



Preventing Cyber Crime & Business Identity Theft

Aaron Hanson

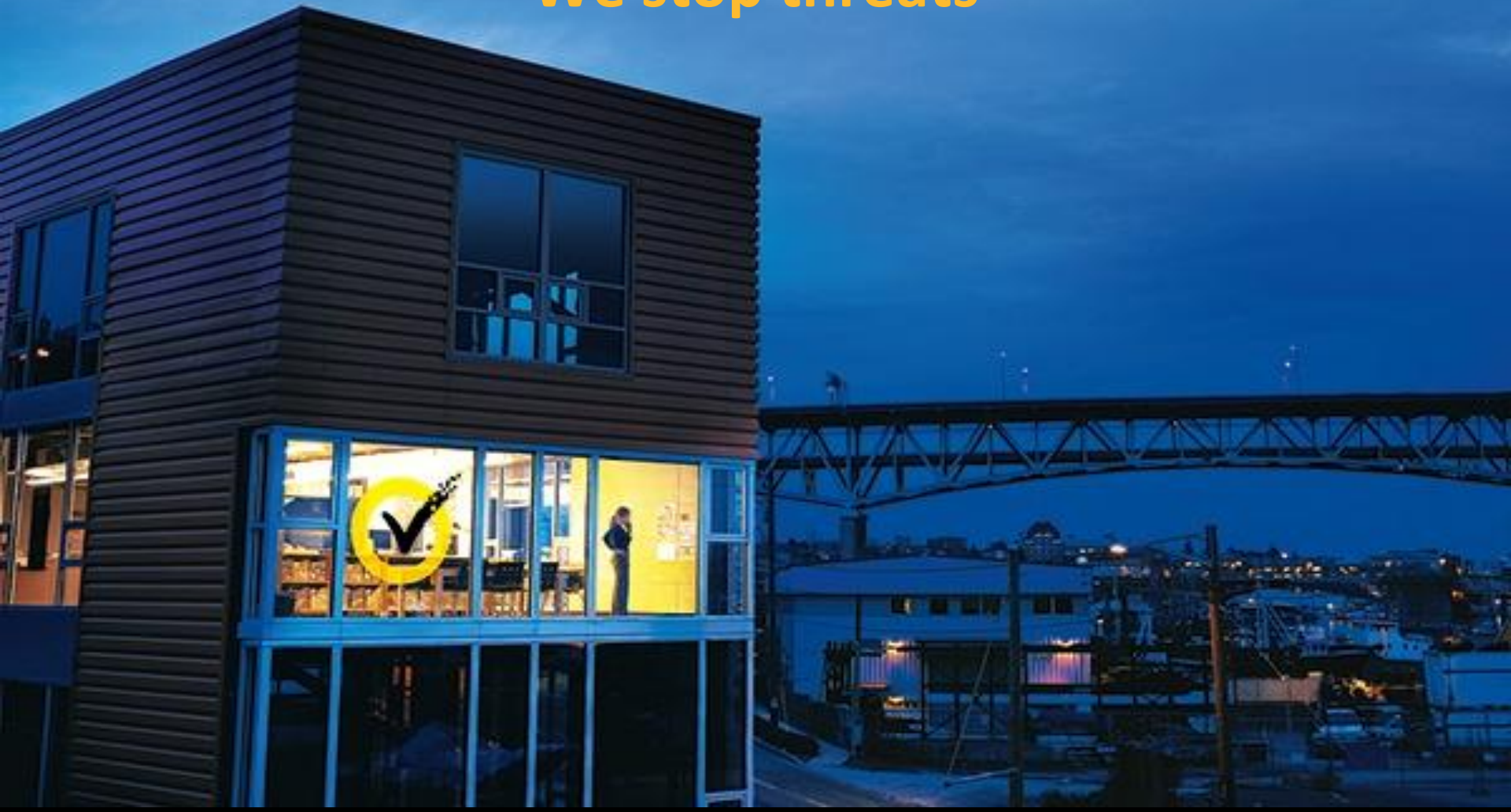
Senior Manager, Regional Product Marketing, SMB & .cloud



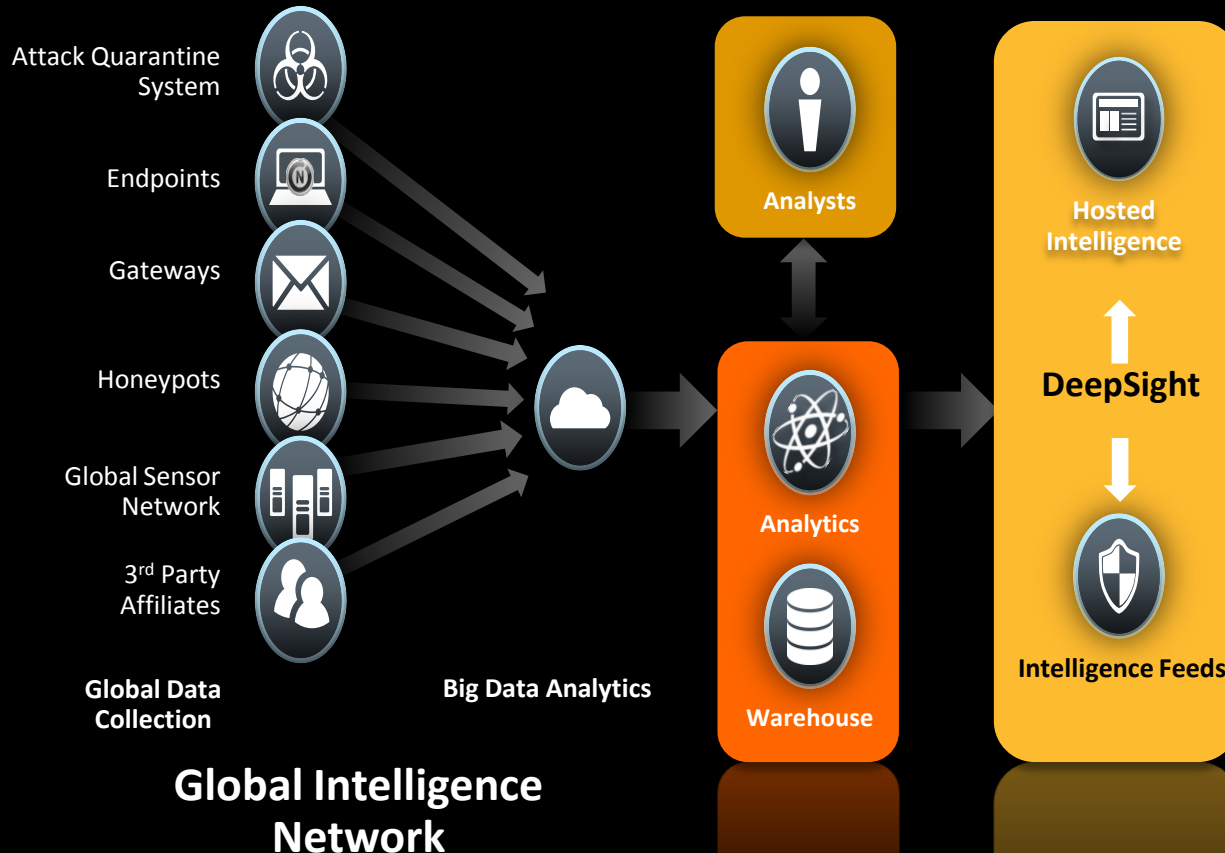
Symantec Mission

**We protect the world's people
and information.**

Threats stop business
We stop threats



Powered by Security Intelligence



Probes in **200**
countries & territories

Visibility into **30%** of
global email traffic

Over **2 million**
decoy accounts

Today's Threat Landscape

INTERNET
SECURITY
THREAT
REPORT

2011 Trends
Volume 17
Published April 2012



 Symantec.

5.5 billion

attacks blocked by Symantec in 2011 (3 billion in 2010)

4,989 new vulnerabilities

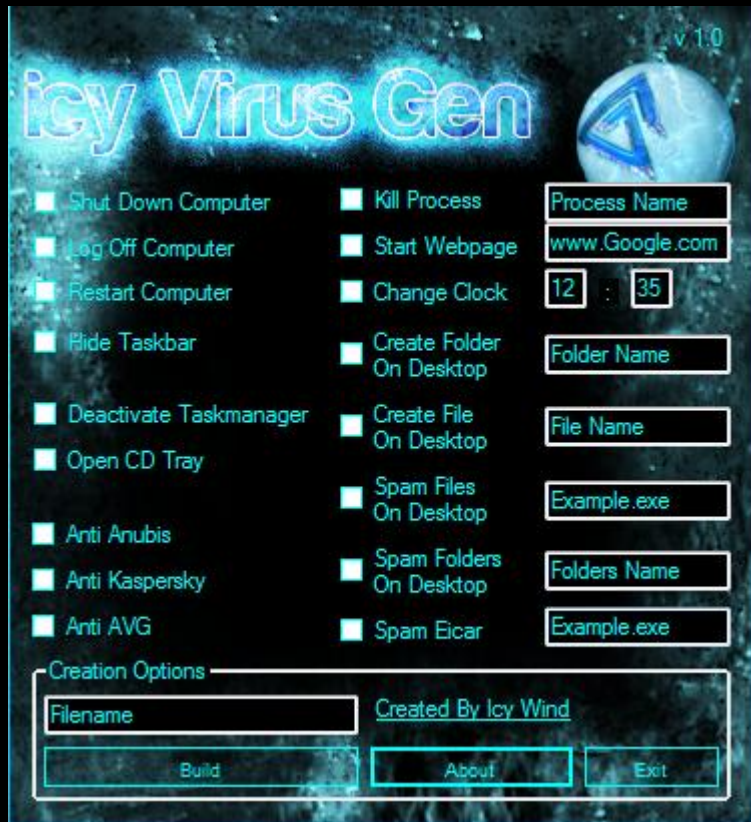
1.1 million identity exposed per breach

4,595 Web attacks per day blocked

403,000,000 unique malware variants vs. 286,000,000 in 2010

<http://www.symantec.com/threatreport/> for more details.

A Whole Industry Exists To Help Malware Authors Evade Detection



Bare Minimum Security **No Longer an Option** for SMBs

- Small businesses are increasingly being targeted
 - Targeted attacks against SMBs **doubled** between 2011 and 2012.*
 - Direct correlation between a **rise in attacks against small companies** and a drop in attacks against larger ones.



*Source: Symantec Intelligence Report, June 2012

SMBs Are **Weakest Link** in Supply Chain

- **Hackers use SMBs** as stepping stone into larger companies
 - 28 percent to 41 percent of data breaches caused by a third-party¹
- Top 500 global businesses average 60 alliances each with smaller companies²
- Becoming the gateway to a major client's or partner's data can **destroy an SMB**
 - Contracts now demanding partners have top-level security

¹ Source: Ponemon 2011 Global Cost of a Data Breach

² Source: [House Small Business Committee](#)



No Cybersecurity Plans...No Worries

Nearly **3/4** of SMBs

- Indicate a safe Internet is important to success
- Say strong cybersecurity is good for their brand

However – over **6 out of 10** SMBs

- Say they are not concerned about cyber threats
- Don't even have an informal internet security policy



AND the majority of SMBs surveyed (59%)

- **Do not have a contingency plan to respond to a breach**

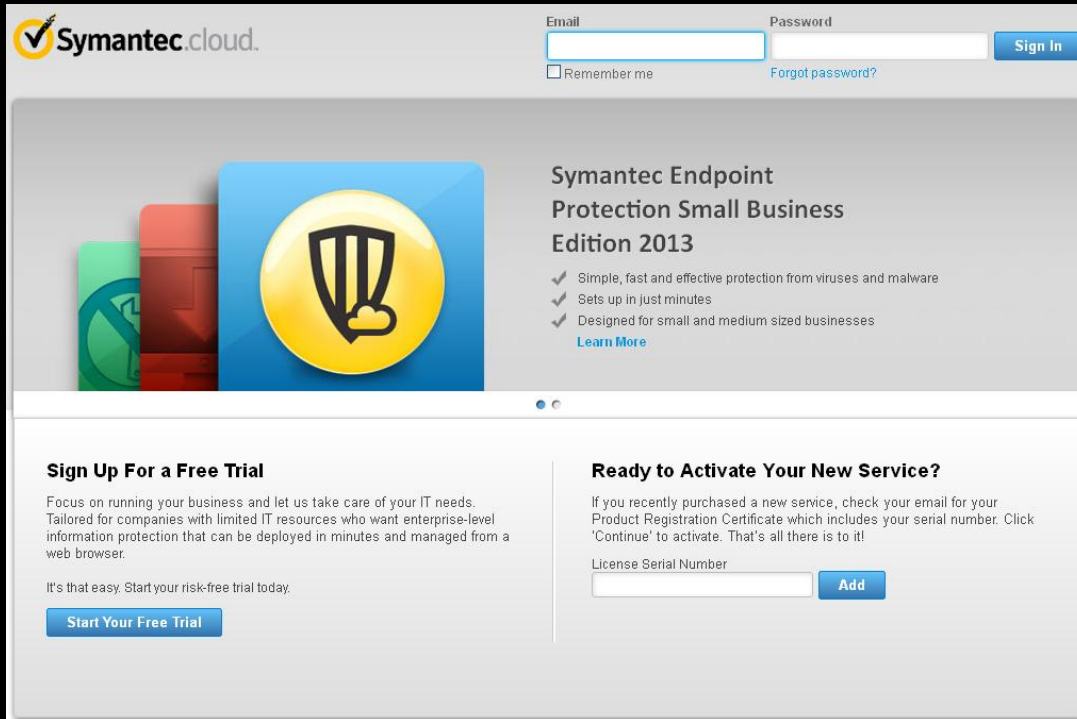
Source: National Cyber Security Alliance & Symantec 2012 National Small Business Survey, October 2012

Small Businesses Need:

**Simple, Affordable, Automatic Protection
That is Easy to Manage**



Symantec Cloud Solutions Make Protection Simple



The screenshot shows the Symantec Cloud Solutions website. At the top left is the Symantec Cloud logo. To the right are input fields for Email and Password, a 'Sign In' button, a 'Remember me' checkbox, and a 'Forgot password?' link. Below this is a large graphic with a shield icon and the text 'Symantec Endpoint Protection Small Business Edition 2013'. To the right of the graphic are three bullet points: 'Simple, fast and effective protection from viruses and malware', 'Sets up in just minutes', and 'Designed for small and medium sized businesses', with a 'Learn More' link. Below the graphic are two sections: 'Sign Up For a Free Trial' and 'Ready to Activate Your New Service?'. The 'Sign Up' section describes the service and includes a 'Start Your Free Trial' button. The 'Activate' section includes a 'License Serial Number' input field and an 'Add' button.

Symantec.cloud.

Email Password [Sign In](#)

☐ Remember me [Forgot password?](#)

Symantec Endpoint Protection Small Business Edition 2013

- ✓ Simple, fast and effective protection from viruses and malware
- ✓ Sets up in just minutes
- ✓ Designed for small and medium sized businesses

[Learn More](#)

Sign Up For a Free Trial

Focus on running your business and let us take care of your IT needs. Tailored for companies with limited IT resources who want enterprise-level information protection that can be deployed in minutes and managed from a web browser.

It's that easy. Start your risk-free trial today.

[Start Your Free Trial](#)

Ready to Activate Your New Service?

If you recently purchased a new service, check your email for your Product Registration Certificate which includes your serial number. Click 'Continue' to activate. That's all there is to it!

License Serial Number [Add](#)

- Set up in minutes with Web-based management from anywhere
- No hardware, software, or specialized training needed
- One login to manage both backup and security in one easy-to-use console

Start your free 30-day trial:

<http://go.symantec.com/trycloud>

Symantec Web-Based Console Makes Management Easy

The screenshot shows the Symantec.cloud web-based console interface. At the top, there is a navigation bar with the Symantec logo, a language dropdown set to English, and links for My Profile, Support, Feedback, Help, and Logout. Below this is a user profile section for Joe Smith (joesmith@bwd.com) at XYZ Company. The main navigation menu includes Home, Computers, Policies, Users, Alerts, Reports, Settings, and Subscriptions. The 'Computers' tab is selected, showing a welcome message for Joe Smith and the current date and time (Friday, November 09, 2012 7:53:04 PM GMT). The interface is divided into several sections: 'Backup Exec.cloud' showing a summary of 2 computers configured for backup, with details on total files (4953), protected status, last backup activity, and usage; 'Endpoint Protection' showing a summary over the last 7 days with metrics for total computers, viruses, blocked USB devices, and security risks; 'Computer' health status showing 3 computers with a green checkmark, 0 with a yellow warning, and 0 with a red error; and 'News Alerts' featuring a reminder about a Symantec Cloud Service Agent Upgrade. The interface is clean and organized, providing a centralized view of backup and security management.

Backup Exec.cloud

Summary

2 computers configured for backup

Total Files: 4953 files

Protected: 4953 files

Last Backup Activity: Friday, November 16, 2012 4:49:25 PM

Usage (Upgrade): 32% full (15.98 GB / 50 GB)

Endpoint Protection

Summary over the last 7 days

Total Computers:	2	Quarantined Items:	0
Viruses:	0	Unresolved Security Risks:	0
Blocked USB Devices:	0	IPS Blocked:	0
		Other Risks:	0

Computer

Computer Health

100%	0%	0%
3	0	0

There are no computers at risk.

News Alerts

Reminder: Symantec.cloud – Cloud Service Agent Upgrade

Dear Client,

Previously, we announced that your Symantec Endpoint Protection.cloud service would be automatically upgraded to our new Symantec Endpoint Protection Small Business Edition 2013...

Wednesday, October 10, 2012 8:53:00 AM (News)

Symantec.cloud – Cloud Service Agent Upgrade

Dear Client,

We're thrilled to announce Symantec Endpoint Protection.cloud is now Symantec Endpoint Protection Small Business Edition 2013. The new features

Manage computers, users, and policies for both backup and security

Centralized view of computers protected against viruses and malware

Centralized view of computers configured for backup

Get the critical information you need at a glance

<http://go.symantec.com/trycloud>

Simple, Fast, Effective Cloud-Managed Security

Symantec.cloud Home Settings About X

Endpoint Protection.cloud

Secure

Last Definition Update: Thursday, November 15, 2012 at 4:06:12 PM
Last System Scan: Thursday, November 15, 2012 at 1:59:46 PM
Next Scan: Idle Scan Enabled

Current Settings

Computer	Web	Network
Antivirus	Download Intelligence	Intrusion Prevention
Antispyware	Browser Protection	Email Protection
SONAR	Safe Surfing	Smart Firewall
USB Devices Blocked		

[View History](#)
[View Quarantine](#)
[Quick Scan](#)
[Manual Scan](#)
 [Override USB Device Control](#)

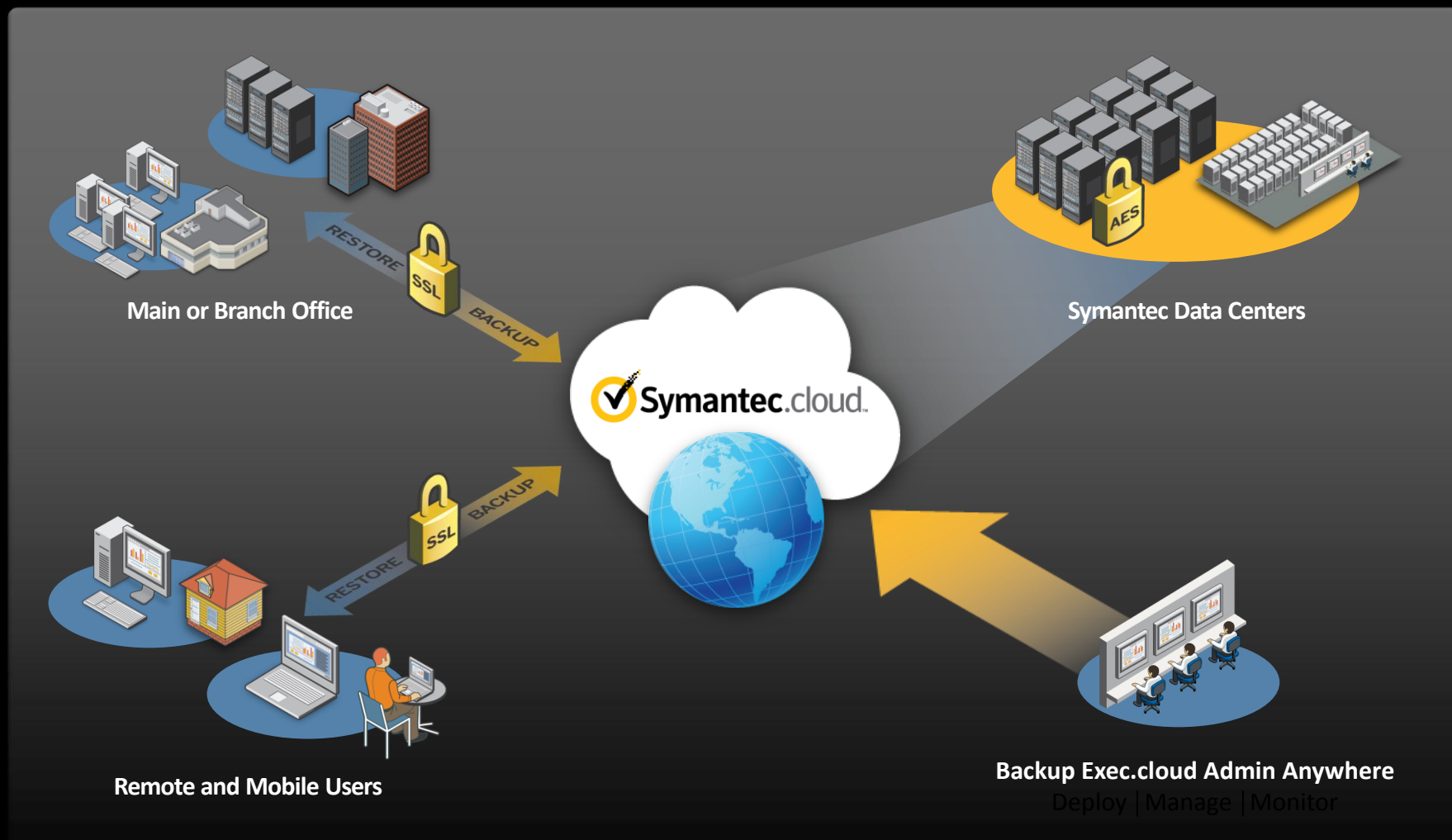
Connected to Symantec.cloud

Get the critical information you need at a glance

Simple view of settings and status

Shortcut links makes it easy to view details or perform maintenance tasks

Automated, Continuous, Secure Online Backup & Recovery



Automated, Continuous, Secure Online Backup & Recovery



The screenshot displays the Symantec Backup Exec.cloud web interface. At the top, there's a navigation bar with the Symantec.cloud logo, a 'Home' button, a 'Settings' button, an 'About' button, and a close button (X). The main content area features a large yellow circular icon with a database cylinder and a cloud. To its right, the text 'Backup Exec.cloud' is displayed, followed by a green checkmark and the word 'Protected'. Below this, it states 'Continuous backup is active' with a 'Pause' link. A summary box on the left contains the following information:

Total Data Protected:	4.6 GB (3265 files)
Last Recovery Point Created:	-
Next Recovery Point Scheduled:	Tuesday, November 20, 2012 @ 12:00:00 PM

On the right side of the main content area, there's a sidebar with three links: 'Configure Backup', 'Restore Data', and 'Configure Throttle'. At the bottom of the interface, a status bar shows 'Connected to Symantec.cloud' on the left and the Symantec logo on the right.

Get the critical information you need at a glance

Quickly and easily configure backups or restore data



Steps you can take

- **Know** what you need to protect
 - Where is your information being stored and used
- **Encrypt** confidential information
- Use a **Reliable** Security Solution
 - You need more than just Anti-virus

Steps you can take

- Map out a **disaster preparedness** plan today
 - Don't wait until it's too late
- Protect Information **Completely**
 - Combine backup with robust security
- **Stay up to date**
 - Security is only as good as the frequency with which it is updated



A man with short brown hair and a light beard, wearing a light blue and white striped button-down shirt, stands in an office. He has his arms crossed and is looking towards the camera. The background shows a bright window on the left, a desk with a white lamp and a potted plant on the right, and a blurred office environment.

Steps you can take

- **Educate** employees
 - About latest threats
 - Spammer/Social media techniques
 - Develop Internet security guidelines
 - Enforce strong passwords: 8+ characters with letters, numbers, symbols

Resources to Help You Get Started

- **Internet Security Threat Report**
- In-depth view of **cyber threat landscape**
- Understand how it affects you
- Learn to **defend your business** and employees

www.symantec.com/threatreport

Best Practice Guidelines For Businesses

Employ Defense-In-Depth Strategies:

Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network.

Monitor For Network Threat, Vulnerabilities And Brand Abuse.

Monitor for network intrusions, propagation attempts and other suspicious traffic patterns, identify attempted connections to known malicious or suspicious hosts. Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious Web site reporting.

Antivirus On Endpoints Is Not Enough:

On endpoints, signature-based antivirus alone is not enough to protect against today's threats and Web-based attack toolkits. Deploy and use a comprehensive endpoint security product that includes additional layers of protection including:

- Endpoint intrusion prevention that protects against unpatched vulnerabilities from being exploited, protects against social engineering attacks and stops malware from reaching endpoints;
- Browser protection for protection against obfuscated Web-based attacks;
- Consider cloud-based malware prevention to provide proactive protection against unknown threats;
- File and Web-based reputation solutions that provide a risk-and-reputation rating of any application and Web site to prevent rapidly mutating and polymorphic malware;
- Behavioral prevention capabilities that look at the behavior of applications and malware and prevent malware;
- Application control settings that can prevent applications

and browser plug-ins from downloading unauthorized malicious content;

- Device control settings that prevent and limit the types of USB devices to be used.

Secure Your Websites Against MITM Attacks And Malware Infection:

Avoid compromising your trusted relationship with your customers by:

- Implementing Always On SSL;
- Scanning your website daily for malware;
- Setting the secure flag for all session cookies;
- Regularly assessing your website for vulnerabilities;
- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users;
- Displaying recognized trust marks in highly visible locations on your website to inspire trust and show customers your commitment to their security.

Make sure to get your digital certificates from an established, trustworthy certificate authority who demonstrates excellent security practices. Protect your private keys. Implement strong security practices to secure and protect your private keys, especially if you use digital certificates. Symantec recommends that organizations:

- Use separate Test Signing and Release Signing infrastructures;
- Store keys in secure, tamper-proof, cryptographic hardware devices, and
- Implement physical security to protect your assets from theft.

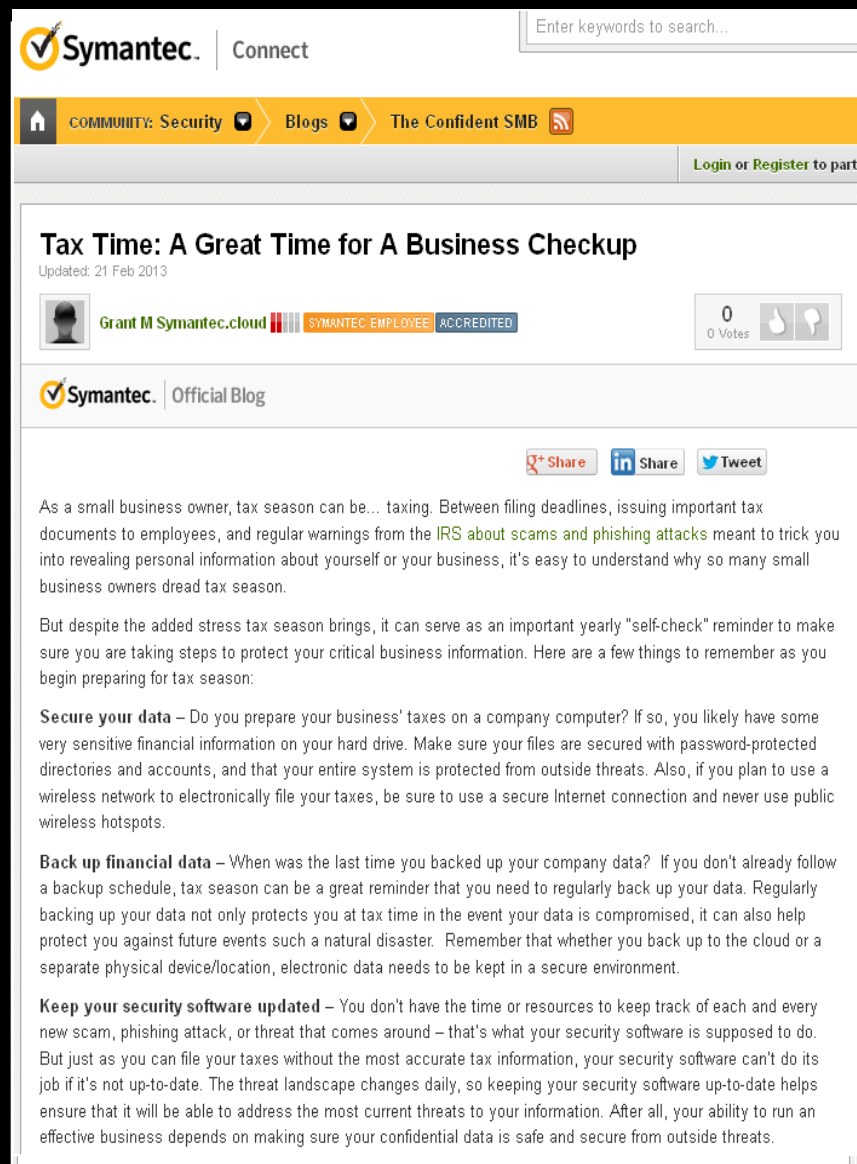
Use Encryption To Protect Sensitive Data:

Implement and enforce a security policy whereby sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution, which is a system to identify, monitor, and protect data. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization.

Resources to Help You Get Started

- **Connect** and join the conversation

www.symantec.com/connect



The screenshot displays the Symantec Connect website interface. At the top, the Symantec logo is on the left, and a search bar with the placeholder text 'Enter keywords to search...' is on the right. Below the header, a navigation bar features a home icon, the text 'COMMUNITY: Security', and links to 'Blogs' and 'The Confident SMB'. A 'Login or Register to participate' link is on the far right. The main content area shows a blog post titled 'Tax Time: A Great Time for A Business Checkup', updated on 21 Feb 2013. The author is 'Grant M Symantec.cloud', a Symantec Employee and Accredited member. The post has 0 votes. Below the post title, there are social sharing buttons for Google+, LinkedIn, and Twitter. The post text discusses the challenges of tax season for small business owners, including filing deadlines, important tax documents, and warnings from the IRS about scams and phishing attacks. It emphasizes the importance of protecting business information and provides three key tips: 1. **Secure your data**: Advise on securing financial information on a company computer, using password-protected directories, and ensuring secure Internet connections for electronic filing. 2. **Back up financial data**: Reminds users to regularly back up their company data to protect against future events like natural disasters. 3. **Keep your security software updated**: Stresses the need to keep security software up-to-date to address current threats to confidential data.

Looking Ahead in 2013 – Top 5 Security Predictions

1. Cyber conflict becomes the norm
2. Ransomware is the new scareware
3. Malware adds to the insanity
4. Monetization of social networks introduces new dangers
5. As users shift to cloud, so will attacks



Source: Symantec Connect Security Blog:

<http://www.symantec.com/connect/blogs/top-5-security-predictions-2013-symantec-0>



Thank you!

Aaron Hanson

Aaron_Hanson@symantec.com

Start your free 30-day trial: <http://go.symantec.com/trycloud>

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.