connectis

Cyber Security Professional Services

Eliminate Threats Early Before Damage Control Is Required

THREAT MANAGEMENT SERVICES OVERVIEW

As a Canadian company headquartered in Toronto, Canada, Connectis Group provides detailed security assessment services and technical security solutions focused for organizations concerned with maintaining brand reputations, prevention of data breaches, defining strategies to reduce risk and ensure client services are compliant.

Most capable network and endpoint security architectures will inevitably be compromised at some point, even though security architectures emphasize early detection of compromise or abuse. Our assessment techniques utilize industry best practice methodologies, recommend actions that mitigate risk, and provide an analysis of those actions including the recommended implementation steps to avoid compromise.

***Services include**:*

Vulnerability Assessment

Before you can protect your infrastructure environment, your IT Team needs to know what to focus on, hardening servers is just the start.

Engage Connectis to provide a Vulnerability Assessment to analyze all your network devices, web applications for weaknesses that need the attention of your IT Team or Connectis to remediate.

Once you've provided your device IPs and credential access to your apps, our analysis will begin. Our detailed Summary of Findings report is of value to both management and your IT Team and includes the number and detailed description of vulnerabilities found, classified in terms of severity and risk to your organization and along with clear steps on what and how repairs must take place to secure your environment. Although Vulnerability Assessment services can be run once, it's highly recommended to be run quarterly as network environments dynamically change. Services are available as both Credential and non-Credential scans.

IN BRIEF

- *Vulnerability Assessment*
- *Penetration Testing*
- *Network Configuration Review*
- *Network Security Architecture Review*
- Physical & Data Center Security
- *Cloud App / Server Security*
- *Data Loss Prevention (DLP)*
- PCI ISO Compliance Validation
- *ISO 27001 Implementations*
- *GAP Analysis*
- Risk Assessments & Program Advisory
- *PCI-DS Implementations*
- Security Awareness & e-Learning
- Backup & Disaster Recovery
- Antivirus & Antispam Protection

connectis group

When performing analysis on your web applications we review each critical component, using manual techniques, proprietary and commercial tools, and custom programs created uniquely for an application, we pinpoint specific vulnerabilities and identify underlying problems.

Our assessments are based on open source security frameworks like OWASP 10 and other to check for vulnerabilities in the areas of configuration management, authentication, authorization, data protection, data validation, user and session management and error and exception handling. The tests that cover each of these areas are usually performed first without proper authentication credentials for the application and then, with valid authentication credentials for each role within the app.

Security Configuration Review

For organizations that require regular quarterly reviews of network and app infrastructure, Connectis can provide a Security Configuration Review and report on the current state of network device configurations, gaps and server hardening to protect against targeted attacks. Security is compromised when devices are left at their default settings, have been misconfigured, or servers may use weak passwords and default accounts.

Penetration Testing

We'll find your network and web app weakness in a controlled ethical manner before criminals can exploit them. Pen testing differs from Vulnerability Assessment in that we'll attempt to gain access to your systems and app's using various techniques that a hacker might employ. We'll gather our evidence and provide a Summary of Findings, once again, identifying and classifying the weaknesses with recommendations on how to repair each exposure. This critical service should be part of every organizations security strategy and should be performed on a regular basis.

Our significant expertise and experience in Web Application security enables us to comprehensively identify and clearly explain the nature of the security exposures. We follow, maintain and update our methods to ensure we're compliant with the changing industry standards so our services are always based on the current software security framework to ensure our assessments provide comprehensive and valid results.

Although our consultant testers can be creative when leveraging their hacking skills, all are required to follow our methodology to remain consistent. Our Consultants have gained expertise having performed many Web application assessments over the years for clients in financial, e-commerce, healthcare, gaming, and software industries whose applications range from multi-server, load-balanced web farms to single- host kiosks.

Our experience includes Internet deployed applications, intranets, VPN-restricted applications, and co -located systems. Our assessments examine the technical implementation and business purpose of web applications, enabling our Summary of Findings report to provide technical solutions to individual vulnerabilities as well as prioritized remediation strategies based on corporate risk reduction. A discovery meeting with your IT team will reveal the quantity of network devices and web apps to be analyzed, after which we'll provide fees and timing deliverables.

Mobile Application Security

Organizations wishing to achieve a thorough and complete test should request Penetration Testing to include Smart Phone Mobile Application Security Assessments.

Mobile applications may become exposed to many critical security vulnerabilities which can jeopardize the confidentiality and integrity of the data being stored on mobile devices. Smart Phone Mobile apps and platforms are often open to enable many parts of the mobile eco-system to delivering flexible program and service delivery, options that may be installed, removed or refreshed multiple times in line with the user's needs and requirements. However, the same openness produces exposure and

risk to your systems as they integrate with the mobile apps, due to potentially unrestricted access to mobile resources and APIs by applications of unknown or untrusted origin could result in damage to the user, the device, or the network.

Network Security Architecture Review

Over time, all organizations' network infrastructure change. Changes often reflect organizational needs, process changes, resource needs as well as other factors. Typically, these changes are looked at from a tactical standpoint. How do we get from point A to point B as seamlessly as possible? In many cases, security is an afterthought. Network and System changes take place and inadvertently open holes or attack vectors without the knowledge of current systems owners. Even when best of breed security technologies have been implemented won't help if the underlying security architecture is flawed.

During a Security Architecture Review, we'll conduct a systematic examination of all the layers of your organization's network. We'll examine the existing network topology, privilege access management policy, deployment of the security controls within the organization like firewalls, IDS/IPS, network segmentation and make recommendations to increase the effectiveness of the security controls.

Often part of a compliance engagement, we can review the state of your networks' security in regards to how its been architected. We'll identify gaps & potential threats in the existing environment. Evaluate if systems are secured, configured, and patched according to international best practices and security standards.

During a network architecture review, the assessor will evaluate the security of Client network architecture and infrastructure. Existing network diagrams and network documentation will be reviewed and interviews with network security analysts, network engineers, and network architects will be conducted in order to confirm documentation and answer outstanding questions. The network architecture review will evaluate the function, placement, and gaps of existing security controls and compare their alignment with the organization's security goals and objectives. Activities may include:

- Review the latest Threat Risk Analysis report produced from a Vulnerability Assessment or Penetration Test.
- Conduct interviews with Network Administrators focusing on best practices in infrastructure design, and validate the findings from a documentation review and vulnerability scans.
- Analysis of current IT network, information flow according to business requirements and points of access to information.
- Analysis of current security controls and management, policies and procedures related to network design.
- Analysis of existing network security architecture, including topology / configuration, and security components / features, including:
    - Key design assumptions
    - Technology inventory
    - Security administration procedures
    - Network topology
    - Network access controls
    - Authentication and access requirements
    - Host access controls
    - Administrative and maintenance channels
    - Interview / Observations

Physical & Data Center Security

Physical and Data center security services help address client's security requirements in all aspects including protection of personnel, hardware, networks, and data from physical circumstances that could lead to a serious damage.

Our Consultants have completed many physical security engagements using an integrated approach that enables bridging the gap between the client's physical security, IT and their business goals.

Our Consultants follow best practices and standards when helping clients to build Physical Security requirements for Data Centers, systems or sensitive sites.

Cloud App / Server Security

For organizations who's key server applications reside in the cloud, Connectis will provide a Security Audit. The audit will include Vulnerability Assessment and Configuration Review. The gathered information detailed in the final Summary of Findings Report includes:

- Technical Findings classified by severity
- Recommendations on how to remediate

As organizations embrace digital transformation they face challenges to establish an end-to-end security framework for their cloud deployments to protect data and applications. Our Consultants will provide the expertise to ensure the deployments are configured and completed according to best practices and industry standards and ensure any regulatory compliance and privacy requirements.

Data Loss Prevention (DLP)

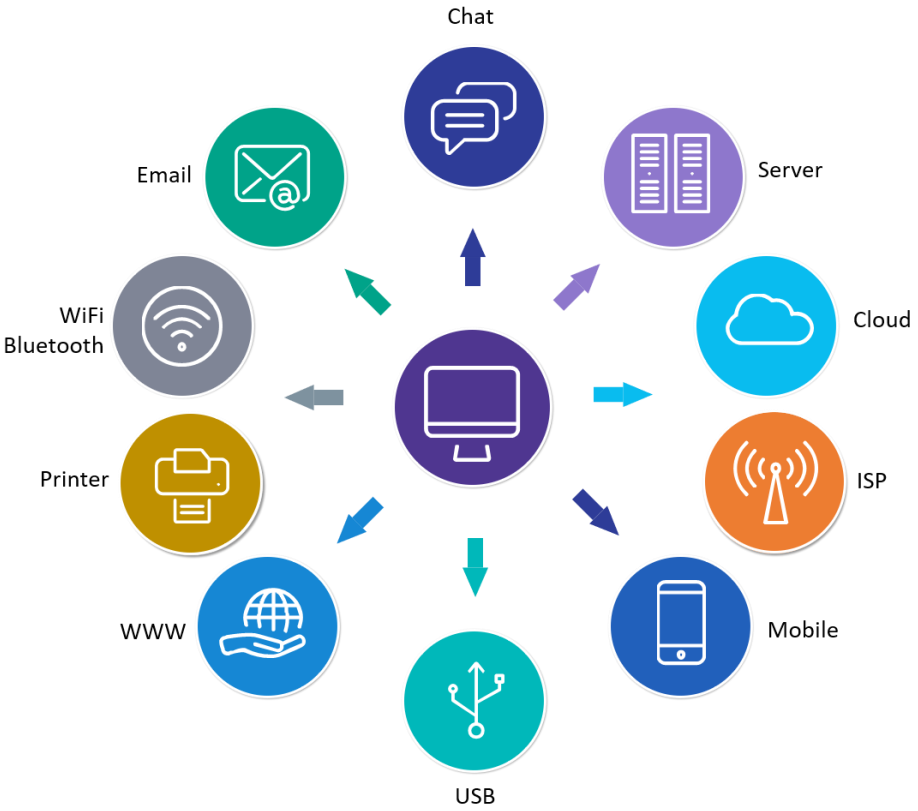
For organizations concerned with the loss or public exposure of important and often confidential data, Connectis will provide a Summary of Findings for Data Loss Prevention. Our service will detect and prevent data breaches, exfiltration, or unwanted destruction of sensitive data, often used to protect and secure data and comply with regulations. It includes identifying and classifying information that is Confidential, Public and Private. Consultants meet with and interview key stakeholders, along with our technologies, gather information on how data at rest and data in motion are stored, how internal systems that push data categorize the classification of the data, recognizing the security implications that must be maintained based on the classification. Our report identifies and makes recommendations to how your policies should control the data flow.

After a DLP service, organizations will be better equipped to defend against data loss and data leakage such as a ransomeware attack.

Organizations typically use our DLP service to:

- Protect Personally Identifiable Information (PII) and comply with relevant regulations
- Protect Intellectual Property critical for the organization

- Achieve data visibility in large organizations
- Secure mobile workforce and enforce security in Bring Your Own Device (BYOD) environments
- Secure data on remote cloud systems



Connectis DLP services help organizations recognize which assets require protection and how to protect them from leakage. Leakage refers to data that's unintentionally pushed out, accessible to theft, easily exposed to download via web apps or USB devices and others.

Service objectives include:

- Advise on the DLP controls required
- Effectively manage data loss risks
- Prevent the intentional or unintentional disclosure of sensitive data
- Maintain adequate security and usability
- Enforce compliance

PCI DSS Compliance

Connectis offers a suite of compliance services to help organizations meet PCI DSS requirements. We not only provide consulting services to audit and comply with PCI, but also work with clients to streamline ongoing compliance maintenance.

We have strategic partnerships with leading Quality Security Assessors (QSA) companies to validate compliance and help align security requirements and business goals to cost-effectively minimize risk and enhance business performance.

ISO 27001 Implementation

Connectis provides ISO 27001 compliance services and implement the full range of controls within this international standard of best practice for information security. Our team of security experts provides a systematic approach to help organizations continuously manage information security.

Connectis has years of experience implementing major ISO 27001 projects with clients from high visibility sectors. Our certified auditors can guide organizations through the certification process and enable them to meet contractual obligations with customers and business partners.

GAP Assessment Analysis

A Gap Assessment can be summarized with 3 questions:

1. What's the state of your network security performance today?
2. What are the security goals you want to achieve down the road, and
3. Define the steps, differences and deliverables needed to close the gap?

Engage Connectis for a GAP Assessment

Analysis to identify 'gaps' in your business action plan. Once implemented, it's expected your business' efficiency, your data / product quality and your profitability will benefit. Once the Report is delivered, discussed and acted upon, organizations will be better equipped to focus resources and energy to areas that will lead to achieving your stated security goals quickly. As with all Connectis Professional Services, our service includes provisioning of our data gathering documents, followed by personal interviews with key stake holders, investigation and analysis of your network devices and apps, followed by the delivery and discussion of our Summary of Findings Report. As in all services, our fees are related to the scope of the network devices, apps and locations involved.

Security Risk Assessment & Program Advisory

For organizations that need to:

- Identify key information risks or constraints that could potentially impair the achievement of your security objectives
- Provide management with insights into risks requiring attention.

The Assessment approach will provide an understanding of the organizational context and departments related processes, from the perspective of the individuals responsible for controlling such risks. Inherent risk is defined as the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.

We'll Identify:

- Conduct meeting with stakeholders that collect data / information related to the current risks
- Map current risks to sectors / departments

We'll Assess:

- Conduct a Risk Assessment Workshop session to assess the likelihood and the impact of the applicable risks considering associated risk drivers.
- Develop Risk Assessment Matrix summarizing risks scores.

We'll Prioritize & Report:

- Prioritize risks based on calculated risks scores
- Map the Prioritized Scores on risk heat map
- Develop detailed Risk Profile
- Develop a risk based mitigation plan

Our risk management capabilities enable organizations to gain a clear insight into the risks they face and make risk-aware decisions more effectively. You'll be able to:

- Develop a proactive program for protecting your environment.
- Identify, quantify and analyze potential vulnerabilities.
- Accelerate and organize risk processes to reduce costs.
- Proactively stop attacks before they stop your business.

Security Awareness Program

Your staff are a line of defense that should be considered to complete any security program. Security awareness is a continuous process that should be regularly evaluated and updated to maximize its effectiveness. Our unique security awareness programs are designed to meet compliance requirements, minimize risks and build skills and knowledge.

We provide on-site Security Advisory Training and online web portal access Security Training services. While the on-site services may be customized to your requirements and environment, our eLearning portal provides anytime anywhere web access to our content. The eLearning Portal can be private labelled. clients build a custom information security awareness program that compasses different components including training, campaigns, reinforcement materials and much more. We aim to address the human element of organizations, create an understanding of security threats and raise the need to change user's behavior.

PCI-DSS Implementation

Professional Service to implement PCI DSS or assess against PCIDSS which is mandatory for any entity storing or processing Card holder data.

End to End Data Protection with Backup & DR & Migration Solutions & Services

Connectis provides protection for your network servers, device endpoints and data recovery solutions for unplanned disasters and data and server migration solutions for the Enterprise. Solutions include both on-premise servers and server farms with VMs spread over multiple cloud locations, disaster recovery solutions for on-premise and cloud as well as Microsoft 365 backup solutions.

Enterprise Antivirus Antispam

We provide threat management and defense for endpoints and enterprise servers, web apps, workstations, mobile and Industrial Cyber Security for IoT devices. Volume license agreements are available upon request.

connectis.ca

Connectis Group
600 Bowes Road, Unit 32
Concord, ON, Canada L4K 4A3
905.695.2200 / 888.707.8221
info@Connectis.ca

About Connectis Group
Connectis is the security services & solutions company that helps customers protect and manage their IT infrastructure investments, reduce the burden to prepare for, prevent and respond to cyber attacks. We provide cyber security assessments, cyber security training, backup and disaster recovery solutions, antivirus protection, application cloud enablement services and solutions for networks.

connectis