Tech Data 2011 Application and Data Security Sales Playbook:

How to build security offerings into your practice

Author: Mark S.A. Smith, OCE, Inc.
Editor: Kimberly Stagg, Tech Data Corporation
Subject Matter Expert: Matthew Dreger, Tech Data Corporation
OCE Project Manager: Debbie Albayati, OCE, Inc.
Project Manager: Effie Hayward, Tech Data Corporation

Printed in the USA
V1.0

Disclaimer
Neither the author nor the publisher assumes any responsibility for errors, inaccuracies, or omissions. Any slights of people or organizations are unintentional.

This publication is not intended for use as a source of security, technical, legal, accounting, financial, or other professional advice. If advice concerning these matters is needed, seek the services of a qualified professional as this information is not a substitute for professional counsel. Neither the author nor the publisher accepts any responsibility or liability for your use of the ideas presented herein.

Some suggestions made in this document concerning business practices may have inadvertently introduced practices deemed unlawful in certain states, municipalities, or countries. You should be aware of the various laws governing your business practices in your particular industry and in your location.

Any websites referenced were personally reviewed by the author; there are no guarantees to their safety. Practice safe Internet surfing with current antivirus software and a browser with active security settings.

Tech Data 2011
Application and Data Security Sales Playbook:
How to build security offerings into your practice

Welcome to the Tech Data Application and Data Security Sales Toolkit. We think that you'll find this guide valuable when you want to expand your security practice to reach more customers and become more tightly integrated in their operation.

You'll find this guide offers lots to think about with specific recommendations and ideas that you can use to boost your practice and your profits.

How to Use this Toolkit

If you are new to security sales, you'll find this toolkit to be a great way to launch your practice. You will get plenty of tips, checklists, things to consider, and success ideas that you can use to expand your practice into security services.

If you're an old hand at selling security services to your customers, you may find this tool to be a good checkup. Just like you go to a doctor to make sure you're healthy, you might use the ideas in this guide to make sure that you're getting all the profits that you can. You'll probably discover one or two ideas that you haven't thought of before and implementing those may make a big difference in your practice.

While we can't cover every aspect of the security business in this toolkit, you have lots of resources at Tech Data that you can tap into to get more answers. Contact your Tech Data sales rep with any questions that you have. We're here to help you make a difference.

A great way to get started with this toolkit is to quickly skim through the guide to get an idea of what's in here. Stop and read what grabs your attention. You're much more likely to get what you need out of this guide if you pick and choose versus reading it from front to back. Use your best judgment on how to make the right adjustments for your business and make these ideas work best for you.

What is Application and Data Security?

In this Tech Data Application and Data Security Sales Toolkit, we will discuss how to implement fundamental security measures such as email and web-based threat protection. Ask your Tech Data rep for other Security Sales Toolkits that cover other aspects of security.

For most companies, their greatest assets after customer loyalty, are digital.

It's About Protecting the Customer's Data

If your clients store information about their customers that can be used by third parties to steal, defraud, or impersonate those customers, then your client is a target. Perpetrators want to pilfer proprietary property, cheat customers, hinder employees, and attack the heart of your client's business—their information systems and vital customer assets.

Electronic intellectual property is more than 70 percent of the market value of a typical U.S. company according to PriceWaterhouseCoopers.

Application and data security is about protecting those assets. The good news is that security technology is more affordable and more reliable than ever. The bad news is that the bad guys are more clever and vicious than ever.

The usual attack vector is with malware (such as viruses, Trojans, worms), email payloads (scams, phishing, spam), or weak protection from unauthorized access.

Most Application and Data security offerings are delivered by a software solution, hardware appliance, or cloud-based service or a combination of these items. Let's look at each of these.

Software Protection

- Battles threats within the firewall, inside the network or when off premises
- Works well with smaller organizations
- Small scale solution, often free with PC purchase
- Spam and malware detection not as effective
- Focused on consumers, not business
- End user must often perform or allow updates to stay protected
- Ongoing annual maintenance costs

Appliance Protection

- Hardware bought and installed on site, usually limited or no protection off premises
- Works well with larger organizations
- Scaling requires more hardware, can create performance limitations
- May require constant, daily attention from IT resources
- May not be able to keep up with rapidly changing threats
- Capital expense
- Ongoing annual maintenance costs
- Single point of failure

Managed Services Protection

- Works well with any size organization
- No hardware or software to buy, price charged by user or usage
- Keeps malware and email threats outside network
- Works either on or off premises
- Scalable
- An operating expense instead of capital expense
- No upgrades or maintenance
- On-demand capacity
- Reduces bandwidth, storage costs
- IT staff is free to do other duties
- May not be trusted by IT staff
- Monitored 24 x 7

Your Clients are Responsible

Virtually every company that has been attacked had staff who knew they were vulnerable, but hadn't done anything about it. After the fact, they found out that they were responsible. Could your client be in this position?

The responsibility for ensuring security in your company lies with your client and their leadership team. The responsibility of putting security into practice lies with each member of your client's company. You can help.

How this Landscape is Changing

In the past, an antivirus program might have been enough to do the trick. That's no longer true.

In 2010, 95,000 unique pieces of malware in total appeared, doubling the volume of malware seen in 2009.[1] New malware appears, on average, once every 0.9 seconds. You client can't keep up with all of the changes without your help.

The courts of law have almost always made businesses responsible for the security of their customers and associated data. Legislators mandate corporate responsibility, and with it, more pernicious penalties for the executives involved. The bar is being set higher as to what constitutes reasonable care in providing security for customers, employees, and their data. If there's a security breach in your client's company, they can count on being asked tough questions by stakeholders and the law.

[1] http://www.sophos.com/en-us/security-news-trends/security-trends/security-threat-report-2011.aspx

What this means is that how we approach delivering security to our clients changes as the nature of the attacks change. Even a savvy IT administrator can't keep up with all of the threats, security strategies, and mitigation methodologies along with all the other things they need to know about traditional IT infrastructure.

Your clients need you!

Why a Security Practice is Valuable for You

Application and data security is usually the first step that business partners take to enter the lucrative business of selling security services to their clients. Most vendors make it easy to get the market by providing simple-to-install security applications or software-as-a-service tools that don't require technical expertise to deploy and maintain.

You get started by selling just a few seats to your clients and expand as you grow comfortable with the technology. Usually not much training is required and you don't need to have anybody with security certifications on your staff to be effective.

Business Requirements to Successfully Sell Application and Data Security

The good news is it won't take much to begin selling security services and your practice. It's more a matter of asking the right questions when you speak with your client's and then having new things to talk about when you identify opportunities.

- If you're selling software applications now, then it will be easy to deliver security software applications.
- If you're selling hardware now, it will be easy to sell security appliances.
- If you're providing infrastructure assessments now, it will be easy to add security assessments to your offering.
- If you're offering cloud-based services now, it will be easy to add software-as-a-service to your line card.

Many business partners find that as they move into security, the business grows organically as they add more services and products based on discovering what their clients really need.

In fact, you can start out just by asking the questions that follow in this sales guide and then decide what to offer once you've identified an opportunity.

The Application and Data Security Market Opportunity

Most of your clients have some type of security solution, even if it's just the free antivirus package that came with their computer. The problem is that while it's a good start, it's not enough.

Business Drivers

Industry analyst, Gartner estimates that 70 percent of corporate break-ins are motivated by money or political reasons. The other 30 percent are random attacks to grab whatever unsecured assets are available and cash in on your client's hard work.

The attacks come from everywhere: checking email, going to a website, interacting on Facebook or Twitter. It can even come become through a brand-new computer just purchased. A recent study by the Internet Storm Center claimed that an unpatched, unprotected Windows® PC on the Internet will be compromised in less than 6 minutes. [2]

Some shocking facts about digital attacks:

- **The probability of an attack from a random web page is about 1 in 3,000.** [3]
- **Between 80 and 90 percent of all email is spam.** [4]
- **Corporate data breach average cost hits $7.2 million.** [5]

Negligence remains the main cause of the data breach in 41 percent of attacks. The problem is that there is no legal defense against an intrusion caused by negligence. You can easily use this statistic as a door opener to conduct a security assessment for your clients.

Malicious or criminal attacks account for 31 percent of data loss in 2010. This is what most customers think that they're covered against, yet as you've just learned, this is only a third of the potential risk.
System failures accounts for the rest of the data loss. And of course you can help by providing the right hardware, storage, and software systems.

Technology Drivers

A major technology driver for updating security approaches is mobile computing. Your clients and their employees want anytime anywhere access to the corporate database. Their customers expect to transact business 24 x 7 securely, and reliably.

Yet mobile computing brings its own challenges with unsecured or insecure Wi-Fi access points, a wide variety of access devices (such as Windows devices, Android devices, Apple OS devices, and many more), and operating systems that are unpatched and outdated.

Future Trends

The bad guys trying to get to your clients data are way more sophisticated than most of your clients. And as compute power gets faster and bandwidth gets cheaper it's only going to get worse for those who are unprepared.

- Using social media opens up additional security holes. While many companies block Facebook and Twitter, users can still get around these by using anonymizer websites.
- New, online applications are being created all the time that will pose security risks to organizations.
- As bandwidth demands increase, the security scanning strategies must keep pace with the data throughput.
- More organizations will have a mix of operating systems that will need to be protected and patched, complicating the security task for IT administration.

[2] When installing a new Windows PC that is connected to the Internet without firewall protection, infection is probable because the time to download critical patches exceeds the unprotected survival time. isc.sans.org

[3] http://security.cbronline.com/news/one-in-3000-websites-harbouring-malware-kaspersky-240211

[4] For the current spam levels, virus attacks, and phishing attempts, see http://www.messagelabs.com/globalthreats

[5] http://www.networkworld.com/news/2011/030811-ponemon-data-breach.html

How to Identify Likely Prospects for Application and Data Security

When looking for security services opportunities, you can begin your reconnaissance by asking everybody you speak with, “What is your biggest concern about data security?”

The reason why this question works so well is because almost everybody has a difficult time keeping up with security issues. What you learn from these questions gives you an insight into where to probe further in your client’s organization.

Who to Talk With: Getting to the Decision-Making Team

You may already have access to the decision-making team now. Or you may need to find some new contacts if you want to sell them security solutions. The first step is to identify who is impacted when there is a breach of data security. It doesn’t make sense to talk to anyone else to begin with.

The responsible party could have a title such as security officer, legal officer, IT administrator, compliance officer, or similar title. It could also be the chief financial officer.

In any case, you can most efficiently find the security decision-maker by asking your contact the question, “Who is responsible for data security including email and web access?”

If the person you’re speaking with isn’t responsible, they will gladly point you in the right direction. Hey, they don’t want to be responsible.

How to Get the Meeting

Ask your contact to introduce you to the responsible party. If that’s not possible, or you don’t have a contact in your target customer, you’ll have to create your own introduction. (See sales tools on page 8.)

Sales Tools

Suggested Introduction Email:

New Security Threats

Appleseed, John <John.Appleseed@techdata.com>
To: Myia Client <m_client@aol.com

According to a recent security report, new malware hits the network at the rate of more than one a second. This means the average technology user can't hope to keep up with the onslaught from the bad guys.

If this concerns you, let's talk. If not, would you let me know who should be concerned?

I am (your name) with (your company). Our clients tell us they choose to work with us because they can let us worry about these issues so that they can go about what's important in their business.

Please let me share with you some the things we've done for our clients and identify if we can help you in a similar way.

Just drop me an email to schedule a time to speak or call my cell phone at (your phone number).

P.S. You might find this information helpful. (Web address for additional information about your security services.)

Suggested Voicemail Script:

I'm (your name) with (your company). I've been working with technology for a long time and yet I've never seen anything like the number security threats hitting the network. There is a new virus being released every second. This means the average technology user can't hope to keep up with the bad guys.
The purpose of my call is to share with you some ideas that I've found to solve this problem. Our clients tell us they choose to work with us because they can let us worry about these issues so that they can go about what's important in their business.
Please let me share with you some the things we've done for our clients and identify if we can help you in a similar way.
Just drop me an email at (your email address) to schedule a time to speak or call my cell phone at (your phone number).
I'm looking forward to sharing what I've learned, (their name).

What to Say: Aligning with Their Motivation

Once you can have a conversation with them, confirm they are indeed responsible for data security and then asked them, "How do you plan and budget for data security?" This will give you some insight in to how they approach their job. If they aren't responsible for planning and budgeting, they are the wrong person to speak with. Find out who is and get to them.

Follow-up with the question, "How would you like that to change?" What they want to change is what they're willing to buy. Now it's just a matter of matching what you have offer with what they'd like to do differently.

Managing Common Objections

No doubt you'll run across some objections when you talk with your customers about security solutions. Here are some most common ones that show up in some suggestions on how to manage them.

The most likely objection that you'll hear is, "Our systems are already secure."

Your response to this should be, "I'm sure they are! Yet when was the last time your system was reviewed and tested? We'll be glad to do this for you and if we find anything, it'll save you the cost and embarrassment of an attack. If we don't find anything, you can say that you're just being cautious."

Another common objection is, "We don't have the money."

I'm sure you hear this all the time. Next time you do, try this: "I hear that all the time. Yet how much have you budgeted for when your security system doesn't work and you have to clean up from an attack? Your company probably retains lawyers and hires locksmiths to keep it safe. Yet your most valuable asset is your data. Let's take a look to see what it would cost to protect your data the way you protect the rest to your company."

Yet another common objection is, "We're going to be looking at that in the future."

Try this response: "That's a great idea! How do you plan to protect your data between now and then? Let me at least put together an interim plan to keep you protected until you can put together a full solution."

Exploring the Application and Data Security Opportunity

You can identify opportunities for your security practice by asking smart questions and intelligently identifying what security topics to discuss with your clients.

Qualifying Questions for Application and Data Security

These questions let you examine your client's current security situation to determine if expanding their security makes sense.

- If your data system was disabled, either from an intentional attack or an accident, how confident are you that you could quickly restore critical business systems before there was substantial impact?
- How long do you have after an occurrence before your customers would begin looking for other vendors?
- What records are you required by law to maintain?
- How are you assuring that these records are secure?
- What is the potential legal exposure if your organization cannot fulfill contractual obligations?
- What would happen if your company's financial records were destroyed?
- What would that cost?
- What incidents have you planned for?
- When was the plan last reviewed?

Triage Questions: Deciding What to Discuss for Greatest Impact

When it comes to security, there are so many things to talk about that you may be uncertain where to begin. Use this simple guide to identify where to start the conversation with your client.

What is your data security policy?

If they don't have a security policy, it's going to be very difficult to identify the holes in their security beyond the basics. Your first step will be to help them develop a policy that can then be enforced. Many of your small clients need help developing a security policy. In the process, you'll identify may ways that you can help your client become secure.

When was the last time your security policy was reviewed?

Even if the organization has a security policy, the odds are good that it hasn't been reviewed or tested since it was created. The next step is to examine the policy to identify where it needs to be revised and where there are implementation holes. The powerful thing about this approach is that management has already agreed to the policy, now it's just time to fund the implementation. You don't have to sell them anything; they just get to buy with a board agreed to.

What is your biggest concern around data security?

Where your client has a concern, they know that there is a weakness in their security strategy. You can help them explore the costs of securing this weakness and identify the value of managing the issue.

What is your roadmap for securing your data?

If your client has an idea of where they want to go, your job is going to be easy. If they don't have a roadmap, you can consult with them on their security goals—based on corporate and legal mandates—and help them figure out how to get there.

Aligning with Your Client's Motivation

When you work with your client, there will most likely be multiple people involved in the decision-making process. You'll need to satisfy the concerns of the executives, the IT department, the legal department, and your client's customers. Each of these people has their own view of what's important in the decision-making process.

For example, the IT administrator will focus on making sure the security solution is going to be effective and have limited impact on the rest of the IT operation. They will also want to know how you plan on delivering the security solution. The legal department needs to make sure that they are covered in case of a breach so that they have legal defense if they're brought to court. The executives want to make sure that they can maintain and grow operations with minimal risk. The customers want to make sure that their proprietary data stays private.

This means that in the discussion of your proposed solution, you need to cover each of these motivating factors of the decision-making team. Now that you understand some of the issues and motivating drivers for your client, you can position your security offerings in a way that is compelling.

Communicating Powerful Value Propositions

If your key contacts are in the IT department and they ask you for proposal, it means that they are interested in what you have to offer but need to communicate the value of your solution to the rest of the decision-making team. Your proposal must include all of the value propositions and information that the decision-making team requires to say yes.

When creating your proposal, focus primarily on outcome instead of methodology. The reality is that in security, the methodology will change because the nature of the threats change. Instead, focus on how you will actively help your client protect their data and mitigate any issues that might arise.

If the IT administrator needs additional information about the methodology, include that as an appendix consisting of data sheets and white papers provided by the vendors you've selected.

Illustrating Compelling Value of Application and Data Security

When you choose a vendor (with the help from your Tech Data sales rep) for deploying application and data security solutions, you'll frequently get access to tools that will help develop strong value propositions to share with your clients.

Couple this with the research that you've done by asking the questions discussed above and you'll be able to present a compelling reason for your clients to take action now.

You can calculate what a data breach costs for your clients with the Ponemon Institute/Symantec Data Breach Risk Calculator.[6] You can also get current comparisons with others in the industry to benchmark data risk costs from this resource.

Closing the Deal

Using your chosen solution's TCO or ROI calculator you can calculate the value of the security solution you're proposing. If you're calculating TCO, divide the resulting number by 36 if it's a three-year figure, or by 60 if it's a five-year estimate. This gives you the monthly savings for the solution. Use this number to illustrate the value of making a decision sooner instead of later.

For example, if the security solution you're recommending saves them $30,000 a month, every month they delay the decision means they write an unnecessary check for $30,000.

Align with their internal deadlines. If the CEO has promised the Board of Directors that a security solution will be implemented in the next six months, use this information to your vantage. When you can link your proposal to their internal deadlines, you will speed the deal.

Expanding the Application and Data Security Opportunity

The process of delivering security services is similar to delivering any other technology. Break up the task into manageable chunks and just get started on the most important pieces.

Begin by reviewing what level of security you need. Then identify the barriers to making that happen. Next, assemble your team to craft strategic approaches to eliminating the barriers and evaluate potential solutions. Create smart questions that uncover the necessary information so that you can make intelligent choices, balancing risk and reward.

Services

Here are some of the services you can offer to your clients. Pick and choose those that you feel will enhance your business.

Creating, Reviewing, and Auditing Security Policy

Security strategy is based on policy, education, technology, measurement, and enforcement. You can deliver services in each of these areas.

A policy is a document that summarizes requirements and prioritizes expectations that must be met for specific areas of the company. It details what's authorized, what's unauthorized, when policies apply, and who is responsible for maintaining and enforcing the policies.

A standard is a specific technical requirement that must be met by everyone. For example, a computer must be in a specific, secure configuration before connecting to the corporate network. Following industry standards provides a level of indemnification when a contract demands reasonable care.

A guideline is a recommended best practice that becomes established through experience. Effective security policies use existing standards and guidelines. This speeds adoption because it capitalizes on the corporate culture.

[6] http://databreachcalculator.com

Start by creating a policy that defines roles and responsibilities. It's easier to write and approve a three-page document than a 200-page tome. Keep it short and focused, assigning responsibility to the right people and moving implementation details to the right level of expertise.

Classic policy details scope, reasons, definitions, domains, roles and responsibilities, management, documentation, implementation, measurement, and updates and changes.

Sample Policies

A quick Web search of "sample security policies" turns up a number of free and for fee examples.
SANS offers sample security policies developed by a group of experienced professionals; a good starting point. [7]

The IT security policy for Murdoch University in Australia is a tight document covering the key points, including permission for use by others.[8] You might use other university sites for policy examples. Just make sure that the policies are in the public domain so that you can use them.

The SAFE Blueprint from Cisco Systems is a best-practices technical discussion about business computer networks. It takes a defense-in-depth approach so the failure of one security system won't compromise the rest of the network. Although the recommendations are product agnostic, the solutions center on products from Cisco and partners.[9]

An expensive but widely regarded book, Information Security Policies Made Easy includes electronic templates and fully-developed examples.[10]

Education

Security breaches begin with, "I don't have to worry about a password; I only use the network for printing."
The biggest bang for the security buck is educating your client's people because it puts security into action. Educate all employees and vendors about security procedures and consequences of non-compliance.

Yes, this costs money, but so does insurance and the legal team. Some managers complain, "If I train them, they'll just leave." Well, what if you don't train them, and they stay?

Most education is simple, like reminding employees to not discuss sensitive procedures with outsiders. Teach them that security is a group responsibility; a chain is only as strong as its weakest link.

You can either purchase security training sessions or develop your own proprietary materials based on the needs of your client.

Measurement

It makes no sense to have a policy that's not measurable because no one knows how well they're doing or where they need to improve.

Some things are easy to measure, for example your client can survey who's wearing an ID badge and who has access to sensitive information.

Software tools can measure company-wide security policy compliance and can tell you how secure your client's premises are. (We will cover that in another Security Sales Toolkit.) Many of these tools come pre-configured with security policies based on standards and best practices, making policy easy to implement and measure.

---

[7] http://www.sans.org/security-resources/policies/
[8] http://www.murdoch.edu.au/index/policies/it
[9] http://www.cisco.com/go/safe
[10] http://www.amazon.com/Information-Security-Policies-Made-Version/dp/1881585131

Audits
Your clients need a regular, third party audit to illustrate that they are in compliance and to illustrate best effort. You can regularly audit access to confidential information to determine how vulnerable your clients are. Review what information is accessible, by whom, and where and how it is accessible.

You can purchase tools that help with the security audit process. In addition you'll find a similar security sales toolkit written specifically about security compliance and vulnerability assessment and management.

Enforcement
Few people want to play the heavy in enforcing security policy. Yet, a policy without enforcement is a set up for major trouble. You, as a third party, can help with this.

Rules and polices don't have the force of law. Your clients can't physically detain someone because they broke a corporate rule unless it's backed up by legislation. But they can be dismissed.

One of the easiest ways to enforce policy is to show your clients how to make security compliance part of the regular performance review process. A good worker who isn't safe isn't good for the company.

Devise a series of warnings with increasingly stiff sanctions. Some infractions need to carry the penalty of instant dismissal, such as committing felonies on company property. Your client may wish to create rigorous responses to seemingly minor security infractions if those lapses result in legal exposure.

If a client's employee, vendor, or customer breaks the law, call law enforcement.

Likely cross sell and up sell options
There are plenty of other items to sell your clients as you dig into their security requirements. We have created sales toolkits to help in quite a few of these areas. As your Tech Data rep for these sales kits:

- Identity & Access Management
- Secure Content and Threat Management
- Security Compliance and Vulnerability Assessment & Management
- Video Surveillance

Your clients will also potentially need additional networking, upgrade storage, and improved data center physical security.

Supporting Resources
There is certainly much more to discuss then we can cover in this sales kit. Use these resources as a good starting point to gather what you need to expand your security practice.

Industry Resources
Look at these web sites for sources of up-to-date statistics, ideas, and insights.

National Vulnerability Database
nvd.nist.gov – National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data.

The SANS (SysAdmin, Audit, Network, Security) Institute
www.sans.org/top-cyber-security-risks – SANS is a great resource for computer security training, network research, and resources.

Hoax Reference Site
Nothing kills your credibility faster than sharing bad data. http://snopes.com is the first stop for a quick check to see if an email warning or story is a hoax.

The Security-Specific Search Engine
SearchSecurity.com – Offers a variety of newsletters or Web casts dedicated to security. The site offers security-specific daily news, thousands of links, and interaction with leading industry experts.

Security and Privacy Research Center
www.cio.com – From creating and implementing a security policy to dealing with rogue programmers, the CIO Security and Privacy Research Center can help with ideas to keep a network and site secure.

Computerworld Knowledge Center
www.computerworld.com/securitytopics/security – Leading with the latest security headlines, Computerworld's site includes upcoming events, links to vendors, security statistics and reviews, as well as online discussions.

Electronic Privacy Information Center
www.epic.org – This site from the Electronic Privacy Information Center (EPIC), a public interest research center, covers the gamut of online privacy issues.

Computer Security Institute
www.gocsi.com – Publishes the annual FBI/CSI computer crime and security survey. Educates computer and network security professionals about protecting information assets.

The CERT Coordination Center
www.cert.org – Web site for the CERT Coordination Center at Carnegie Mellon University, a major reporting center for Internet and network security vulnerabilities.

Information Systems Security Association
www.issa.org – A non-profit association for information security professionals that facilitates interaction and education to promote secure information systems management practices.

Center for Internet Security
www.cisecurity.org – CIS members identify security threats of greatest concern and develop practical methods to reduce the threats. Provides methods and tools to improve, measure, monitor, and compare the security status of your Internet-connected systems and appliances. CIS is not tied to any specific product or service.

NIST's Computer Security Resource Center
csrc.nist.gov – Resources from the National Institute of Standards and Technology's Computer Security Division.

Assessment Tools

Most security vendors include a vulnerability assessment tool as part of their suite of products or as a sales tool. Ask them about what they have available for you to complement any tools you already have.

Tech Data Resources

Tech Data Security Solutions Hub

http://www.techdata.com/techsolutions/security/

Tech Data's Security Solutions cover endpoint to endpoint and all points in between. We've closed the loop on security technologies and provide you with the tools and services you need to make your security business the most profitable.

TDCloud

http://www.techdata.com/content/tdcloud/default.aspx

TDCloud is a set of products, services and enablement tools available from Tech Data that help VAR customers find, develop and close Cloud opportunities.

TDAgency

www.techdata.com/tdagency

TDAgency is Tech Data's full-service advertising and marketing agency and we have something other agencies don't have—IT industry experience and expertise. Why waste time explaining your solutions to someone who doesn't live and breathe IT? We can hit the ground running and work with you to develop a targeted strategy and customized marketing plan for resellers of all sizes and budgets.

MyLicense Tracker

http://www.techdata.com/tools/licensing/LicenseResendSearch.aspx

This automated search enables you to search for and forward license e-mails for select vendors.

Software License Selector Powered by StreamOne [SM]

http://www.techdata.com/TDSKUSelector.aspx

Tech Data's Software License Selector powered by StreamOne[SM] significantly surpasses contemporary software licensing tools in breadth and ease-of-use. It supports 40 major software vendors, representing more than 99 percent of the software licenses sold through Tech Data. It eliminates the need for you to spend valuable time researching each vendor's unique and often complex software licensing programs, because Tech Data has done all the work for you.