization a snapshot-in-time perspective on how well you are managing risk—a fully managed security solution gives you a proactive perspective of where you stand with your risk management and compliancy requirements, 24×7×365. For organizations required to comply with HIPAA, PCI, GLBA, or FISMA, this provides the complete picture of your organization's ability to stay in compliance over time.

Comprehensive Security Solutions and Services

Our portfolio of security services and solutions is fully managed by our in-house experts and delivered by our nationwide network of PC Connection, Inc. premier partners. Our security offerings include:

- Unified security stack solutions
- HIPAA Security Assessment
- PCI Security Assessment
- GLBA Security Assessment
- FISMA Security Assessment
- Penetration and vulnerability testing
- Application Security Assessment and code review
- Data Loss Prevention Security Assessment
- Network Security Assessment
- Wireless Security Assessment
- Security policy, program, and risk governance development
- Managed Security Services

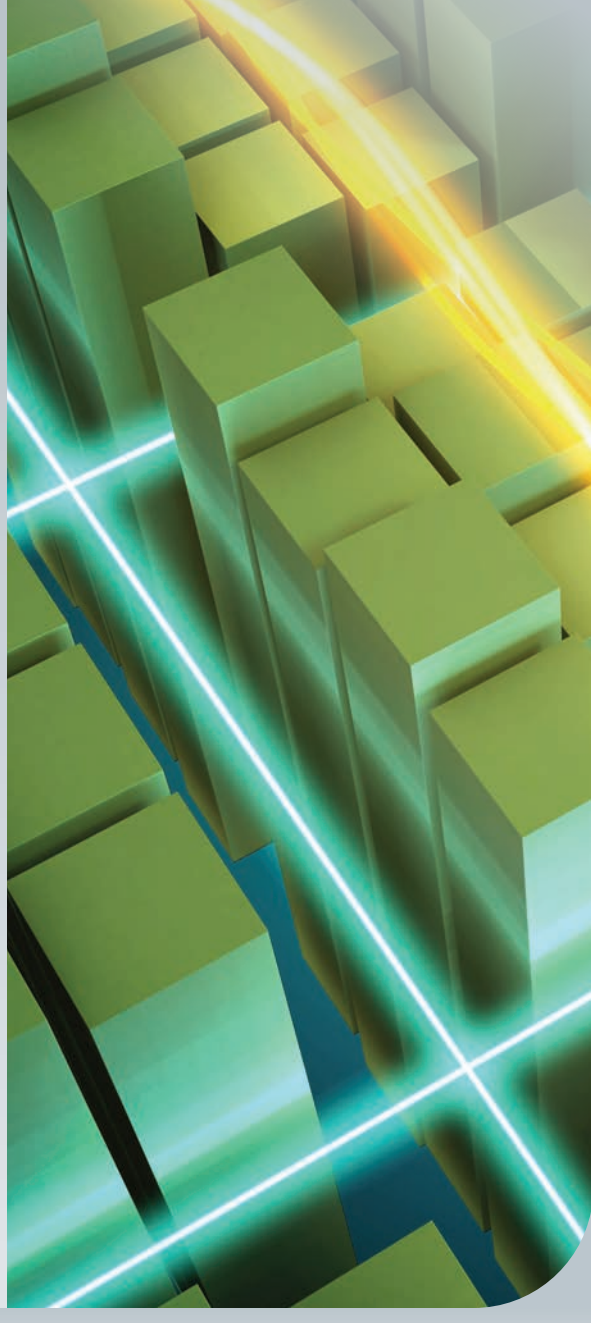
Today's security professionals—Director of IT, CIO, Director of IT Security, and CISO—often struggle with not only the identification of vulnerabilities, but also comprehension around how those vulnerabilities translate to threat vectors that can impact their environment. The true cost of a security breach goes well beyond financial damages, often with a lasting, adverse impact to customer and partner relationships and significant regulatory penalties. We offer the guidance, resources, and tools to help you manage risk, reduce costs, and build a more stable and secure information security program.

Your Unique Environment, Our Expertise

We offer security services to address the most critical security needs, stringent compliance requirements, and complex technology challenges across many industries. With a deep understanding of your unique environment, needs, and goals, our experts can help you:

Manage healthcare risks and address HIPAA Security and privacy rules, HITECH, and Meaningful Use through:

- HIPAA gap analysis
  - Assess information security program to measure its compliance
  - Identify which systems, processes, and procedures are in scope for HIPAA
  - Review policies, standards, guidance, and procedures
  - Perform spot check on controls
  - Interview key personnel, advise, and selectively measure and audit security controls across defined control areas
- HIPAA, HITECH, and Meaningful Use analysis
  - Penetration and security vulnerability testing
  - Assess risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI and EMR your organization holds
  - Interview key personnel, advise, and selectively measure and audit security controls across defined control areas
- HIPAA risk management
  - Manage/monitor IPS/IDS, firewalls, SIEM, vulnerability scanning, and threat intelligence

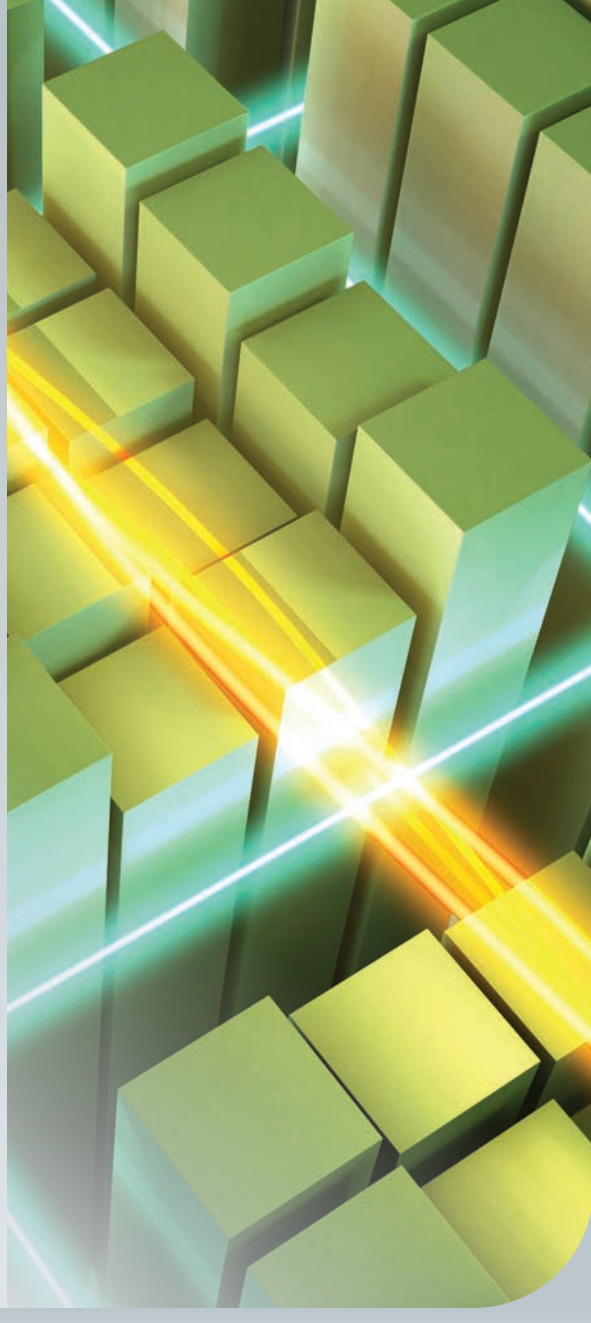


Manage Payment Card Industry (PCI) Compliance in accordance with PCI and Payment Application (PA) Security Standards version 3.0:

- Identify cardholder data and assess IT assets and business processes for vulnerabilities
- Identify which systems, processes, and procedures are in scope for PCI
- Provide a prioritized roadmap for remediation
- Deliver validation reports, QSA support for ROC preparation, and ongoing MSS support

Achieve compliance with government security standards:

- Assess information security program to measure its compliance with FISMA and NIST 800-53
- Perform penetration and security vulnerability testing to assess risks and vulnerabilities to the confidentiality, integrity, and availability of critical data
- Review policies, standards, guidance, and procedures to ensure compliance
- Perform spot check on controls
- Interview key personnel, advise, and selectively measure and audit security controls across defined control areas

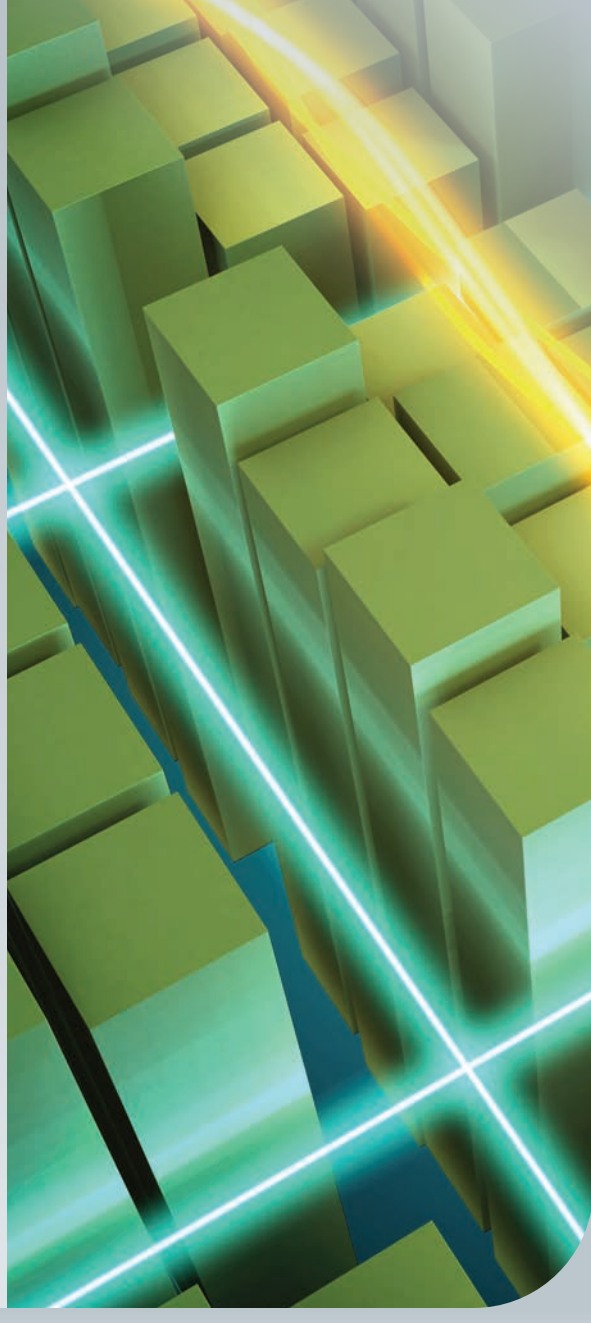


Achieve compliance with GLBA and FFIEC standards:

- Assess information security program to measure its compliance with GLBA and FFIEC standards
- Perform penetration and security vulnerability testing to assess risks and vulnerabilities to the confidentiality, integrity, and availability of critical financial and personal data
- Review policies, standards, guidance, and procedures to ensure compliance
- Perform spot check on controls
- Interview key personnel, advise, and selectively measure and audit security controls across defined control areas

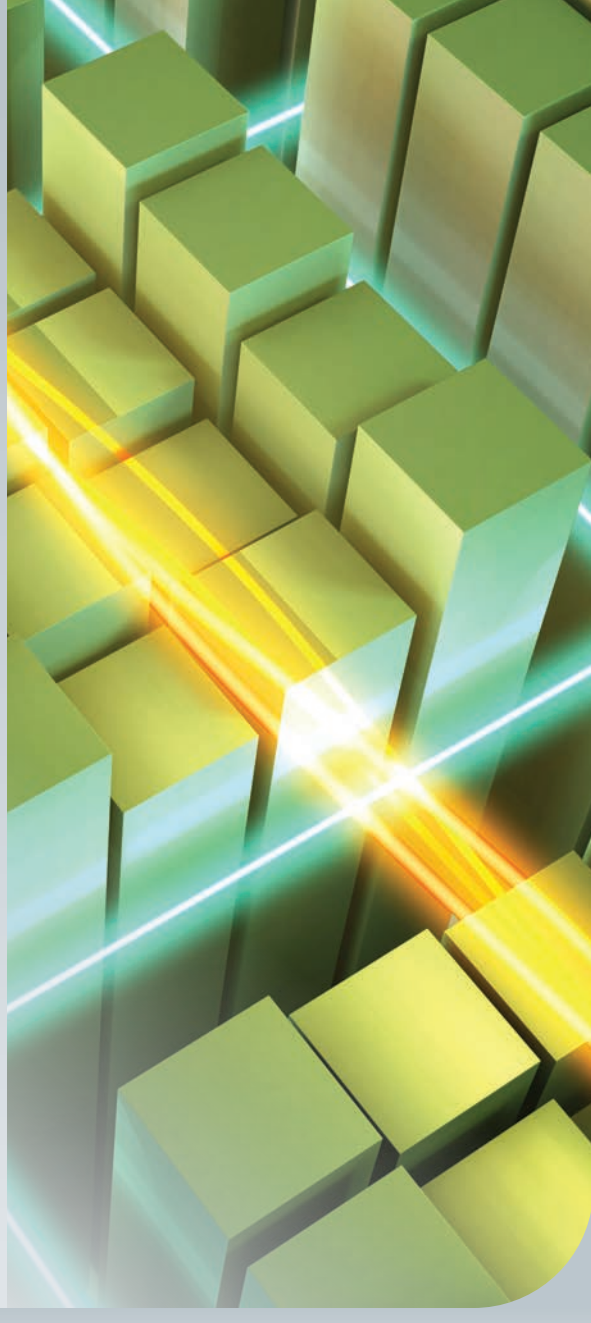
Unified security stack—review and deploy solutions to:

- Provide real-time visibility and automated situational awareness
- Improve staff focus/expertise
- Reduce operational security costs—volume/package pricing; improve stack ROI
- Leverage flexible "suite" licensing models; lower security stack TCO
- Reduce FTE demand to manage stack
- Provide an integrated solutions approach
- Consolidate security management
- Reduce number of dashboards
- Improve compliance and policy enforcement
- Enhance coordination for disaster recovery



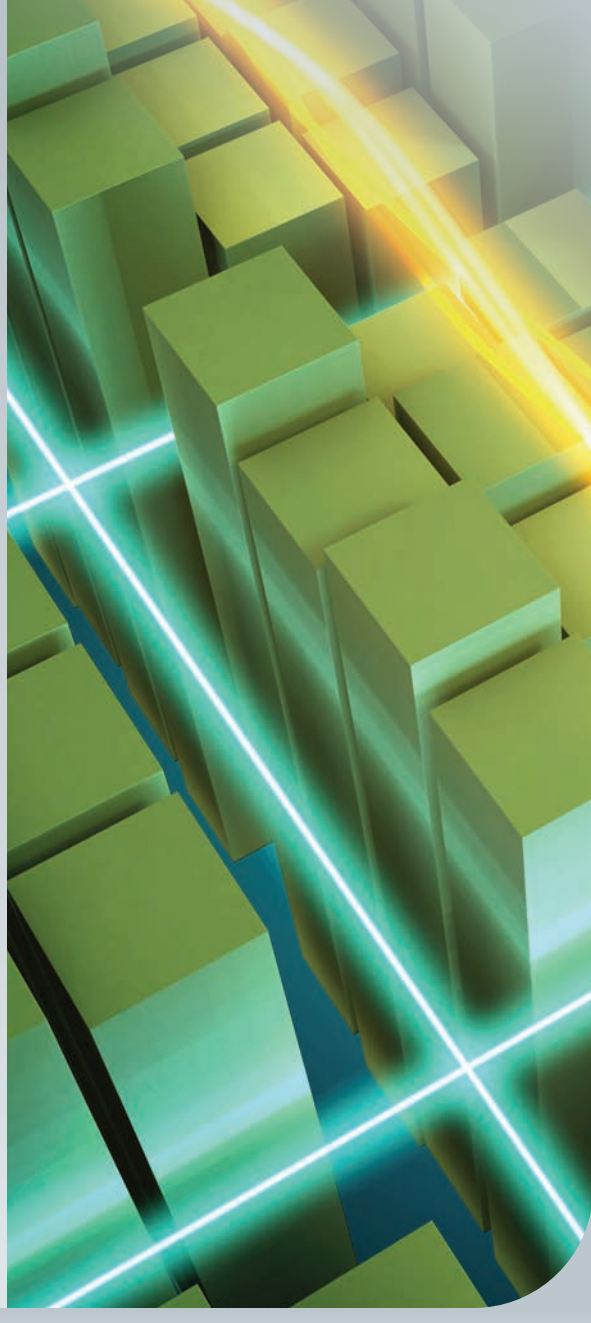
Security testing and assessments:

- Penetration and vulnerability testing (to include wireless)
  - Internal and external testing and risk analysis
  - Exploitation or attack risk analysis
  - Risk enumeration and prioritized remediation plan
  - Reporting (to include detailed vulnerability enumeration)
- Application security testing and secure code review
  - Build a threat model
    - Identify key security requirements and threats
    - Create a threat model that documents attacks that could be carried out
  - Build assessment action plan
    - Convert potential threats into action plan
    - Test against the conditions of attack described in the threat model
  - Execute assessment
    - Execute attacks as described in the action plan
    - Discover vulnerabilities, explore for variations
  - Report results
    - Document findings and remediation recommendations



Security governance, risk, and compliance:

- Security risk governance program
  - Help build a strategy that has full executive support—documented and managed
  - Top down direction
  - Timely decision enablement and buy-in from all senior management, business units, technical departments, and security risk owners
- Security risk management and compliance program
  - Help build a strategy that has full executive support—documented and managed
  - Business and cross-functional direction
  - Documented and managed "risk register"
  - Timely decision enablement and buy-in
  - Security compliance management program
  - Integrates with risk governance program
  - Budget, planning, and execution of required compliance audits (e.g. PCI, HIPAA, FISMA, etc.)
- Information security program and policy development
  - Information security program and policies—documented and managed
  - Development of industry standard security policies
  - Employee education and awareness training
    - Prepare employees to recognize threats and attacks
    - Provide employees with action plans



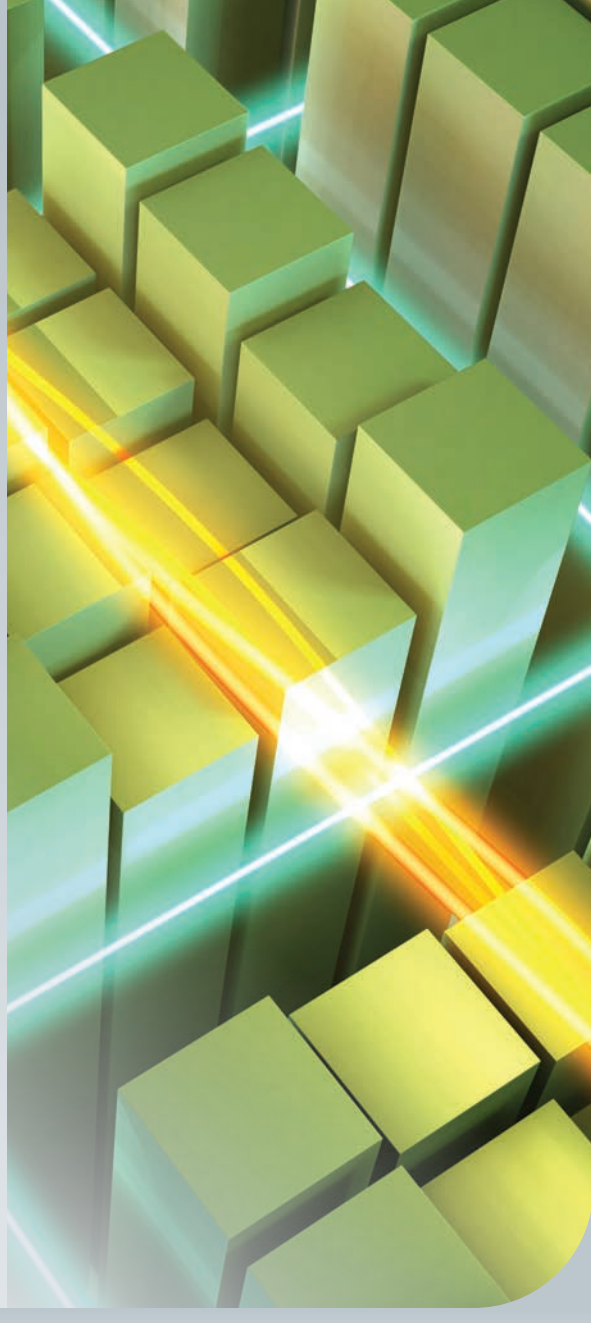
Managed Security Services—protect your environment 24×7×365:

We offer the following managed services to provide constant vigilance and protection for your critical information assets and data:

- 24×7 security monitoring
- Advanced endpoint threat detection
- Log management
- Managed advanced malware protection
- Managed SIEM
- Managed server protection
- Security device management
- SIM on-demand
- Vulnerability management
- Vulnerability prioritization
- Web application scanning

Your Trusted Security Partner

Protect your organization from today's evolving security threats with guidance from our experts. We are committed to keeping our Security Practice on the cutting-edge, because we understand the threat landscape changes on a daily basis. Our experts rely on the most sophisticated, innovative tools and strategies, ensuring we're able to meet your changing needs day after day. Contact an Account Manager to learn more about our complete offering of security solutions and services.



About PC Connection, Inc.

As a leading National Solutions Provider, we've been trusted for more than 30 years to connect people with technology that enhances growth, elevates productivity, and empowers innovation. PC Connection, Inc., a Fortune 1000 company, has three sales companies: PC Connection Sales Corporation, MoreDirect, Inc., and GovConnection, Inc., headquartered in Merrimack, NH, Boca Raton, FL, and Rockville, MD, respectively.

PC Connection, Inc.™
we solve IT™

Customized technology solutions and services
are available through the PC Connection, Inc. family of companies.

PC Connection™ GovConnection™ MoreDirect™