THE BIG SHIFT TO CLOUD-BASED SECURITY

How mid-sized and smaller organizations can manage their IT risks and meet regulatory compliance with minimal staff and budget.

QUALYS®
CONTINUOUS SECURITY

TABLE OF CONTENTS

“We’re too **small** to be a **target** for **cyber attacks**”

As a mid-sized or smaller organization, there is a lure of feeling safety in obscurity. “We’re too small to be a target for cyber attacks” is a common refrain used to justify a lax network security posture. Unfortunately, it’s a refrain that may come to haunt you. **The truth is your company doesn’t have to be a giant global corporation to be in the cross hairs of an attack.** Automated exploits of common vulnerabilities can equally sweep up victims on any Internet-facing network. As for targeted attacks, smaller companies are often hit first precisely because cybercriminals know these organizations have weak security – and may be a steppingstone to connected business partners or a large parent company. The good news is you don’t need to hire a crew of security experts to effectively manage IT risks and comply with security and privacy regulations. This paper explains how you can use cloud-based security to protect your network and ensure compliance without breaking the bank.

WHY SMALLER ORGANIZATIONS ARE VULNERABLE

Media stories about breaches tend to focus on big exploits such as Target and Heartbleed, which helps foster the illusion of safety for smaller organizations. Eight breaches during 2013 alone exposed more than 10 million identities each, according to Symantec's Internet Security Threat Report 2014. But to say, "My company doesn't offer a sliver of that opportunity to a cybercriminal," misses the key point. The direct and indirect costs of just one effective breach can bankrupt a mid-to-small sized company. And any sized company connected to the Internet is vulnerable. Here are three reasons why:

- **Cyberthreats and regulations don't care about business size**
  Most attackers don't care whether they're targeting a Fortune 25 firm or a small town manufacturer with 25 employees. In fact, the number of security incidents with confirmed data loss affected more small companies than large in 11 of 18 industries, according to the Verizon 2014 Data Breach Investigation Report. These breaches were overwhelmingly skewed to smaller companies (defined by Verizon as under 1,000 employees) in the Accommodation, Professional, and Retail industries. The common driver for cyber criminals is to steal and sell data and identities. Regulators are expecting the same security diligence from mid-sized and small firms as from large corporations. Consider the various data breach disclosure laws. They're not based on the size of the company but the quantity and type of customer records that are breached. While there may be slight differences in how regulations such as HIPAA, PCI DSS, and others affect mid-sized and even smaller firms, their overarching impact is the same.

- **Software flaws: an ever-growing concern**
  The number of software vulnerabilities announced daily shows no sign of letting up. According to the Common Vulnerabilities and Exposures List, sponsored by the National Cyber Security Division of the U.S. Department of Homeland Security, there were more than 6,100 software flaws reported during August 2013 through July 2014. That's over 16 newly announced software flaws every day. And these vulnerabilities, which make it possible for many forms of malware and attackers to gain entry to protected systems, are equally detrimental to businesses large and small. It's not just end-point operating systems, servers, and on-premise software that are at risk. Websites also pose an enormous risk. According to Symantec's report, 77% of legitimate websites have exploitable vulnerabilities and one out of every eight websites has a critical vulnerability.

- **The extended business risk: partners, suppliers, and other stakeholders**
  All businesses are under internal and external pressure. Targeted attacks such as spear-phishing often aim at smaller organizations. During 2013, 61% of spear-phishing attacks were on organizations smaller than 2,500 people, and 30% hit companies with less than 500 people, according to Symantec. The supply chain department was a primary target. Consequently, businesses are demanding to see the security and risk management plans of those with which they do a significant amount of business. They want to know about your disaster recovery and business continuity procedures. They want to know how you manage security defenses. And they want to know how you are protecting their confidential information.

COMMON APPROACHES TO SECURITY ARE TOO EXPENSIVE

Unfortunately, while the security threats and mandates for regulatory compliance affect all companies, it’s the mid-sized and small businesses that often don’t have the right staff or budget necessary to cost-effectively fight the threats and maintain compliance. Consider the SMB Information Protection Survey by Applied Research (published by Symantec in 2010) that shows that globally small and mid-sized businesses spend two-thirds of their IT management time and $51,000 annually focused on cyber security. That’s twice the amount of time and 27.5 percent more budget spent than for other areas of computing. That’s simply too high a price for security.

> *Small and mid-sized businesses today are spending 66% of their IT management time focused on security concerns.*

Qualys customers in mid-size and smaller organizations are telling a similar story. They say too much time is wasted on installing, maintaining, and managing security software and hardware. The biggest portion of this cost is labor.

The net result? Security efforts fall short: the tools prove tough to manage, require dedicated teams of experts, and the resulting reports provide inconsistent and too often inaccurate results. This means compliance and security objectives go unmet and the software proves too burdensome to maintain and troublesome to use. Eventually, cumbersome tools go unused. That means vulnerability assessments and remediation go undone, firewall policies go without updates, and flaws on web servers accumulate over time. Eventually, security slips, successful attacks against the business increase, and regulatory compliance mandates go unmet.

CLOUD-BASED SECURITY IS MORE AFFORDABLE & EFFECTIVE

Avoiding the cost and the complexity of traditional software is one of the reasons why Software-as-a-Service (or cloud) has become a mainstream delivery method for security solutions. Key benefits are low cost, faster-time-to-value and flexibility – without having to buy and maintain dedicated infrastructure.

Consider the example of updating security software. Traditionally, updates are performed by individual organizations, and duplicated for every system and at every business installation. With a cloud solution, the provider centrally updates its software applications and all customers are immediately updated without having to perform any special actions. Cloud delivery eliminates many of the security issues that plague traditional business-technology systems such as patching and software misconfiguration. The automation of software updates eliminates a substantial burden for the IT staff, and reduces the amount of time and expense required to manage ongoing operations.

In its Small and Midsize Business Cloud Trust Study (2013), Microsoft Corporation found half of respondents in the U.S. said 'time saved managing' and 'fewer internal IT resources' were the biggest benefits of cloud services. Significantly, 94% said they have experienced security benefits from cloud solutions that they did not achieve with their on-premises service. About 91% said organizational security had improved and 70% said they have reinvested money saved thanks to using cloud-based services.

These business benefits, cost savings and reduction in complexity are fueling the movement of many security, risk management and compliance applications into the cloud. Examples range from e-mail management to content-filtering, to disaster-recovery/business continuity, to vulnerability management and many other processes and technologies. Navigating and reaping the benefits of this transformation in risk management is one of the most important steps a mid-size or smaller business can take to manage ever-spiraling IT costs.

The adoption of cloud solutions is driven by the need to innovate, simplify and cut costs.

SEIZING OTHER BENEFITS OF CLOUD-BASED SECURITY

Adoption of cloud solutions is driven by the need to innovate, simplify and cut costs. One of the key distinguishing features of cloud-based security is the lack of equipment or software that must be deployed by the end user. All infrastructure is furnished and maintained by the cloud provider and hosted in secure data centers. This arrangement allows a business to avoid capital expenditures and to control ongoing costs. Some of the other benefits of security delivered via cloud solutions for mid-sized and smaller businesses include:

- **No hardware or software required**
  Since there is little or no equipment required on-premise and no software agents to install that might conflict with other applications, businesses can deploy the cloud-based service with ease. All that's required to operate the solution is a standard web browser.
- **Fast deployment, quality of service and maintenance**
  Cloud computing can be in use within a matter of minutes or hours, and its use of the web as a transport mechanism to provider data centers actually increases the availability of the service to the organization.
- **Scalability**
  Allows organizations to immediately respond to new operational requirements without having to deploy additional resources or staff. Expands to works automatically with the largest global networks.
- **Automation**
  Cloud delivery provides automated updates, automatic enterprise-wide collection and

collation of network assets and vulnerability data, and automatic reporting and alerting of new vulnerabilities with recommended paths to remediation.

- **The most up-to-date threat information**
  Recognizing the latest vulnerability, malicious code, or rogue web site requires a dedicated team of researchers to characterize the threat and update the security inspection process. The cloud ensures that the most recent information and functionality is provided every time the business uses the service.

QUALYS' CONTINUOUS SECURITY AND COMPLIANCE SOLUTIONS

Recognized as the leading provider of continuous security and compliance management solutions, Qualys enables organizations of all sizes to easily and cost-effectively ensure that their business technology systems remain secure and within regulatory compliance. Qualys makes it possible for businesses to strengthen the security of their networks and applications, as well as conduct automated security audits that ensure regulatory compliance and adherence to internal security policies.

Qualys delivers these solutions through a single Software-as-a-Service platform: Qualys Cloud Platform. All Qualys continuous security and compliance solutions can be deployed within hours anywhere around the globe, providing an immediate view of your organization's network assets, network and application security posture, vulnerability management and remediation workflow, and compliance with regulations and organizational policy. As a result, Qualys is the most widely deployed continuous security and compliance solution in the world, performing more than one billion audits per year.

Qualys
solutions include

Enterprise for global organizations
Express for SMEs
Express Light for SMBs
Consultant for auditors and consultants
Private Cloud Platform for MSSPs, enterprises and government agencies

For more information visit: **http://qualys.com**

QUALYS EXPRESS

Everything a mid-sized business needs to quickly discover network and application security risks and ensure policy compliance.

Qualys Express uses the power of the cloud to simplify your IT security and lower the cost of compliance. It helps you keep track of your networks, computers and web applications, and accurately tells you where they're vulnerable so that you can fix problems before attackers find you. It also automates many of the tedious parts of complying with regulations such as PCI and HIPAA so that you can spend more time growing your business and less time worrying about it.

Core components of Qualys Express include:

Asset Management

- Discover rogue devices & web applications
- Automatically identify, tag and organize assets
- Dynamically select assets for scanning or reporting

Security

- Find & track vulnerabilities in network servers & devices, and web applications
- Report security trends across systems & time
- Identify needed patches
- Prioritize & manage remediation
- Predict impact of Zero-Day attacks
- Interactively view security posture throughout your network
- Feed actionable security data to SIEM, GRC, ERM, WAF and more

Compliance

- Verify that systems implement required controls (such as password enforcement and information access policies)
- Test system configurations against golden images or baseline standards such as USGCB
- Test and submit PCI certification online
- Check for compliance with HIPAA, SOX, GLBA, Basel II, and more
- Automate procedural questionnaires for employees, vendors and partners
- Centralize collection of assessment evidence files

QUALYS®
Continuous Security

Qualys, Inc. – Headquarters
1600 Bridge Parkway
Redwood Shores, CA 94065 USA
T 1 (800) 745.4355

Qualys is global company with offices around the world.
To find an office near you, visit, **http://www.qualys.com**