

How IFCG Protects Their Data With Managed Security

Independent Financial Concept Group protects client confidential information and gains competitive advantage with NPC secure managed computers

Key Takeaways

- IFCG required a comprehensive secure managed endpoint solution to meet their data protection requirements
- Performance and transparency of the solution was critical
- Affordability and cost predictability were essential
- The solution needed to be equally available to its independent agent network

The Situation

The insurance and financial services industry faces daunting challenges in the face of increasing privacy regulations and the resulting need to protect client data. Its model of acting as the “manufacturer” and relying on managing general agencies (MGAs) to be the distribution arm for its services means that, although insurance and financial services companies hold a lot of confidential information about their clients that has to be safeguarded, they don’t directly control the agents and advisors who supply that information. Those agents and advisors are usually not employees of an MGA, but independents who are in turn the MGA’s clients. For those concerned about privacy and data security in that highly regulated industry, it’s a challenging environment. Also, says president of Independent Financial Concepts Group (IFCG), Gary Mandel, when it comes to security and compliance best practices, “Advisors think they’re doing the right thing, but they’re often not. They may do backups, but are backing up corrupt data. They don’t realize that when they have downtime or lose their device, it’s their business at stake.”

IFCG is an MGA that works with independent insurance sales contractors. Those independents provide their own computers and office software, and IFCG provides a sophisticated back office system, training, administrative support, and connections to the eleven major insurance companies it represents.

Private Data, Big Problems

Whether an MGA is large or small, the issues are the same: it is still responsible for overseeing the confidentiality of the customer information entrusted to it. That means keeping all of its computers up to scratch, secure, and with properly protected data, as well as advising its independent advisors on their mutual need for data security.

Independent Financial Concepts Group

Offices	Toronto, Ontario; Concord, Ontario
Founded	April 1999
Business	Financial services – Managing General Agency (MGA)
Agents	Employee agents and independent advisors
Represents	Blue Cross, Bank of Montreal, Canada Life, Empire Life, Equitable Life, Industrial Alliance, Manulife Financial, RBC Insurance, Standard Life, Sun Life Financial and Transamerica Life

A lost or stolen machine could lead to compromised data and the resultant administrative nightmare dealing with privacy issues, as well as the expense of replacing the system and rebuilding the data. Along with those hard costs comes the risk of losing customers, and according to Mandel, it doesn't matter whether the lost data is on a staffer's computer or an independent advisor's stolen laptop, because the insurance companies have effectively outsourced compliance to their MGAs.

Computer Reliability a Factor

To add to the complexity, there is the issue of malfunctioning machines. A computer that isn't working properly, whether because of a hardware or software malfunction, not only affects productivity, it could put customer data at risk of compromise. If the data on the malfunctioning system hasn't been properly backed up, it could also cause loss of business. However Mandel says that many in the industry are not aware of the availability of new technologies and services that can manage the problem for them.

A Secure Solution

To mitigate its own internal risks, and set an example for its independent agents, IFCG needed someone to provide configured, secured and supported laptops and desktops, which could be an expensive proposition. So the solution needed to be affordable and on an inclusive monthly fee basis, in order to be predictable. In addition, says Mandel, it required someone who could talk directly to its staff, without either side needing an interpreter, to deliver the best, most expedient service.

After considerable frustration with an outsourced thin-client provider that had outages and support reliability issues, IFCG decided it had to make a change. Its search led it to a solution from No Panic Computing (NPC).

NPC offers security hardened laptops, desktops and tablets, which are monitored and managed with 24/7 support, to its customers all for a single monthly fee. The machines boast biometric access, encrypted hard drives, sophisticated anti-virus monitoring, and optimized operating systems to ensure that they run well and protect the user's data. They are continually monitored; customers receive calls from NPC support if their computers are unexpectedly accessed in an unusual way, to verify that they are indeed the authorized individuals using them. If they are not, the machines are remotely locked and can be wiped to protect the precious customer data.

Backups are performed automatically every day, and data is stored in secure datacentres run by Autonomy, a world leader in secure, compliant data storage. To ensure that the datacentre itself isn't a weak point, the data is replicated securely across two geographically separated datacentres in Canada.

If a machine ever does misbehave, NPC's support organization connects to it remotely for troubleshooting and remediation. Should a machine be lost, stolen, or totally disabled, NPC ships a fresh computer, complete with data restored from the latest backup, within 48 hours. The company also includes secure decommissioning services for every unit, so data can't be compromised after a machine is retired.

The NPC Advantage

▶ Security

NPC achieves security-in-depth for endpoint devices, laptops, desktops and tablets, via a multi-layered approach to data defense. All security measures such as biometrics, strong encryption, and automated remote backup work as a unified system- monitored and managed at the NPC security operations center via console.

▶ Managed Service

Integrated endpoint managed services drive improved efficiencies, increased performance, and the benefits of specialized infrastructure without the burden of a large financial investment. It is a turnkey solution for corporate offices or independent advisors requiring either a single unit or large multi-endpoint deployments, on a monthly service fee.

▶ Performance

One of the most striking elements of an NPC secure managed computer is its performance. From short boot time, quick access to password protected web sites, immediate file search results and rapid program load, an NPC provides significant productivity enhancement.

▶ Low Cost

Managed by a dedicated team of Canadian security and computer professionals, and utilizing the cost-saving power of cloud-services in a data compliant model, NPC's consolidated service delivery mechanism achieves a level of performance and cost savings that is hard to beat, for organizations of any size.

Customers can opt for a 4G wireless connection if they need continuous connectivity. For Mandel and his staff, and the independent advisors, all of whom are frequently on the go, this keeps them in touch at all times and able to process business wherever they are without the nuisance and security exposure of public or customer WiFi.

Finally, employing NPC as a managed security services provider for a complete endpoint solution means they don't need to keep IT staff on call 24 hours a day. That service is provided with the solution.

For those who don't wish to replace existing computers at the moment, NPC offers Data-Guard; a service that encrypts files, and supplies anti-malware software and automatic backup as well as the monitoring and data protection features similar to that supplied with their leased machines.

Mandel strongly recommends NPC to his independents, and many have taken the advice, hoping to eventually get his entire independent channel secure, pointing out that the investment is small compared to the \$100,000-\$150,000 compliance cleanup cost of the mess caused by a lost, stolen or virus compromised system. IFCG can point to the specific action it is taking to secure the confidential client data shared with its agents.

"Security-wise, I don't think anyone can do what NPC does," he says. "We're getting performance, endpoint compliance and peace-of-mind for a predictable monthly fee, well beyond the level of technology we could have done or specified on our own."

"Security-wise, I don't think anyone can do what NPC does"

- Gary Mandel, President, IFCG

About NPC

No Panic Computing offers secure, professionally managed computers featuring a suite of backup, wireless, security and customer support services, controlled and supported by a sophisticated cloud-services strategy, all for one low monthly payment.

Every NPC features biometric access with professionally managed encryption and is automatically backed up each day. All systems are constantly monitored for security and backup compliance, malware attacks, physical unauthorized intrusion attempts and system performance. Lost, stolen or defective systems are replaced within 48 hours, with data and applications restored.

NPC provides specialized expertise without the burden of hiring and maintaining in-house specialists, the benefits of infrastructure without a large financial investment, and keeps pace with rapidly changing privacy and compliance demands, security threats and industry trends to provide certainty and control of confidential information.

For more information, visit www.nopaniccomputing.com, email nopanic@npcmail.net or call 1855 NO PANIC.