

# THE ULTIMATE SECURITY GUIDE

CLOUD  
EDITION

**THE AGE OF RESPONSE:**  
HOW AI ENABLES NEAR-INstant  
REACTIONS TO DIGITAL THREATS

**WHO IS  
ACCOUNTABLE  
FOR A HYBRID  
CLOUD  
SECURITY  
BREACH?**

**HOW HACKERS CHANGED THE  
WAY WE BUILD AND PROTECT  
NETWORKS AND WHY IT PROS  
MUST ADAPT...OR GET HACKED**

**1400 SENIOR  
IT PROFESSIONALS  
WEIGH IN ON  
CLOUD SECURITY**

**THE HIDDEN VALUE OF  
CLOUD MANAGED  
SERVICE PROVIDERS**

**USING CROWD INTELLIGENCE  
TO FIGHT EMERGING THREATS**

**THE 6 BUILDING BLOCKS  
OF A CLOUD SECURITY  
PROGRAM**



## PLATINUM SPONSOR



## GOLD SPONSORS





# outthink threats

## What's Watson working on today?

Seeing threats others might miss helps you respond to attacks before they endanger your business. IBM Security and Watson can draw security intelligence from thousands of security blogs, online forums and images—including those hidden within unstructured data and unseeable by other systems. By connecting data-points, you can discern patterns, detect and prioritize threats and even anticipate attacks. Cognitive security is here. [ibm.com/cognitivesecurity](http://ibm.com/cognitivesecurity)

**When everything thinks, you can outthink.**





# SPRING 2017 ISSUE 4

COMPLETE LIST.  
WHAT'S IN THIS ISSUE

▶ PAGE 02  
ULTIMATE SECURITY GUIDE SPONSORS

▶ PAGE 05  
WELCOME LETTER

▶ IBM - PAGE 08

THE AGE OF RESPONSE: HOW AI ENABLES  
NEAR-INSTANT REACTIONS TO DIGITAL THREATS

▶ TREND MICRO - PAGE 10

WHO IS ACCOUNTABLE FOR A  
HYBRID CLOUD SECURITY BREACH?

▶ SOFTCHOICE - PAGE 12

THE HIDDEN VALUE OF CLOUD  
MANAGED SERVICE PROVIDERS

▶ KASPERSKY - PAGE 14

USING CROWD INTELLIGENCE  
TO FIGHT EMERGING THREATS

▶ FORTINET - PAGE 16

THE 6 BUILDING BLOCKS OF  
A CLOUD SECURITY PROGRAM

▶ MCAFEE - PAGE 18

1400 SENIOR IT PROFESSIONALS  
WEIGH IN ON CLOUD SECURITY





## ▶ CONTRIBUTORS

**ANGELI GHELANI**

Marketing Coordinator

**AYUMI BUCKLE**

Marketing Database Lead

**EMILY DAVIDSON**

Digital Marketing Lead

**KARLY PIERCE**

Marketing Manager

**MARTIN PIETRZAK**

Digital Marketing Supervisor

**MICK WARNER**

Marketing Enablement Supervisor

**GEORGINA BURNS**

Marketing Manager

**PATRYK BOGNAT**

Graphic Design

## ▶ ADVERTISING INQUIRIES

**GEORGE MYRTOS**

Category Lead

Enterprise Software and Security

[George.Myrtos@softchoice.com](mailto:George.Myrtos@softchoice.com)

## ▶ ULTIMATE SECURITY GUIDE

SPRING 2017 - ISSUE 4

PLATINUM SPONSOR

**IBM**

**FORTINET**

GOLD SPONSORS

**Kaspersky**

**McAfee**

**Trend Micro**

Softchoice LP © 2017



**George Myrtos**

Category Lead, Business Development

**Softchoice Enterprise Software & Security**

**Dear reader,**

**AS** the security industry feels the reverberations from ransomware attacks like WannaCry and HospitalGown, it raises an important question for front-line security professionals like us: How do we prevent these types of attacks?

**For me, the answer lies in the cloud.**

According to the McAfee study featured in this guide, almost eighty-five percent of the 1400 security professionals surveyed report that they trust some or all their sensitive data to the public cloud. But the security talent supply is low, and the cost of breaches is very high. With a perpetually-exploding dataset to manage, companies have little choice but to trust a cloud service provider with their data.

Once that dataset is virtualized and distributed, it creates a divided ecosystem. Trusted networks and certified devices sit opposite untrusted networks and the Internet of Things (IoT) edge. Arguably, distributed networks are harder to hack, but they're also tougher to manage. When a hacker breaches your network, questions around accountability, due care, and brand perception will fly, fingers will point and shareholders will demand answers.

To quote the ancient philosopher Socrates, "The only true wisdom is in knowing you know nothing." So much of what IT staff must manage is unknown, like Shadow IT, licensing requirements, and unknown network devices. In my experience, I have not seen a client yet who did not have something to discover about their environment after we completed an assessment.

At the end of the day, YOU are responsible for securing your data. Not a cloud service provider, not the latest Magic Quadrant solution, and especially not a firewall. In a paradox, we have discovered that companies who take a step back from cloud security, actually increase the rewards they gain from it. How?

**IT staff must choose to take a step back from a huge volume of work they clearly can't afford.**

By working with a trusted partner, companies offload the work of day-to-day tasks like patch management and IT procurement. No partner will ever understand the user base (or have the same access) like the IT staff will. But they just have to make the choice to free up their time and focus on a strategy that reflects the true needs of their business.

The end goal is risk management, and you can manage risk using best-in-class partners. Partners who offer advice from experts that have dedicated their careers to guiding IT staff like you through a complex world of service providers and products. To me, this is a much more cost-effective strategy than hiring expensive (and increasingly rare) security staff.

I would like to thank all our partners for being part of this journey with us and to you for taking the time again to read this guide.

**George Myrtos**

Category Lead, Business Development

**Softchoice Enterprise Software & Security**

# MEET OUR DEDICATED SECURITY TEAM



**ANDREA KNOBLAUCH**  
PreSales Technical Architect



**GEORGE MYRTOS**  
Category Lead,  
Enterprise Software and Security



**MIKE COIT**  
PreSales Security Architect



**ANDREW CAMPBELL**  
PreSales Technical Architect



**JEFF KROTH**  
Security PreSales Architect



**MIKE STINES**  
PreSales Security Architect



**ALEXANDRA LEE**  
PreSales Technical Architect



**JEREMY BANDLEY**  
PreSales Technical Architect



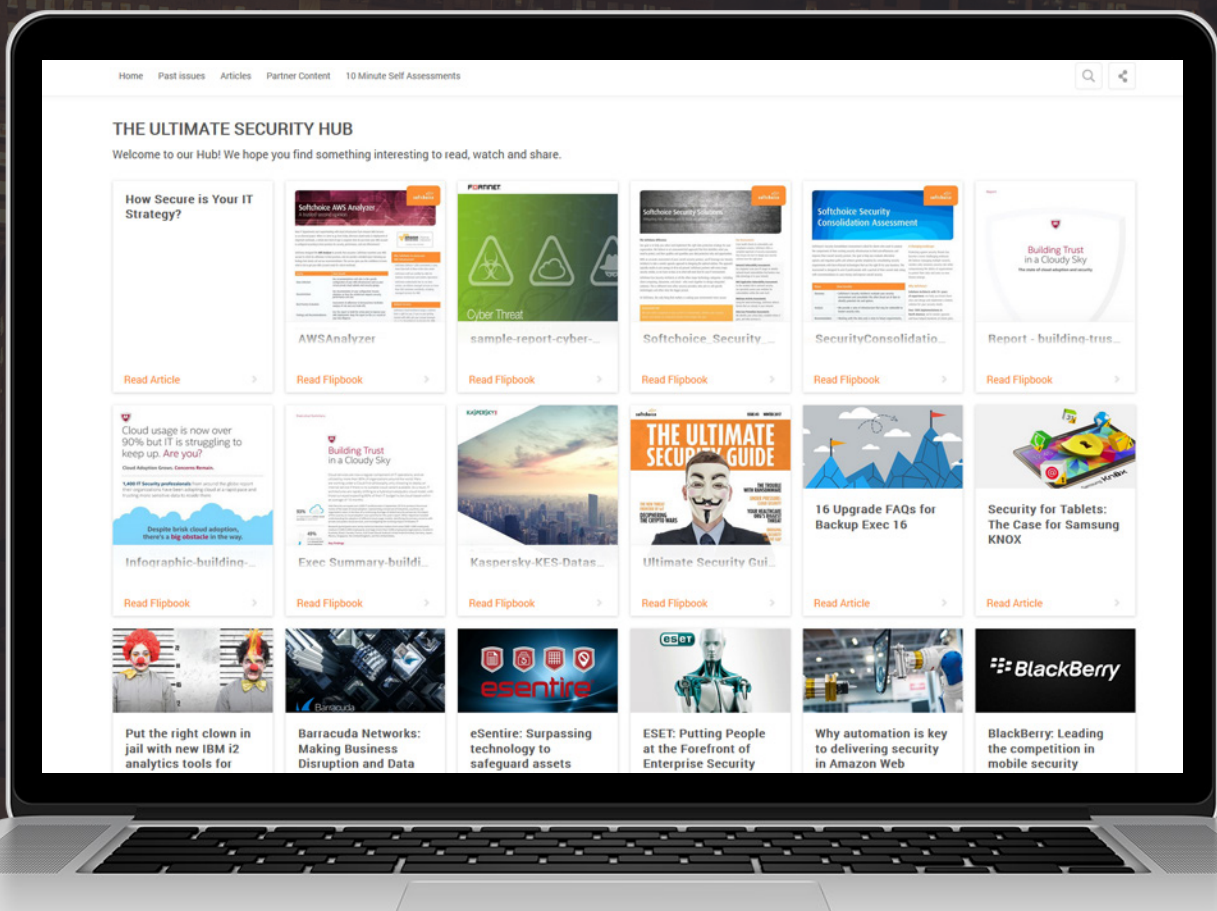
**TREVOR MULVIHILL**  
PreSales Technical Architect



# THE ULTIMATE HUB FOR SECURITY

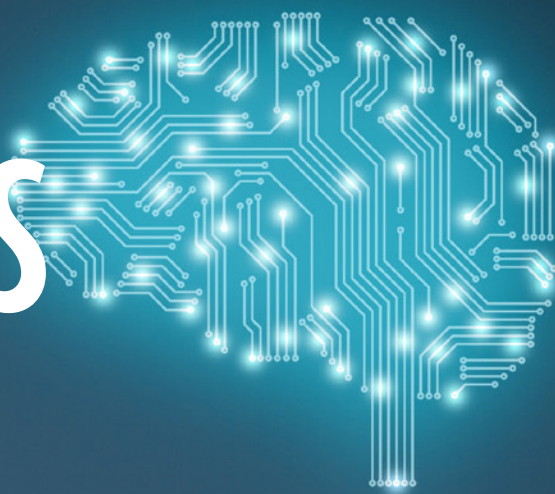
Visit Our Microsite To Access:  
**Free Assessment Tool**  
**How-To Content From Our Partners**  
**The Latest Security News And Updates**

►► BROWSE MORE CONTENT ◀◀





# THE AGE OF RESPONSE: HOW AI ENABLES NEAR-INSTANT REACTIONS TO DIGITAL THREATS



**I**t wasn't long ago that IT security meant building a network fortress of technologies and controls to keep the bad guys out. Then the cloud, BYOD, Shadow IT, and massive attacks on Home Depot, Sony, the U.S. Office of Personnel Management and other well-fortified victims arrived. Suddenly, organizations had to face the truth that they would get hacked despite their best efforts. The focus has now moved to quick, effective response.

We spoke with Michael Bright, IBM Security Operations and Response Leader for Canada, for an update on how Watson's AI, paired with a security intelligence tool, is accelerating threat detection and response in the cloud-enabled enterprise.

► **MOST ORGANIZATIONS HAVE SECURITY CONTROLS IN PLACE BUT MANY LACK FULL OPERATIONAL VISIBILITY**

"If you don't have a way to get that visibility, you can't detect and react—let alone be proactive—in the face of today's attacks," says Bright. In many cases, when a company is breached, it has powerful security tools generating lots of alerts. "Unfortunately, the difficulty lies in pulling all those alerts together to see the danger of the attack in progress."

"The biggest challenge organizations face is how



## outthink threats

### What's Watson working on today?

Seeing threats others might miss helps you respond to attacks before they endanger your business. IBM Security and Watson can draw security intelligence from thousands of security blogs, online forums and images—including those hidden within unstructured data and unseeable by other systems. By connecting data-points, you can discern patterns, detect and prioritize threats and even anticipate attacks. Cognitive security is here. [ibm.com/cognitivesecurity](http://ibm.com/cognitivesecurity)

**When everything thinks, you can outthink.**

IBM and its logo, ibm.com and Watson are trademarks of International Business Machines Corp, registered in many jurisdictions worldwide. See current list at [ibm.com/trademark](http://ibm.com/trademark). Other product and service names might be trademarks of IBM or other companies. © International Business Machines Corp. 2017

to analyze all that information and understand that it's one security incident."

## SECURITY INTELLIGENCE IS ABOUT USING COGNITIVE INTELLIGENCE—A COMBINATION OF MACHINE LEARNING, NATURAL LANGUAGE PROCESSING, AND OTHER AI TECHNOLOGIES— TO DO THAT FOR YOU AUTOMATICALLY.

It's also about the response. "In the face of a suspected attack today, an analyst typically does an online search and looks at hacker sites, security forums and blogs to figure out what this hash of a file or that fishy IP address indicates and how to respond," says Bright. "Security intelligence harnesses analytics, cognitive computing, and automation to do most of that research and analysis for you." That means analyzing a lot of unstructured data, as opposed to the structured data generated by various security logs.

### ► SECURITY INTELLIGENCE PROVIDES THE DEEP SECURITY EXPERTISE AND KNOWLEDGE OF THE LATEST THREATS THAT MOST IT TEAMS SIMPLY CANNOT MATCH

"We offer an application powered by Watson called IBM QRadar with Watson," says Bright. "It takes advantage of the QRadar infrastructure to normalize the security skills gap. When you suspect you have an issue, QRadar Advisor with

Watson provides cognitive intelligence, infrastructure insight, and knowledge of everything on the Internet related to security to analyze the scope and seriousness of an attack."

For the past two years, IBM has worked with MIT, the University of Ottawa and the University of New Brunswick, among others, to teach Watson the Internet language around security. QRadar goes out to the entire Web and the Dark Web to do its own research to give you a view of what it sees. "It will tell you based on its research that you've been hit by X malware perpetrated by Y attack author," says Bright. "It even provides visualization of the attack chain and explains why you must address it."

Resilient Incident Response Platform (IRP) is another IBM tool that spells out the steps you need to take to respond to that attack.

"In sum, QRadar shortens the time from seeing something that might be bad to the realization that it is bad. Resilient IRP shortens the time it takes to understand what attack is taking place, what it has access to and the steps you must take to mitigate it."

### ► EVEN IN THE CLOUD, SECURITY IS STILL SECURITY. THE ONLY DIFFERENCE IS THAT YOU MUST RELY ON A SERVICE PROVIDER

"You need to make sure each cloud service has the right security infrastructure in place and gives you full cloud visibility," says Bright. "With Software as a Service (SaaS), such as Office 365 or Microsoft Exchange, it's important to understand

the nature of the security logging it provides and make sure it's activated." For example, initially, Microsoft Office 365 didn't activate logging by default.


You also need to know where your confidential information is stored. "Is it in the cloud? What security controls do you have in that environment? How do you protect that information either in the cloud or as it leaves your organization and moves into the cloud? What are your users doing with that information? Are they copying it onto their email accounts? What are the company's policies around putting that information out there?"

This is all critical, as there's a transition in 2017 from hackers stealing and monetizing structured data, such as credit card information, to unstructured data, such as email archives, confidential financial information and source code.

### ► SECURITY GURU, BRUCE SCHNEIER HAS SAID THAT THE EARLY 2000'S WAS THE AGE OF CONTROLS. NOW WE'RE IN THE AGE OF RESPONSE

"Yes, analytics and cognitive intelligence can help with detection," says Bright "but even more important for the future is that they can enable instant response—what do I do, how do I control the threat situation and how can I be proactive in my response strategy?"

Organizations may not be able to control the behavior of hackers, but they are the pilots of what they do (or what they don't do) about it.



# WHO IS ACCOUNTABLE FOR A HYBRID CLOUD SECURITY BREACH?

**A**ccording to Mark Nunnikhoven, Trend Micro Vice President of Cloud Research, the answer is obvious: You are. Your organization entrusts you with their data and they expect you to take the proper precautions.

We interviewed Mr. Nunnikhoven about risky assumptions companies make, detecting shadow IT, choosing a provider and the key to a resilient hybrid cloud. Despite obvious risks, he remains optimistic that the cloud is the way of the future.

#### ► THERE ARE 6 LAYERS OF OPERATIONAL CLOUD SECURITY

According to Nunnikhoven, you achieve hybrid cloud security by first understanding the security stack and shared responsibility between on-premises data center IT and the public cloud service.

"There are six layers of operational security," says Nunnikhoven: "The physical layer, which includes buildings and real estate leases, is the bottom of the stack. The next layer is infrastructure, such as power and cooling. Then comes virtualization, operating systems, applications, and data. For each of those layers, someone is responsible for security and operations. When you move into the cloud you share those duties with the cloud provider. You need to understand exactly what their respective responsibilities are."

It is also vital to establish a recovery plan for when (not if) something goes wrong.

#### ► SENSITIVE DATA IS 99.999999999% MORE SECURE IN THE CLOUD

According to Nunnikhoven, keeping data in-house is riskier than storing data in the public cloud, as

most IT departments overestimate their security capabilities. "The top cloud services offer up to eleven nines of availability (99.99999999 percent) and twenty-four hour expert security monitoring and response. Very few IT departments can match those capabilities in house."

**A MORE EFFECTIVE STRATEGY USES THE PUBLIC CLOUD FOR PRIMARY DATA STORAGE AND BACKS UP TO YOUR ON-PREMISE DATA CENTER OR TO A DIFFERENT REGION IN THE CLOUD WITH A DIFFERENT SET OF INFRASTRUCTURE.**

... continue next page



# WHAT'S YOUR X?

Solve it with Hybrid Cloud Security,  
powered by XGen™

Learn more at [www.trendmicro.com/xgen-server](http://www.trendmicro.com/xgen-server)



## ► UNEARTH SHADOW IT, BUT DO NOT BURY IT

Nunnikhoven feels that Shadow IT results from IT service quality limitations. “Most IT departments can’t match the effortless file sharing of DropBox and Box.” Rather than banning Shadow IT, Nunnikhoven suggests cooperation and education. “Go to your file sharing users and let them know there’s a corporate version of Box or DropBox that gives IT the visibility, controls, and reports that benefit the organization’s security stance.”

How do you discover all of your Shadow IT instances? “Start by talking to the finance department, as people rarely pay for shadow IT out of their own pockets. Then analyze outbound network traffic to see if some teams are making constant requests to cloud services.”

Infrastructure in the cloud scales up and down so quickly, there’s no way to put a fence around it all.

“It’s far easier and more effective to protect each of those assets where they are as opposed to where they sit,” says Nunnikhoven. “Yes, you want those defense layers but you need to armor individual soldiers as well.” This means building security features into your applications as they’re developed, instead of trying to secure them after they’re built.

## ► NEVER ASSUME THAT YOUR DATA IS PROTECTED AUTOMATICALLY

The biggest mistake organizations make in the hybrid cloud is extending their existing data center into AWS, Google or Azure, wrongly assuming that everything will route through their security controls. According to Nunnikhoven, “Ignoring the native public cloud security controls is neither productive nor safe. Those that start with a cloud-native security perspective will have much less exposure and better overall security awareness and results.”

## ► ORGANIZATIONS SHOULD RECOGNIZE THEIR NEED TO MOVE FULLY INTO THE CLOUD SOONER RATHER THAN LATER

“Your in-house data centers and investments won’t last forever,” says Nunnikhoven. “By the end of that five-to-seven-year data center lifecycle, it’s probably time to move it all to the cloud. Start designing your operations and security around that future and apply cloud-native philosophies and tools on-premises now to make sure you have one toolset and workflow across the hybrid environment.”

## ► CHOOSE CLOUD-AWARE SECURITY SOLUTIONS

Make sure any hybrid cloud security solution you choose understands and integrates easily with AWS, Google or Microsoft Azure and will scale easily up and down automatically with the service. Look for programmability as well, as just about everything in the cloud is accessible via an Application Program Interface (API).

“The key to a resilient hybrid cloud is understanding that security is not simply about keeping things out.”

Nunnikhoven continues, “It’s really about making sure your servers and systems are doing what you expect and nothing more.” For example, make sure your shoe sales website processes only valid transactions and serves up traffic to valid consumers. Deploy multiple fallbacks for each control, such as an intrusion prevention system in addition to a firewall. You must test your processes and adapt continually as change is constant in the hybrid cloud.

**WHEN AN ENTERPRISE-LEVEL  
BREACH HAPPENS, POINTING THE  
FINGER AT YOUR PUBLIC CLOUD  
SERVICE PROVIDER IN FRONT OF  
SHAREHOLDERS IS LIKE TELLING  
THEM YOU’RE FLYING BLIND.**

Ultimately, you are accountable and responsible for proving that you have taken all possible precautions.





# THE HIDDEN VALUE OF CLOUD MANAGED SERVICE PROVIDERS

**T**housands of years ago, our cave-dwelling ancestors depended on a simple set of shared responsibilities. “I hunt the meat. You pick the berries.” With specialized roles and shared responsibility, everyone ate fresh food and more of it.

Unfortunately, today’s cloud security leaders rarely follow the same approach. Too often, organizations have limited IT resources, resulting in one IT manager holding accountability for many specialized areas of the data center. This causes major risks in setting up, maintaining and optimizing cloud and hybrid environments.

“A cloud provider delivers services to replace some of your IT, but not all of it. Where their responsibilities stop, yours begin,” says Michael Lucas, the Amazon Web Services (AWS) Practice Leader for Softchoice.

Lucas, who is a SaaS and DevOps expert, stresses the dangers of not understanding this

relationship. Overlook one small aspect of your security duties, and major damages follow. These include regulatory fines, loss of customer trust, even ransomware assaults.

## ► WHO IS RESPONSIBLE FOR WHAT?

When it comes to security, who owns what responsibility all depends on the cloud service model you use: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS). With IaaS, the cloud service provider is responsible for the core infrastructure security, which includes storage, networking and compute. As you move from IaaS, to PaaS and then to SaaS, you’ll find that you’re responsible for less and the cloud service provider is responsible for more.

But you are almost always on the hook for extremely crucial aspects of your defenses, such as access management, endpoint protection, and data classification.



Knowing what is yours to handle is a confusing and often overwhelming process. But it gets even harder due to what is often seen as the cloud's biggest asset: its ease of use.

► **USERS BELIEVE THEY CAN HANDLE ALL CLOUD DEMANDS ON THEIR OWN.**

And to a certain degree, that is true. Anyone with minor tech knowledge can take the company credit card, spin up a server and be running a new workload in less than a day's work. Lucas points to Amazon's cloud service as an example.

"AWS empowers customers to get in there and 'do it yourself.' DIY at Amazon is big," Lucas explains. "When companies feel empowered, having no managed service provider is actually quite appealing."

But just because you can do something on your own, doesn't mean it's a good idea. Lucas points out that many businesses aren't qualified for all the work and configurations best-practices demand.

"You should be thinking of the cloud like a pile of building blocks. You can do amazing things with it, you can build whatever you want. But if you don't have the right mason, the right architect, your wall is going to fall apart," he says.

► **SECURITY PROS MIGHT UNDERSTAND THEY NEED HELP, BUT BRINGING IN YET ANOTHER PARTY IS HARD TO SWALLOW.**

Remember, when the cloud was still emerging, it didn't just demand new technological approaches. It demanded new cultural attitudes, too. That same concern lingers to this day,

especially when it comes to adding a third partner into the mix.

Similarly, companies look at a managed service provider, offering to help with their cloud needs, and all they see is more complexity.

"It's like adding a service onto another service," he says, "and that just seems counter-intuitive."

► **WHEN YOU FIND THE RIGHT MIX OF SHARED SERVICES, EVERYTHING GETS BETTER.**

Teaming up with a managed service provider gives you direct access to a very select group of individuals whose only job is to understand the cloud, and help organizations configure their environments according to best practices and to avoid mistakes. Hiring resources with the same level of expertise is a challenge — due to a limited supply of expensive and hard to retain IT security talent.

Not to mention, the sheer volume of work entailed is more than the average company can afford. Take for example security updates and patches. Take security updates and patches for example. "AWS released more than one update a day last year," says Lucas. "With each change came an opportunity for an exploit." Staying on top of these patches is a full-time job.

**ONE OF THE ESSENTIAL VALUES OF THE CLOUD IS THAT IT GIVES IT A FIGHTING CHANCE AT GETTING CLOSER TO THE BUSINESS**

- by working on strategic goals instead of 'keeping the lights on'. The same is true for the security team.

Remember, shared responsibility means you still have some work on your plate. When you work with another provider, they help prioritize your actions by identifying gaps and showing you what you can do to close them. Businesses need to see what is lacking before they can act. Plus, no partner will ever understand your user base or have the same access as you do. By freeing you to focus, you're more likely to build a security strategy that reflects the unique needs of your business.

"Unfortunately, there is a perception that cloud takes care of all your security problems," sums up Lucas.

► **THE FIRST STEP ON THE PATH TO SHARED RESPONSIBILITY IS BOTH THE SIMPLEST AND MOST IMPORTANT.**

It's about facing reality and realizing that, no matter how much value your cloud provider offers, you still have a job to do.

"If I had to offer one piece of advice to any company adopting cloud services, whether its Azure or AWS or Google, it's this. You, the organization, are primarily responsible for securing your data. Passing liability is not the answer."

And while many businesses would like to think they can handle these new tasks all on their own, they probably shouldn't. It's costly, time sucking and you will be stuck with diminishing returns and less value than if you teamed up with an experienced partner.

## SOFTCHOICE WORKLOAD ANALYZER PLOTting THE RIGHT APPLICATION PATH

Based on client feedback and real-world deployment findings, Softchoice created the Workload Analyzer to fast-track your evaluation of the application environment and cloud options

►► [Learn More](#)



# USING CROWD INTELLIGENCE TO

# FIGHT EMERGING THREATS

**J**eremy Smolik, Channel Systems Engineer at Kaspersky Labs tells the story of how a new malware strain injects itself into RAM without the need for a file or attachment.

"IT personnel rarely lock down their administrative tools," he says. "Kaspersky Labs found it by scanning RAM and looking for patterns in tools that were compromised."

Left undetectable by standard security defenses, the new strain exploits legitimate administrative

tools like PowerShell. The malware hides for months, snooping credit card data and stealing credentials. Today it lurks on banking computers, ATMs and Domain Controllers.

New malware and ransomware threats emerge constantly. How will the average organization (with an average budget) keep up? "There is a necessity to crowdsource threat intelligence," Smolik says. IT services transitioned to the cloud rapidly and now it is more important than ever to share security event information. Here's why.

## ► THE RUSH TO ADOPT CLOUD SERVICES LEFT GAPING HOLES IN SECURITY

The implementation of cloud (or hybrid cloud) security technology is never cheap, but neglecting it comes with a heavy penalty. Osterman Research found that the average security event for a large enterprise costs \$1 million. In some cases, losses are much higher.

Ransomware costs, on average, \$625 per device for an organization. That adds up to



# DEVELOPED SPECIFICALLY FOR SMALL AND MEDIUM-SIZED BUSINESSES, KASPERSKY ENDPOINT SECURITY CLOUD LETS YOU MANAGE SECURITY FOR MULTIPLE ENDPOINTS, DEVICES AND FILE SERVERS REMOTELY, FROM ANYWHERE.



►► [Download Datasheet](#)

millions of dollars in the event of an enterprise-wide breach.

But the loss can stretch beyond technology costs or stolen funds. The fallout can be far more expensive. Newspaper headlines, eroded customer confidence, shareholder action, threatened job security for management and IT professionals, and government fines are just a few of the consequences. IT, therefore, must remain vigilant.

**“IF YOU ARE THE CUSTOMER, YOU NEED TO SECURE YOUR OWN DATA AND APPLICATIONS,” SMOLIK ADVISES.**

He advises everyone to not just back up their cloud data, but to test their backups regularly. “Only 42% of those hit with ransomware recover their data,” said Smolik. “Their backups either failed, were incomplete or were already infected. Backups can fail, data can get corrupted, and large amounts of organizational data missed. Backup all of the data you send to the cloud, and continue to apply security best practices.”

## ► CROWDSOURCED INTELLIGENCE BATTLES A MALWARE MELEE WITH PROACTIVE DETECTION

To address such a massive amount of malware and ransomware, Kaspersky uses all of its endpoints as security event monitors. “The idea is that all of those endpoints, mobile devices, laptops, mail servers and virtual machines

are active as sensors and the platform is monitoring the types of events and traffic patterns that would look suspicious based on what we’ve learned from our cloud intelligence,” Smolik says.

Kaspersky’s crowdsourced pool of research contains 250,000 customers with eighty to one hundred million endpoints connected to it.

**EVERY DAY, THESE ENDPOINTS DETECT 600,000 GLOBALLY-TARGETED ATTACK SAMPLES PER SECOND. AT THE END OF THE DAY, KASPERSKY EXPERTS LABEL ROUGHLY 300,000 OF THESE AS UNIQUE, OR NEW ATTACKS.**

Smolik continues, “...you’re not only crowdsourcing information [globally] from your network, but using the intelligence to take a proactive approach [to security] because you’re learning about it in near real time,” Smolik adds. “What I mean by that is collecting snippets of data and traffic patterns and events around the world that point to certain malware actors or malware activities that you can proactively protect against.”

Then, the data is fed into Kaspersky’s homogeneous solution offerings that employ the same approach, the same dashboard and the same management portal to all endpoints, all servers, and all services. Annually, they publish the top

forty threats to the public and customers in a particular enterprise or region can subscribe to those threat reports to stay on top of threats before they hit the news.

## ► SMOLIK’S BIGGEST PIECE OF ADVICE: QUESTION EVERYTHING AND CONSTANTLY EVOLVE YOUR APPROACH

Smolik recommends a multi-layered hybrid cloud approach. It takes multiple security tools and strategies to stay one step ahead of cyber criminals. Implement safeguards both on-premise and in the cloud to ensure all bases are covered. Every single endpoint must be covered: low-tech endpoints such as ATMs, as well as servers, network switches, routers, laptops, desktops, tablets, mobile devices and even sensors.

“It is best to assume that the bad guys are already inside,” said Smolik. “Question everything and constantly evolve your approach. The enemy is always inventing new ways to infiltrate your defenses.”

At the same time, simplify security management. Kaspersky advocates a system that uses the same dashboard for all services, applications, and endpoints. “Management from a single point is essential,” said Smolik. “Take a holistic approach to the cloud that bakes in enough security and best practices.”

Will crowdsourced intelligence be the answer to beating cybercriminals? Smolik answers confidently, “Without using buzzworthy terms I truly believe that we can- as a global organization.”



# THE 6 BUILDING BLOCKS OF A CLOUD SECURITY PROGRAM

**B**attling relentless nation-state hackers takes security expertise. Unfortunately, demand for expertise constantly increases, without enough experts to keep up with its growth. That's why Jonathan Nguyen-Duy, Fortinet Vice President of Strategic Programs, says organizations must seriously consider outsourcing cloud services as part of their security program. When outsourcing, select established cloud services that can prove they have certified people, processes, and facilities using best-in-class technology.

We spoke with Mr. Nguyen-Duy about the specifics of building a cloud security program. He had a lot to say.

...continue next page



## ► STEP 1: UNDERSTAND YOUR RISK PROFILE

“Organizations expect CIOs to support digital transformation goals that enhance business processes and create new business models, revenue streams, and customer engagement channels,” says Nguyen-Duy. “The cloud is the fastest, most effective way to meet those goals today.”

Understand your risk profile and security goals before you move to virtualized solutions. Consider cloud service providers that execute security controls and governance objectives equivalent to an in-house private cloud.

## ► STEP 2: DIVIDE AND CONQUER

Segmentation is the second essential element of cloud security. Divide the ecosystem into trusted networks of approved, certified devices and untrusted networks, such as the home or the Internet of Things (IoT) edge. “Along with segmentation comes visibility, so you can understand what’s happening across all networks and allow trusted networks to communicate with the rest of the ecosystem while preventing untrusted networks from doing so.”

Many companies now virtualize and distribute their data. “Instead of putting all their information into a single network, they spread it over multiple clouds and networks, with automated visibility and detection across all of them.” Segmentation makes it almost impossible to compromise an entire ecosystem. “You can also distribute the control nodes so there’s no way a Distributed Denial of Service attack (DDOS) or malware will bring down the entire enterprise.”

Visibility also allows more opportunity to respond, so if malware detonates on one network, you can firewall off that segment and limit the damage.

## ► STEP 3: SIMPLIFY, SIMPLIFY, SIMPLIFY

“Complexity is the enemy of security,” says Nguyen-Duy. Fortinet solutions slash security complexity with an open framework of Application Program Interfaces (APIs) and pre-integration with best-in-class third-party technologies and cloud service providers. “Fortinet partners with Amazon Web Services and Microsoft Azure so the same security capabilities on-premises are available throughout the hybrid cloud.” This

enables seamless movement across the private and public cloud with the same visibility, automation, and response capabilities.

## ► STEP 4: DODGE MOM-AND-POP CLOUD PROVIDERS

“Public organizations should demonstrate a reasonable level of due care,” says Nguyen-Duy. Select service providers that use best practices and controls such as those in the National Institute of Standards and Technology Cybersecurity Framework, ISO/IEC 27000 series, Center for Internet Security Controls and other industry standards. Employ certified security professionals and contract with a reputable auditing firm that attests to the adoption and implementation of these controls and best practices.

“When moving to the cloud, determine your risk profile, security, and compliance goals; the business outcomes you’re looking to achieve. Then choose cloud service providers certified and able to execute those goals across the environment,” says Nguyen-Duy. Offshore locations and government standards add other layers of complexity. Cloud providers should be able to produce reports to show their proficiency in handling these unique, complex regulated environments.

## ► STEP 5: OUTSOURCE SECURITY WHERE POSSIBLE

Fortinet offers a service called the [Cyber Threat Assessment Program](#), which analyzes an enterprise’s network traffic to generate reports on network performance, security, and privacy control effectiveness. These findings provide IT professionals with an in-depth evaluation of their current state security posture to determine the steps needed to get to the desired state. Base your decision of whether to outsource cloud security on your understanding of the organization’s goals and risk.

“In-house solutions are daunting. There aren’t enough people in the job market with top-notch cyber security skills and even fewer with skills plus more than ten or fifteen years of experience,” says Nguyen-Duy. “That’s why organizations should consider outsourcing security functions to service providers with the expertise they can’t afford to recruit themselves.”

## ► STEP 6: ASSUME YOUR NETWORK IS INSECURE

Nguyen-Duy has witnessed multiple environments

believed to be closed to the public internet only to find connected devices communicating with bad actors around the world. “We could actually see data exfiltration in action,” he says. “I’ve also seen organizations that never measured the volume of north-south traffic in and out of the data center and east-west traffic among virtual machines. Others failed to question a cloud provider about how it maintains segregation and segmentation across virtual machines and clients. Who owns the data when you terminate your cloud contract? Many organizations don’t know.”

No device, system or network is 100% secure against determined, advanced threat actors. Top-tier threat actors can break into any network.

Across dozens of industry reports and studies, cyber defenders do not keep pace with the velocity, variety, and complexity of threats. The traditional enterprise perimeter is effectively gone – physically, as we move toward private and hybrid cloud solutions and logically, as more holes open to support external communications. With the traditional perimeter gone, why continue to focus on perimeter-based security strategies as defense?

## ► WHAT TO DO NEXT

Viable, effective security strategies include the cloud. “Companies understand that sophisticated nation-state actors, such as China and Russia, can break into any enterprise network,” says Nguyen-Duy. “Instead of putting all their information into a single network, they spread it over multiple clouds and networks, with automated visibility and detection across all of them.” These strategies make it almost impossible to compromise an entire ecosystem.

Distribution raises the opportunity cost for the hacker because a zero-day exploit has diminishing practical value after the first victim. Used together, network distribution, segmentation, and virtualization reduce your risks.

“Understand that the goal is risk management,” says Nguyen-Duy. “You can manage risk with best-in-class service providers, products, and practices. In the long term, that’s much more cost effective than hiring expensive people who are often not even available.

[View a sample report from Fortinet’s Cyber Threat Assessment Program](#)

# 1400 SENIOR IT PROFESSIONALS WEIGH IN ON CLOUD SECURITY





**In** September 2016, McAfee completed a survey of over 1400 senior technical professionals. The results offer a detailed understanding of the state of cloud adoption and security.

We interviewed Magi Diego, Global Editorial Director for the Content Editorial Team at McAfee -who lead the study- to get her perspective on what these results mean. The result was a colorful peek into the world of 1400 senior technical professionals from all over the world: why they trust public clouds over their own networks, the explosion of hybrid infrastructures, what it means to employ a cloud-first strategy and one the thing they struggle with most.

### ► IT LEADERS ARE PUTTING THEIR TRUST IN THE CLOUD

Last year, the sentiment around trust in public clouds reached a tipping point. “A year ago, only about fifty-percent of executives trusted the cloud. Now, five people trust their data to the cloud to every one person who won’t,” said Diego. In 2016, the number of IT leaders who completely distrust public clouds dropped to just four percent, while the number of leaders who have some, or all of their trust in public clouds grew by roughly eleven points (see fig. 1).

In fact, Almost eighty-five percent of professionals surveyed report they trust some or all of their sensitive data in the public cloud. But, this doesn’t mean that organizations are willing to send their valuable data to any cloud service. The survey data revealed that the average number of cloud providers per business dropped from 43 to 29 in the past year.

According to Diego, this indicates consolidation among providers as well as more care being taken by Chief Information Security Officers (CISOs) in selecting cloud services that offer the right safeguards and the lowest risk.

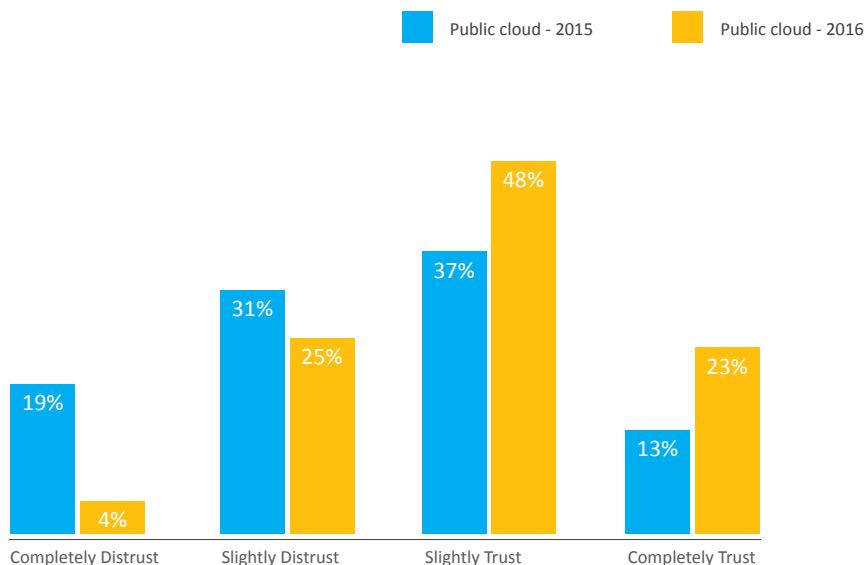
### ► THE USE OF HYBRID CLOUD SERVICES SPIKED DRAMATICALLY IN 2016

More than 80% of the organizations surveyed stated that they are now following a cloud-first strategy. This means giving priority to applications purchased as-a-service or deployed in the cloud vs. applications that require hardware, physical services and systems to be in the data center. This preference has resulted in a spike in the use of hybrid cloud architectures last year:

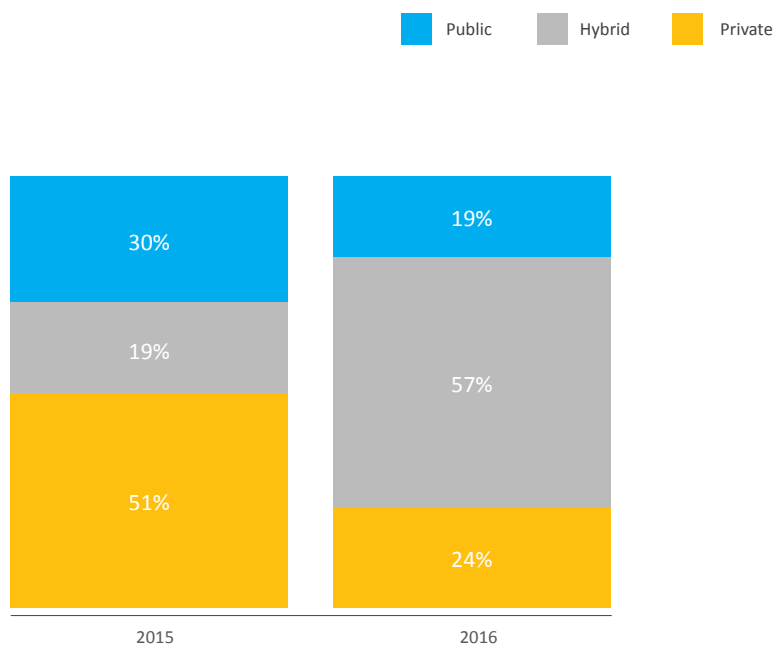
According to **figure 2**, hybrid cloud usage grew by 38% in 2016, showing that more and more organizations moved their IT operations (and spend) to cloud service providers. This spike in demand undoubtedly created challenges for cloud service providers, who had to host and secure increasingly complex volumes of data in an intensely competitive marketplace.

### ► ORGANIZATIONS ARE STILL WORKING OUT ISSUES WITH CLOUD SERVICE PROVIDERS

According to the study, top-tier providers like Amazon, Microsoft, Google, and Salesforce improved their security posture and expanded security resources - increasing the distance between them and smaller service providers. At



**Fig 1.** To what extent do you trust the following to keep your organizations’ sensitive data secure?  
Graph from Building Trust in a Cloudy Sky. Intel Security. September 2016. Web. 6 Jun. 2017. 13.



**Fig 2.** Which type of cloud architecture is your organization currently using? (grouped by user)  
Graph from Building Trust in a Cloudy Sky. Intel Security. September 2016. Web. 6 Jun. 2017. 6.

The cloud has no borders. Neither should your security.

**Together is power.**

With security and compliance more important than ever, see how IT security professionals around the world plan to secure their clouds.

[Learn more](#)



© 2017 McAfee LLC

the same time, the survey revealed that IT professionals still face the following issues with their cloud providers (**see fig. 3**).

Interestingly, the top issue has moved from 'difficulty migrating services or data' to 'high cost/poor value,' while concerns over data loss issues have cooled off. Does that mean companies are offloading the risk to their cloud providers?

"The risk is still yours for any data breach, so you must take responsibility and correctly manage risk," said Diego. "This entails a different set of skills for IT." By this, Diego is referring to the respondents who move forward with cloud initiatives despite the fact that they lack the appropriate cybersecurity skills (**see fig. 4**).

While the skills shortage is still a major challenge for most, the largest organizations were the least likely to have a shortage and in turn, were the least likely to slow cloud adoption plans.

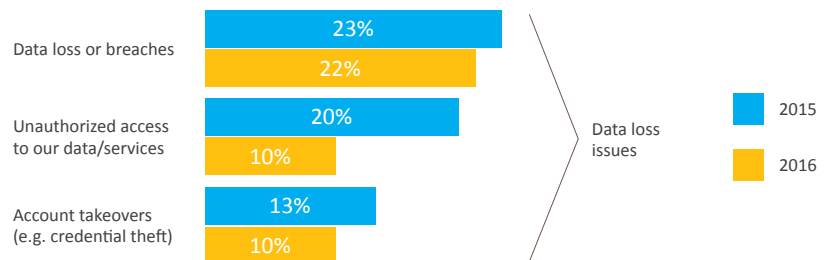
#### ► THE MOST SUCCESSFUL ORGS EMPLOY A CLOUD-FIRST STRATEGY

"Cloud first has to permeate the culture," said Diego. Cloud first means that organizations begin any IT initiative by first seeking out a viable cloud alternative to software or hardware they might typically deploy in a data center. They should only implement the solution on an internal server if nothing suitable is available in the cloud.

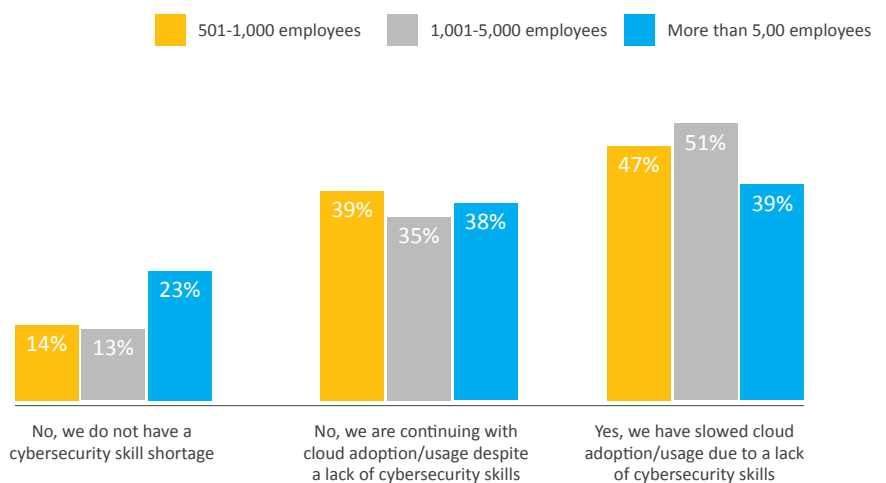
According to the study, participating CIOs and other C-level executives were more likely to be

following a cloud-first strategy, and expected their budgets to be 80% cloud-based within the next twelve months. These senior executives

were also aware of the security skills shortage, and the affect it was having on their cloud adoption rate. To help alleviate the workforce chal-



**Fig 3.** Has your organization experienced any of the following issues with cloud service providers? Graph from Building Trust in a Cloudy Sky. Intel Security. September 2016. Web. 6 Jun. 2017. 17.



**Fig 4.** Is a shortage of cybersecurity skills affecting your organization's usage of cloud computing? (grouped by organization size) Graph from Building Trust in a Cloudy Sky. Intel Security. September 2016. Web. 6 Jun. 2017. 12.



allenges, they were more likely to be operating an integrated or unified security solution. The good news is that organizations are dealing better with risk and executives now place more trust in the cloud than they ever have.

#### ► THAT ONE THING THAT WON'T GO AWAY: HOLES AND HACKERS

The study revealed one important recommendation: existing cloud security and data protection tools are not being used enough. Data Loss Prevention (DLP), encryption and cloud access security brokers remain underutilized. Harnessing such tools more effectively could go a long way toward shoring up existing security holes. "You should know before you put the data in the cloud exactly where you stand," said Diego. "Everything should be thrashed out thoroughly in advance."

The study discovered that as many as 40% of cloud services fall into the Shadow IT category. These are cloud services deployed by individuals

or departments without the knowledge or consent of IT. 65% of IT professionals view this as a major barrier to keeping the cloud safe and secure.

#### ► DIEGO URGES IT TO THINK DIFFERENTLY ABOUT CLOUD SECURITY

Maybe in the past, IT could get away with developing a new application and adding security features later. Those days are gone. IT infrastructure may be better described as an 'IT ecosystem' since it is no longer static, and evolves constantly. With that in mind, security should no longer be added after a major technology initiative.

"Security must be developed into cloud applications from the beginning," Diego says. "Understand the shared security model for each cloud service you use. Find all the data you have on any cloud service, network or endpoint and secure it. You must achieve complete visibility of all your data."

The study echoes Diego's sentiments in its final recommendation: The pressures of speed, efficiency and cost are pushing more applications and data outside the 'trusted network' and into a service provider's clouds, where those benefits can be realized.

As enterprises cloud-enable their operations, gaps in control, visibility, identity, and security are the most likely paths to data breaches. Integrated or unified security solutions are a strong defense against these threats, giving security operations visibility across cloud in-use services and which data sets are permitted to traverse them.

[Read the full-length study](#)

*"I believe our security story is that we are here to help the customer better understand their environment, their current security posture and identify gaps and weak areas. Then, consolidate where appropriate and work to simplify their environment and save them money - All while selecting from our wide partner offerings and services."*

**-Mike Coit,**  
Technical Solutions Architect for Security at Softchoice

►► [Learn More](#)



Because you already have enough to worry about...

**IMPROVE SECURITY.  
SIMPLIFY MANAGEMENT.  
REDUCE COSTS.**

Learn more about the Security Consolidation Assessment

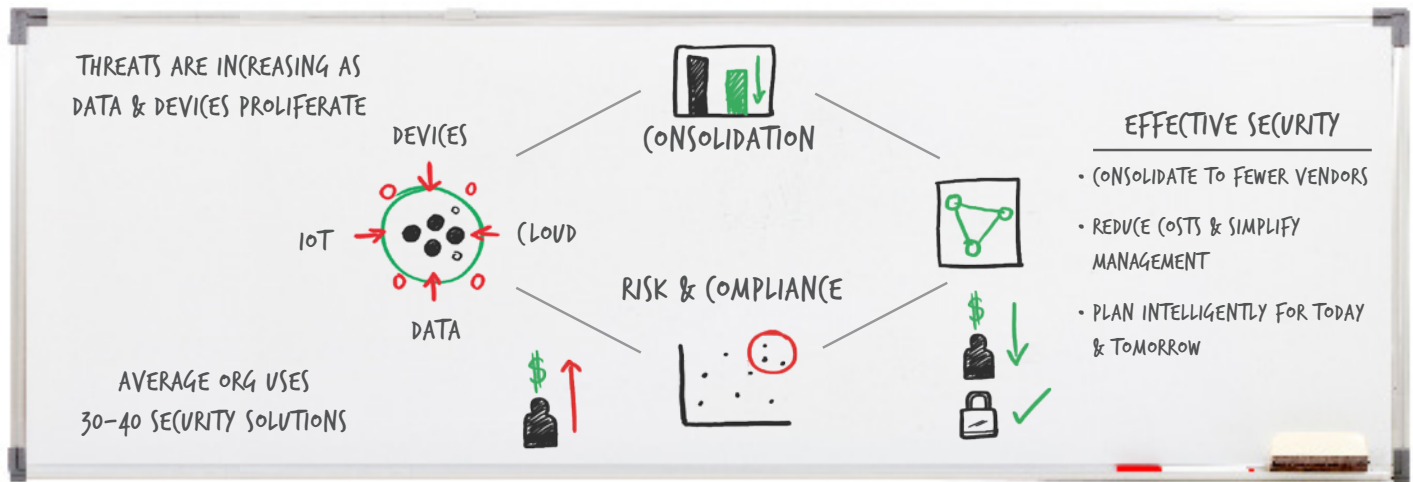
►► [Learn More](#)



Improve Security. Simplify Management. Reduce Costs.

## Security Consolidation Assessment

softchoice



### Business Challenge

To address the latest threats, you continue to invest in new security solutions to protect your data. Yet adding more and more security vendors ends up costing your business money while not necessarily making you more secure.

Many organizations have 30 to 40 independent security vendors operating in their environment. And with internal resources stretched thin, finding the time and expertise to take inventory and develop a more cohesive strategy is simply beyond reach.



### How This Affects You

- **Increased Costs** – spreading security investments across vendors minimizes your ability to leverage volume discounts and likely means you are paying for redundant features.
- **Increased Complexity** – having too many security vendors increases the time and effort required to manage these systems effectively, increasing strain on personnel.
- **Increased Risk** – a patchwork approach means leveraging solutions that aren't designed to work together holistically, creating potential gaps in coverage.



### Customer Success Story

A Canadian-based life insurance company had eight unique security vendors in their environment. Costs were creeping up and internal IT staff were struggling to leverage the different management consoles.

Softchoice recommended the Security Consolidation Assessment to reduce the overall number of security vendors by standardizing on vendors that represented the largest portion of their overall security investment.

#### Softchoice's Consolidation Assessment resulted in:

- Simplifying management by reducing the number of security management consoles from 12 to 2
- Improving security by leveraging vendors designed to work effectively together
- Realizing savings of 45% compared to their previous year's security budget

### According to PWC, in 2015:

**24%** - amount security **budgets** increased  
**38%** - amount security **incidents** increased

- PWC 2016 Global State of Information Security Survey

### Did You Know?

It takes an average of 243 days before an exposure is detected? This is often due to the lack of communication between different security solutions.

softchoice

# YOU CAN SECURE IT ALL

## END-TO-END ADAPTIVE SECURITY THROUGHOUT YOUR NETWORK

The Fortinet Security Fabric delivers better protection with top-rated security devices that share the latest threat intelligence to continually strengthen protection. Our custom-built security processors are built for speed to prevent network slowdowns, and management is simplified through one OS and centralized administration.

**Fortinet is the only company that can truly deliver intelligent protection across the entire network and throughout the entire attack cycle.**

## Security Without Compromise

**FORTINET®**

Learn more at [www.fortinet.com](http://www.fortinet.com)



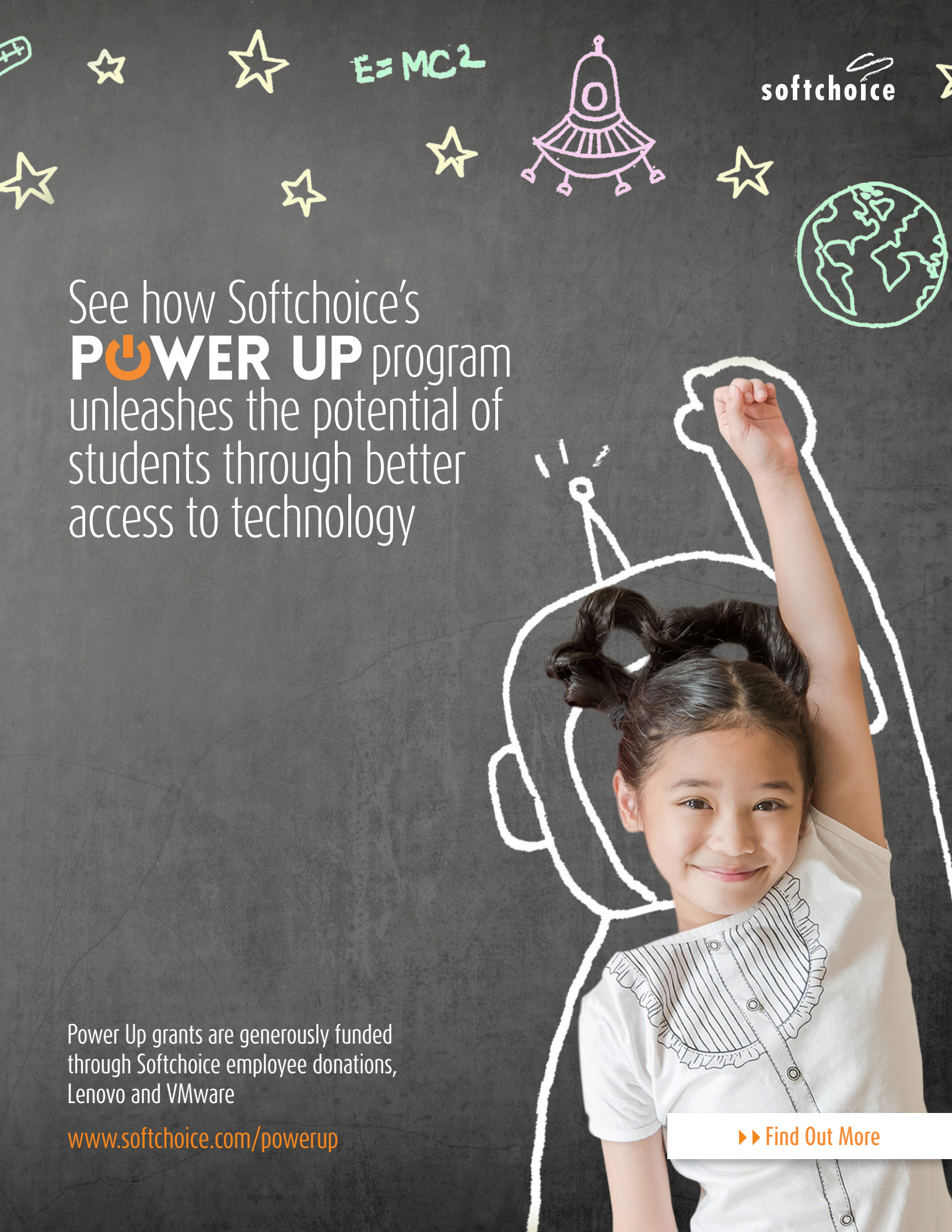
**HOW SECURE ARE YOUR  
DAY TO DAY OPERATIONS?**

**AT RISK, OKAY, STRONG**



**TAKE A SELF ASSESSMENT**





softchoice

See how Softchoice's  
**POWER UP** program  
unleashes the potential of  
students through better  
access to technology

Power Up grants are generously funded  
through Softchoice employee donations,  
Lenovo and VMware

[www.softchoice.com/powerup](http://www.softchoice.com/powerup)

►► Find Out More