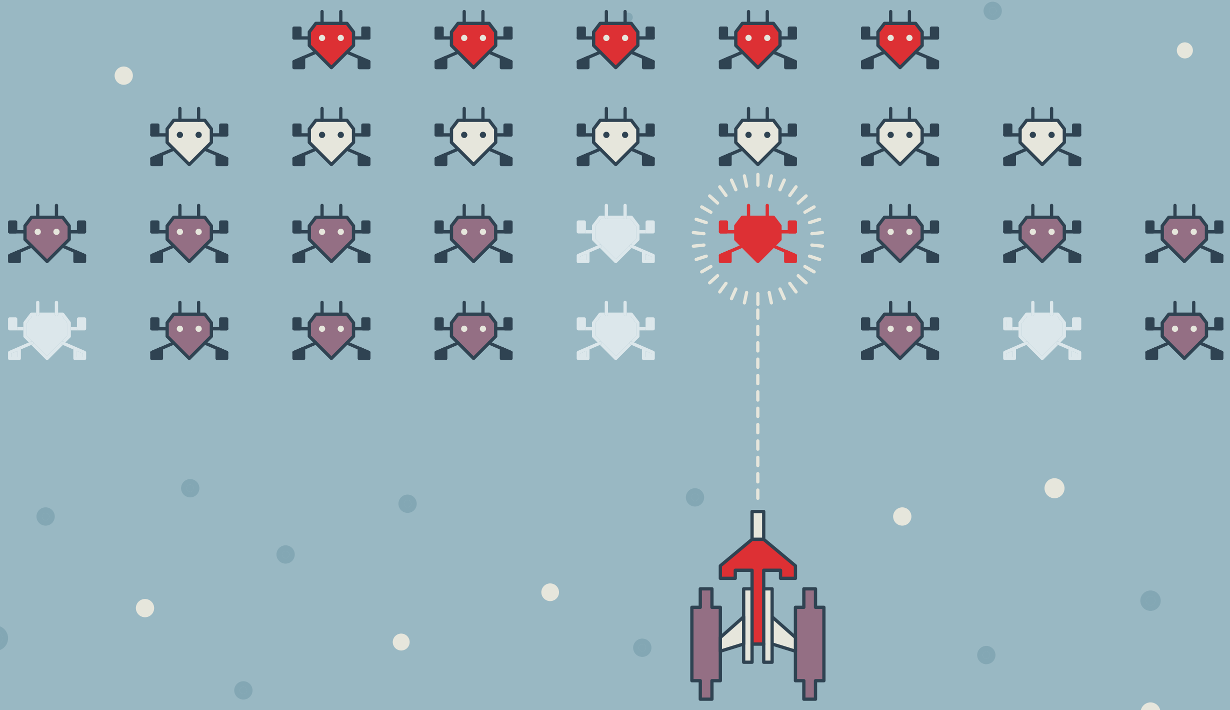
PREVENTING THE NEXT DATA BREACH

Protect your network from emerging threats with the right security solutions



MicroAge®
The IT Solution Experts

DELL PartnerDirect Premier

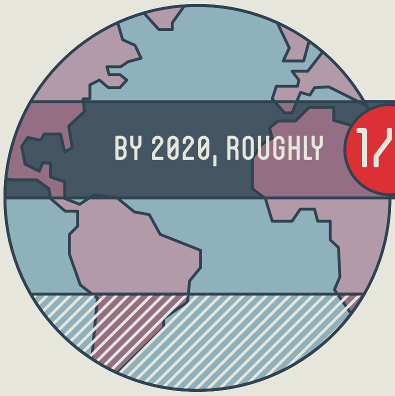
TABLE OF CONTENTS

INTRODUCTION

Hackers and data breaches are no longer the stuff of gripping Hollywood plots. Today, they are a serious business concern. In a world of digital transformation, mobile business and remote workforces, there's one word that's a top priority for any organization: ***Security.***

Over the past decade, the IT security landscape has changed, from one where everything was completely locked down to a more open approach that encourages 24x7 collaboration across company boundaries. At the same time, the threat landscape of vulnerabilities and malware has also evolved, with sophisticated targeted attacks and a range of devices that require 24x7 access to the corporate network. Organizations everywhere are spending considerable amounts of time and resources improving their IT security measures, trying to prevent the kind of attacks that can set a business back by months or years, if not take it down completely.

IDC predicts that by 2020, more than 1.5 billion people, or roughly 1/4 of the world's population, will be affected by data breaches.[1] With the mainstreaming of Bring-Your-Own-Device (BYOD) policies in offices across the globe, the window for a threat widens every day. And it's the unknown that can be the scariest threat of all.



BY 2020, ROUGHLY 1/4 OF THE WORLD'S POPULATION WILL BE AFFECTED BY DATA BREACHES[1]

> *The most stress comes from not knowing. You can prepare for 99% and it'll be that 1% that gets you.*
>
> **IT PROFESSIONAL, SPICEWORKS SURVEY**

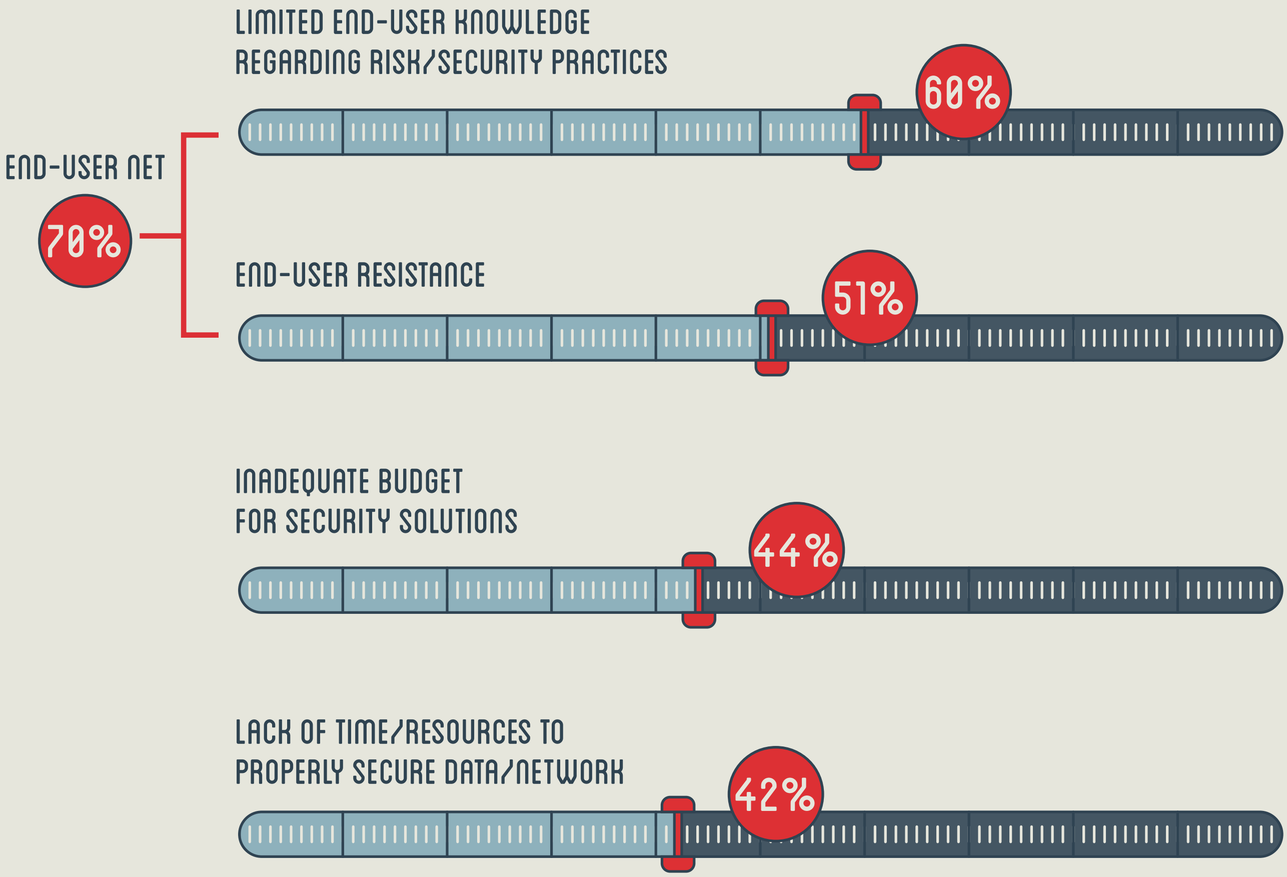
THE PRESSURES ARE REAL

A data breach can have disastrous consequences for a business. A company's failure to keep information—particularly customer information—safe can result in millions of dollars in lost revenue and regulatory fines, not to mention the impact on a company's reputation. A breach isn't just a temporary glitch—it's a serious business problem, which you can't easily shake off.

Besides staggering financial losses, the consequences to companies that suffer a data breach include lost business; significant time, effort and resources spent during the data breach resolution; loss of goodwill and customer churn. Recent research cites the average total cost of a data breach as $4 million. This has risen by 23% since 2013, meaning that a serious breach may eventually drive a company out of business.[2]

Staying a step ahead of these serious breaches is one of the biggest challenges facing today's IT organizations. Spiceworks recently surveyed IT professionals to get their insights on the threat landscape and best practices for keeping data secure. The survey revealed that 7 in 10 IT pros (70%) consider end users to pose the greatest challenge to securing data—far more than inadequate budget (44%), lack of time/resources (42%) or outdated technology (33%).

TOP DATA SECURITY AND PROTECTION CHALLENGES:

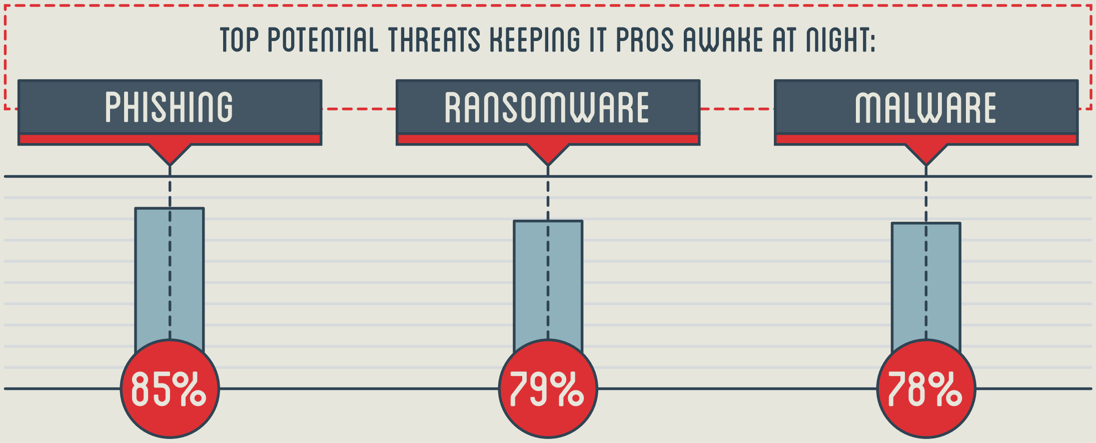


So, how can IT organizations protect against the inadvertent vulnerabilities and outright breaches caused by end users? Getting prepared for the worst-case scenario is a good start.

> *The biggest holes in any security system are people. We can spend millions of dollars on security, only to be taken down by a stupid cat video.*
>
> **IT PROFESSIONAL, SPICEWORKS SURVEY**

BREACHES HAPPEN: BE PREPARED

Today's IT organizations need to be prepared to detect, prevent and respond to issues in an ever-changing threat landscape. According to the Spiceworks survey, the top potential threats that currently keep IT pros awake at night are phishing (85%), ransomware (79%) and malware (78%). And of course, these threats often make their way onto the network via unsuspecting end users.



Some preventive actions that IT pros can take to stay ahead of threats:

CREATE USER AWARENESS:

Make end-user security awareness training compulsory for all employees. Providing privacy and security training to all employees, clients and others involved with data-related activities will bring about greater awareness on data breaches. Training employees can eliminate errors that could lead to a breach, as well as help them pick up on suspicious behavior by malicious insiders.

BAN UNENCRYPTED DEVICES:

Companies should institute a ban on laptops and other portable devices that are unencrypted because they are prone to attacks.

LIMIT DATA TRANSFERS:

Organizations should ban shifting data from one device to another external device. Losing removable media puts the data on the disk at risk.

RESTRICT DOWNLOADS:

Many breaches occur via drive-by downloads—malicious websites that can harm your system simply by being accessed. The ability to block certain types of websites when connected to the corporate network is key to a good security policy.

AUTOMATE SECURITY:

Automating systems that regularly check the password settings, server and firewall configurations can reduce the risk of compromising sensitive information.

PRIORITIZE SECURITY UPDATES:

It's important for IT to stay on top of applying patches and ensure that security-related software updates are current. An unpatched system is, by definition, operating with a weak spot just waiting to be exploited by hackers.

CONDUCT SYSTEM AND NETWORK SECURITY AUDITS:

IT professionals should regularly test and validate that only authorized items are running on the systems and network. It's important to create and review in-depth logs to monitor compliance with security protocols.

FIREWALLS FOR TODAY'S THREAT LANDSCAPE

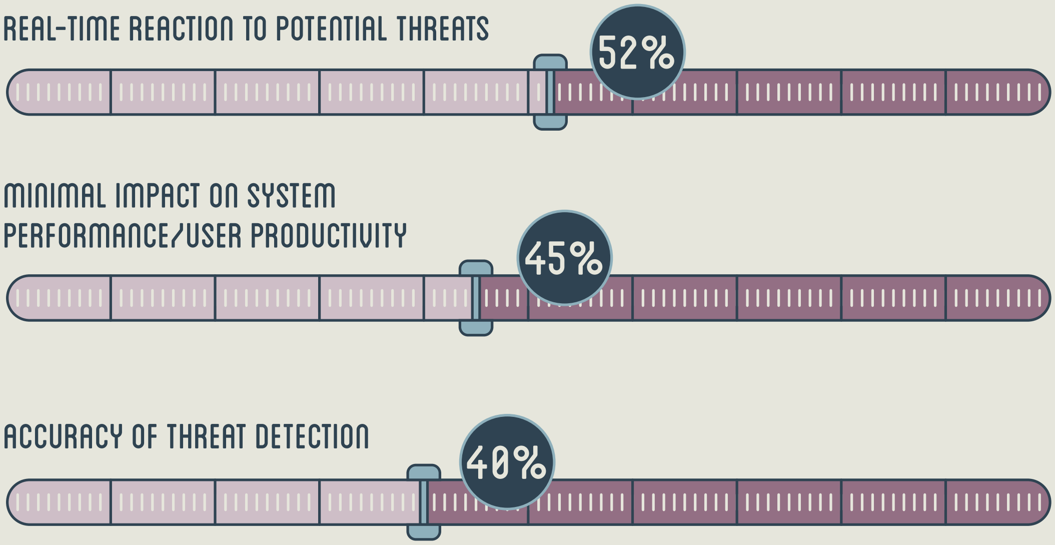
Even with proactive security measures in place, increasingly sophisticated cyber attacks have made it imperative for IT pros to constantly seek out and implement new, innovative security tools. One of the key problems is that traditional firewalls fail to provide administrators with adequate visibility and control over network traffic.

Enter the next-generation firewall.

Next-generation firewalls provide a single point of visibility into multiple areas of security functionality. By integrating multiple technologies in a single platform, they provide security teams with the ability to control network traffic in a manner that protects enterprises against malicious attacks. They combine the features of inspection firewalls, intrusion prevention systems, content filtering, and application control on a single piece of hardware—and allow those components to communicate with each other.

In fact, next-generation firewalls include the capabilities that are most important for data security/protection, according to surveyed IT pros. These capabilities include: real-time reaction to potential threats (52%), minimal impact on system performance/user productivity (45%), and accuracy of threat detection (40%).

NEXT-GENERATION FIREWALL CAPABILITIES:



INTRODUCING DELL SONICWALL

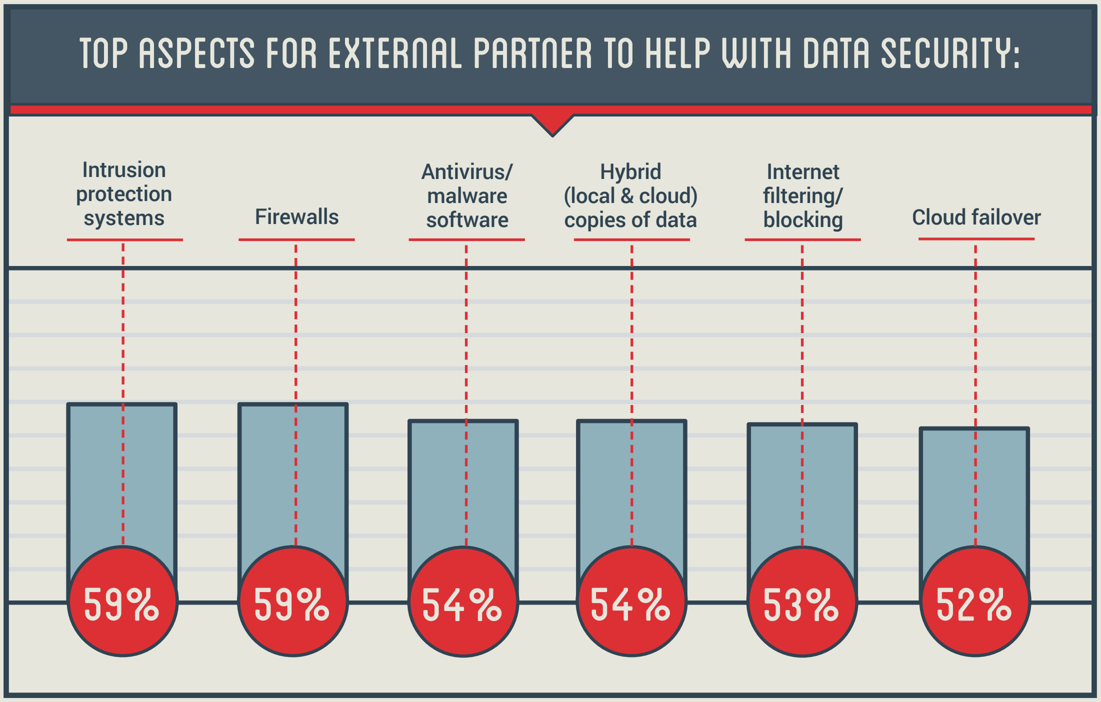
An industry-leading next-generation firewall solution, such as Dell SonicWALL, integrates hardware, software, and services for best-of-breed security. This gives systems, users, and data a deep level of protection without compromising network performance. Every Dell SonicWALL firewall is built on the reputed SonicOS architecture, which uses deep-packet inspection technology in combination with multi-core specialized security microprocessors to deliver application intelligence, real-time visualization, and other robust security features.

Features such as Dell SonicWALL Capture, a cloud-based service available with Dell SonicWALL firewalls, extends firewall threat protection to detect and prevent zero-day attacks. The firewall inspects traffic, blocks known malware, and sends suspicious files to SonicWALL Capture for analysis. The multi-engine sandbox platform executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity and maximizing zero-day threat detection.

PARTNER WITH AN UNBIASED EXPERT

When it comes to making critical security decisions for your business, finding unbiased guidance that focuses on the best individualized solution for your organization's needs can be a serious challenge. You need a trusted expert who's solely invested in strengthening your company's security infrastructure with the right solution.

Working with an objective solutions expert can put you on the fast track to protect your business at an affordable cost—and help you identify ways to optimize your existing infrastructure. The Spiceworks survey revealed that at least half of respondents indicated they are likely to look to a trusted partner to help them identify and implement such key security solutions as intrusion protection systems (59%), firewalls (59%), antivirus/malware software (54%), hybrid copies of data (54%), internet filtering/blocking (53%), and cloud failover (52%).



At MicroAge, our team of solution experts provides an unbiased perspective of technology solutions and supports clients in a way other resellers don't. Our account executives have spent an average of 13+ years in IT and strive to provide their clients with the best solutions to meet their changing business needs and evolving goals. Concerned about protecting *your* unique environment from emerging threats? Determined to find the best resources, but don't have time on your hands to do the research? That's why we're here—to help.

> *MicroAge account execs have spent an average of 13+ years in IT.*

YOUR SOLUTION, YOUR WAY

By partnering with hundreds of manufacturers, our account executives have the right resources to pull together a variety of security solutions—including the best next-generation firewalls—to help you make the best choice. Finding the right mix of cutting-edge, integrated solutions can help your business maintain a competitive edge and stay ahead.

The MicroAge reputation and culture is built on trust. Partner with us, so we can help you find the right fit for your company and prepare your network for the future.

To find out more about MicroAge and how we can help you, please contact us at Security@MicroAge.com or visit us at MicroAge.com/Security.

LEARN MORE

ABOUT MICROAGE

MicroAge is an award-winning provider of information technology solutions and services headquartered in Tempe, Arizona. We serve clients from the data center to the desktop with technology from industry-leading suppliers. Our objective, knowledgeable account executives are true experts, assisting clients with selecting IT solutions that best meet their unique requirements. MicroAge is a well-known name and a respected industry pioneer with a heritage of industry innovation spanning five decades. Top partners include Dell, Cisco, Hewlett Packard Enterprise, Lenovo, Microsoft, HP, VMware, EMC, Apple and APC. MicroAge is also proud to rank #2 among medium-sized businesses on the 2015 *Phoenix Business Journal's* list of the Best Places to Work in Phoenix.

ABOUT THE SURVEY

MicroAge commissioned Spiceworks to conduct a survey in July 2016. The survey addressed IT decision-makers in the US to uncover the insights and understand the decision-making process around data storage, backup, recovery, and security. Results of the survey included responses from 153 participants from IT departments across industries including manufacturing, healthcare, financial services, and education.

MicroAge®
The IT Solution Experts

DELL PartnerDirect Premier

SOURCES:

[1] "FutureScape: Worldwide IT Security Products and Services 2016 Predictions," *IDC*, Nov 2015.

[2] "2016 Cost of Data Breach Study: Global Analysis," *Ponemon Institute*, June 2016.