softchoice

ISSUE #6 SPRING 2018

THE ULTIMATE SECURITY GUIDE

MICROMANAGE WORKLOADS WITH A SECURITY FABRIC

CLOUD SECURITY ACROSS THE FIVE STAGES OF CLOUD ADOPTION

GOING HOLISTIC: A CONVERSATION WITH OUR SECURITY EXPERTS

PASSWORDS: THE NUMBER ONE CAUSE OF DATA BREACHES

USG

ULTIMATE SECURITY GUIDE

PLATINUM SPONSOR

softchoice

GOLD SPONSORS

TREND MICRO

gemalto security to be free

KASPERSKY lab

SILVER SPONSOR

FireEye

SentinelOne

Check Point SOFTWARE TECHNOLOGIES LTD.

SPRING 2018
ISSUE 6

COMPLETE LIST.
WHAT'S IN THIS ISSUE

CONTRIBUTORS

Albert Kramer
Technical Director at Trend Micro

David Balcar
Security Evangelist at Kaspersky

Stephane Vinsot
Senior Director of Product Strategy
& IAM Platforms at Gemalto

Mike Stines
Security Solutions Architect at Softchoice

Mike Coit
Security Solutions Architect at Softchoice

ADVERTISING INQUIRIES

GEORGE MYRTOS
Category Lead
Enterprise Software and Security
George.Myrtos@softchoice.com

ULTIMATE SECURITY GUIDE

SPRING 2018 - ISSUE 6

PLATINUM SPONSOR
Softchoice

GOLD SPONSORS
Trend Micro
Gemalto
Kaspersky

George Myrtos
Category Lead, Business Development
Softchoice Enterprise Software & Security

Dear Reader,

It's amazing how fast the security landscape has changed. Five or ten years ago, security was just like putting up a digital fence, just like physical security. You had a bunch of blinking boxes in a room and you had to enclose them. How easy that was!

What we've got now, with the cloud and IoT, would've been unimaginable. Essentially, we're all each using somebody else's computers. Our devices are globally dispersed. The perimeter isn't the same. It's this almost liquid-like thing that makes fence metaphors nonsensical.

Okay, but let's get concrete. How does this affect us? The picture isn't totally rosy. Security spending is up 24% on average, while security incidents are up 38%. And when it comes to security technology, the average firm deals with 40 different vendors. That should be a typo, but it isn't! When things go up in flames, it's hard to even know who to call. Obviously, a rethink is required.

That's why the theme of this year's guide is "The IT Security Ecosystem." Because we've all got to learn how to think differently about this new landscape. That means consolidating different systems, rather than expanding in all different directions, tacking on new vendors and band-aid solutions willy-nilly.

Included are articles that come at this from all perspectives. We'll discuss common customer complaints, how to deal with the talent gap, what truly integrated cloud security looks like, and how you can make sure you're the only one using your apps.

Security is still possible, and it can even be easy. But it can't be done by putting out a million small fires. It's a question of looking at larger strategic goals, from this very moment.

So, read on. Soon, this won't seem quite so complicated.

George Myrtos
Category Lead, Business Development
Softchoice Enterprise Software & Security

MEET OUR DEDICATED SECURITY TEAM

GEORGE MYRTOS
Category Lead,
Enterprise Software and Security

MIKE COIT
PreSales Security Architect

MIKE STINES
PreSales Security Architect

JEREMY BANDLEY
PreSales Technical Architect

ANDREW CAMPBELL
PreSales Technical Architect

NABIL KHANDAKER
Vendor Sales Specialist

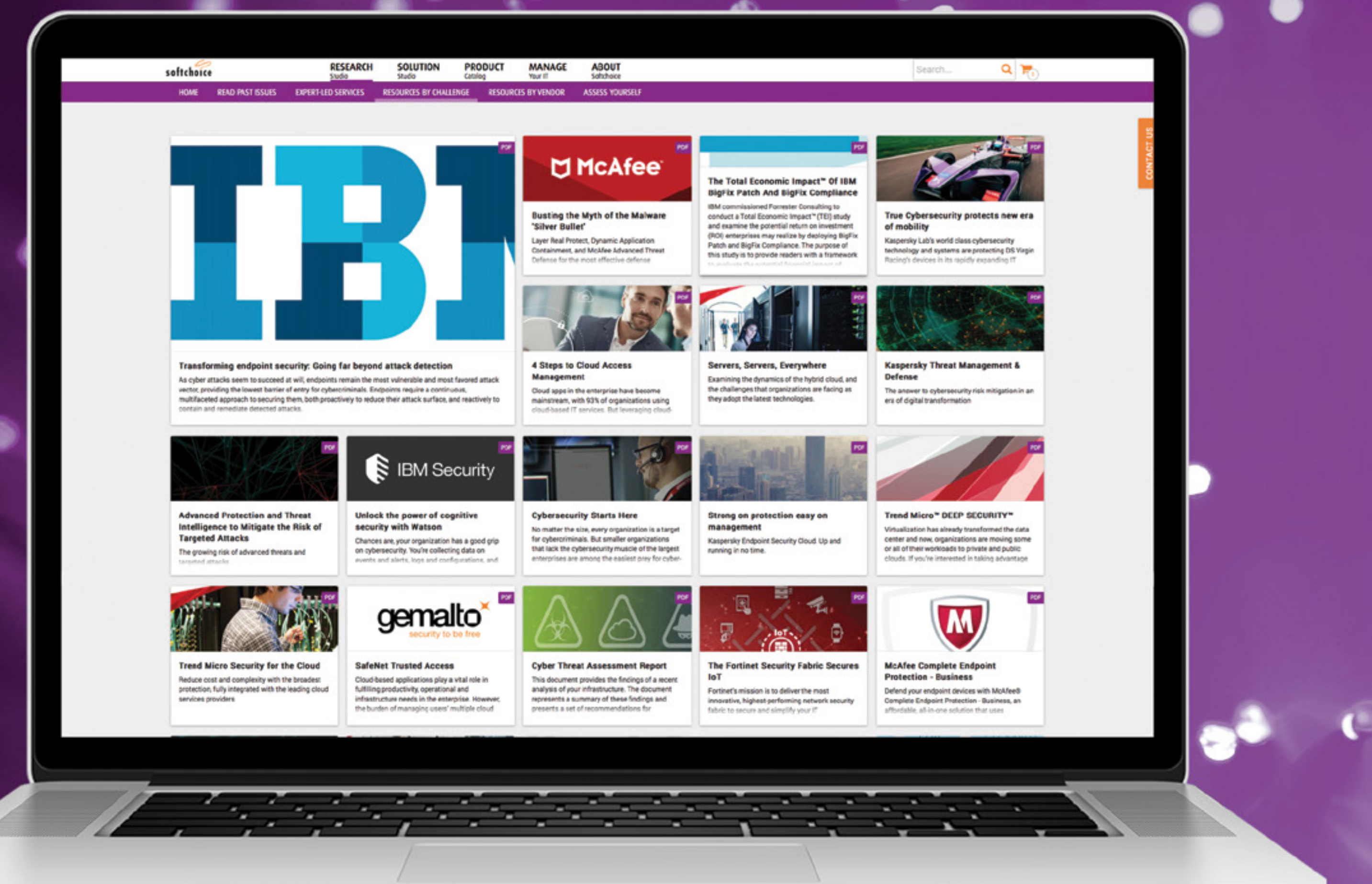
ALEXANDRA LEE
PreSales Technical Architect

ANDREA KNOBLAUCH
PreSales Technical Architect

THE ULTIMATE HUB FOR SECURITY

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

▶▶ www.softchoice.com/security-hub ◀◀



Transforming endpoint security: Going far beyond attack detection
As cyber attacks seem to succeed at will, endpoints remain the most vulnerable and most favored attack vector, providing the lowest barrier of entry for cybercriminals. Endpoints require a continuous, multifaceted approach to securing them, both proactively to reduce their attack surface, and reactively to contain and remediate detected attacks.

Busting the Myth of the Malware 'Silver Bullet'
Layer Real Protect, Dynamic Application Containment, and McAfee Advanced Threat Defense for the most effective defense

The Total Economic Impact™ Of IBM BigFix Patch And BigFix Compliance
IBM commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying BigFix Patch and BigFix Compliance. The purpose of this study is to provide readers with a framework

True Cybersecurity protects new era of mobility
Kaspersky Lab's world class cybersecurity technology and systems are protecting DS Virgin Racing's devices in its rapidly expanding IT

4 Steps to Cloud Access Management
Cloud apps in the enterprise have become mainstream, with 93% of organizations using cloud-based IT services. But leveraging cloud-

Servers, Servers, Everywhere
Examining the dynamics of the hybrid cloud, and the challenges that organizations are facing as they adopt the latest technologies.

Kaspersky Threat Management & Defense
The answer to cybersecurity risk mitigation in an era of digital transformation

Advanced Protection and Threat Intelligence to Mitigate the Risk of Targeted Attacks
The growing risk of advanced threats and targeted attacks

Unlock the power of cognitive security with Watson
Chances are, your organization has a good grip on cybersecurity. You're collecting data on events and alerts, logs and configurations, and

Cybersecurity Starts Here
No matter the size, every organization is a target for cybercriminals. But smaller organizations that lack the cybersecurity muscle of the largest enterprises are among the easiest prey for cyber-

Strong on protection easy on management
Kaspersky Endpoint Security Cloud. Up and running in no time.

Trend Micro™ DEEP SECURITY™
Virtualization has already transformed the data center and now, organizations are moving some or all of their workloads to private and public clouds. If you're interested in taking advantage

Trend Micro Security for the Cloud
Reduce cost and complexity with the broadest protection, fully integrated with the leading cloud services providers

SafeNet Trusted Access
Cloud-based applications play a vital role in fulfilling productivity, operational and infrastructure needs in the enterprise. However, the burden of managing users' multiple cloud

Cyber Threat Assessment Report
This document provides the findings of a recent analysis of your infrastructure. The document represents a summary of these findings and presents a set of recommendations for

The Fortinet Security Fabric Secures IoT
Fortinet's mission is to deliver the most innovative, highest-performing network security fabric to secure and simplify your IT

McAfee Complete Endpoint Protection - Business
Defend your endpoint devices with McAfee® Complete Endpoint Protection - Business, an affordable, all-in-one solution that uses

MICROMANAGE WORKLOADS

WITH A SECURITY FABRIC

THE THREAT LANDSCAPE HAS SHIFTED MARKEDLY. CYBERCRIMINALS NOW LAUNCH SOPHISTICATED, HIGHLY CUSTOMIZED ATTACKS AGAINST HIGH-VALUE TARGETS. ALBERT KRAMER, CYBER SECURITY SPECIALIST AT TREND MICRO INDICATES THESE ATTACKS HAPPEN AT GREAT FREQUENCY AND THE RESULTS CAN BE ECONOMICALLY DEVASTATING.

Traditional security measures are no longer enough. Mounting a perimeter-based defensive strategy will fail and only an integrated approach to security provides enough visibility and control to protect modern workloads.

What smart firms need is a real security fabric. A security fabric is a converged system, weaving together multiple solutions into an agile and flexible whole. When properly established, a security fabric approach allows for the ability to mesh devices and software over a multi-cloud network, while still permitting central automation and monitoring.

▶ FINANCIAL FRAUD IS RAMPANT. KRAMER GAVE THE EXAMPLE OF THE CEO AT A FINANCIAL SERVICES COMPANY:

The criminal organization behind this breach used malware to bury deep into the organization. It gained a deep understanding of company products and processes. It studied past deals. The infiltration lasted many months and the incursion took place invisibly. The hacker devised a strategy to masquerade as an executive from a potential client when he approached the CEO, expressing interest in completing a large deal.

Result: The cybercriminals convinced the CEO about the legitimacy of the transaction and persuaded him to transfer a large sum of money into an account. Instead of securing a lucrative contract, the money disappeared beyond the reach of the authorities.

> ***"This new wave of highly customized attacks is extremely difficult to address," said Kramer. "Some even use crafted domains that are indistinguishable from the original domain."***

A signature-based security (the detection of attacks by looking for specific patterns used by malware) approach no longer works. And this is just one example of the insufficiency of piecemeal security. Combined security fabric systems aren't just cool new technology—they're practically a necessity. ▶▶▶

▶ PART OF THE REASON THESE ATTACKS SUCCEED LIES IN THE SHIFTING ARCHITECTURE OF IT.

It is no longer workable to set up firewalls, IPs and other point tools to secure the perimeter. Organizations typically have multiple internal data centers and support multiple cloud providers. A series of geographically dispersed entities serve thousands of workloads while mobile devices and virtualization technology add further complexity. Combine that with the emergence of IoT, and one can see how traditional IT approaches to security have massive holes.

Data moves so quickly that it is difficult to track. It shifts from inside the enterprise to the cloud and back again. Traditional firewalls and signature-based security can't cope with data and workloads in constant motion.

Unfortunately, modern software development practices add to the problem. The typical application development project is carried out in a rush. Security can be little more than an afterthought and it's up to security personnel to figure out how to shore up the defenses—after the fact. It can be difficult to detect all possible avenues of incursion. That's where the elegance of a security fabric comes in: it gives firms the power to extend a comprehensive solution across new business apps. And new business apps are a constant in today's environment.

▶ SECURITY SHOULD NEVER BE AN ADD-ON. IT MUST BE MADE AN INTEGRAL PART OF THE DESIGN PROCESS.

It must follow workloads—wherever they reside and wherever they go. Security processes and procedures must be able to operate inside or outside the data center, in public and private clouds.

However, the challenge is even greater due to the volume of workloads that now exist—far more than at any time in the past. There is simply too much going on in organizations to maintain a manual approach to security. It requires automated security technology to micromanage so many different workloads.

SECURITY PERSONNEL MUST ADOPT AUTOMATED SYSTEMS THAT DO THREE THINGS:

- Detect incursion attempts
- Perform analytics to isolate harmful or anomalous patterns in workloads
- Take action at light speed to block potential threats

But cybersecurity also involves a balance between stringent security and business agility. If personnel are tasked with overly complex and time-intensive security processes, they will attempt to bypass them. IT, then, should have in place sufficient visibility and controls to a) detect and prevent violations and b) provide a workable security framework that does not inhibit productivity.

True workload security can only be achieved within a unified framework. A patchwork of point tools leaves too many gaps. They make it easy for the cybercriminal. Those gaps have to be stitched together.

▶ A FULLY INTEGRATED AND AUTOMATED SUITE IS REQUIRED THAT CAN MANAGE ALL WORKLOADS, NETWORKS, AND STORAGE.

This is being achieved via a fabric security framework. Such a woven framework decouples the handling software from the underlying hardware, so they're woven together in an interdependent, dynamic configuration. Result: Complete visibility, control, and automation are achieved. This is far more effective than having a single pane of glass. It's an approach that speeds business processes, and allows new workloads to be added confidently without exposing the organization to attack.

One Trend Micro client operated twenty-one datacenters spread globally. It decided to consolidate using the cloud. Trend Micro's automated, software-defined security fabric approach helped the organization realize its vision. Three cloud-based virtual datacenters spread across multiple service providers are managed as one security entity. This architecture facilitated the requirements for the various lines of business. Workloads are added effortlessly. The company enjoys enhanced security—and peace of mind.

74% OF DATA BREACHES ARE CAUSED BY ONE BASIC PRACTICE:

PASSWORDS * * *

BUSINESSES FACE MOUNTING PRESSURES TO SECURE THEIR ENVIRONMENT AS IT MIGRATES TO THE CLOUD. AS EINSTEIN ONCE SAID, "THE DEFINITION OF INSANITY IS DOING THE SAME THING OVER AND OVER AGAIN, BUT EXPECTING DIFFERENT RESULTS" SO WHY DO WE KEEP RELYING ON PASSWORD-BASED SECURITY WHEN IT'S THE CAUSE OF SO MANY DATA BREACHES?

Just ask Stephane Vinsot, Gemalto's Senior Director of Product Strategy & IAM Platforms. He'll tell you it's about time we stopped the lunacy by adopting more comprehensive, user-friendly security practices. This failure to adapt is two-fold, he explained.

ON ONE HAND, ORGANIZATIONS ASSUME PASSWORD PROTECTION ALONE WILL KEEP CLOUD APPLICATIONS SAFE.

"Unfortunately, when it comes to securing cloud applications, organizations are not doing enough," he said. "All too often they are relying on passwords to protect cloud applications."

Slapping on new password requirements for every new cloud application is unruly and dangerous. In fact, according to Gemalto's Breach Level Index Report, compromised identity and stolen passwords were to blame for 74 percent of data breaches in the first half of 2017.

A single stolen password can be devastating, says Vinsot. Bad actors just need to compromise one account. After that, they can then move laterally across the network to cause mayhem.

The second sacred cow Vinsot calls out is perimeter security. In our cloud-bound world, users need continual, global access to their applications. Putting everything behind a firewall no longer makes sense.

> ***"The perimeter does not exist anymore," he says. "Imagine telling your Salesforce.com users they can only access the app from their desk, in their cubicle, behind your firewall. It doesn't work that way."***

WE HAVE REACHED THE CLOUD-APPLICATION ERA.

So, what can enterprises do to keep cloud applications safe and secure?

Gemalto has built a brand around telling organizations to leave behind the notion of "breach prevention." Instead, they say to adopt a mentality of "breach acceptance." The idea is that breaches will always happen. But businesses can stop the bleeding — and prevent most, if not all of the damage — if they combine encryption with advanced access and identity management protocols.

Vinsot likens the task to building a vault at a bank. For a vault to be effective, it needs strong walls, as well as a strong and sophisticated door. If your walls are cardboard, it doesn't matter how complicated the lock is, they're getting in. If your walls are steel-reinforced, but the front door is unlocked, what's the use? A well-designed vault will keep assets safe and secure, no matter where the threat is coming from.

WHEN IT COMES TO CLOUD APPLICATION SECURITY, YOU AREN'T BUILDING ONE BANK VAULT. YOU ARE BUILDING SEVERAL.

Importantly, though, you need global visibility, reporting, and control, from a single dashboard and location. Otherwise, the solution becomes far too complex to handle, and security risks emerge.

"The cloud needs to be managed as an extension of the IT environment. You must have global visibility into what's happening, while at the same time dealing with the specifics of each environment," he said.

Similarly, making things as simple as possible for your end users is essential. For example, Single Sign-On (SSO) can be coupled with Multi-Factor Authentication (MFA) to provide users with a more robust, and easy way to protect identity and data. Forcing users to sign in to each application, every single time, causes frustration.

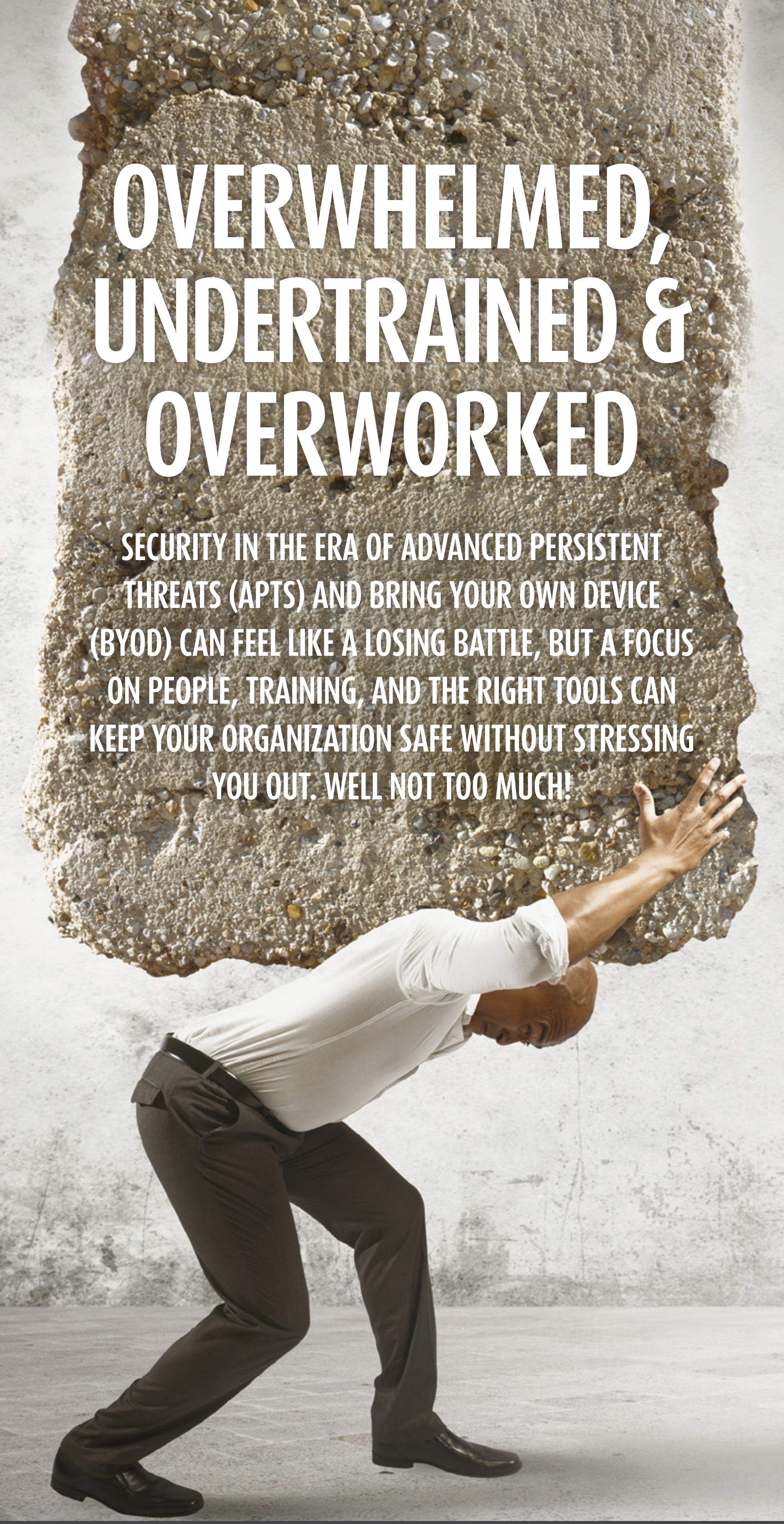
But there is a limit to how user-friendly your cloud application security should be.

VINSOT REMINDS US CONTEXT AND CONTENT ARE BOTH CRITICAL WHEN DESIGNING SECURITY POLICIES.

Perhaps your SSO solution enables unfettered access to the least sensitive applications. But anything involving personal or financial information is locked off behind an extra layer of protection. Similarly, if a user is on your local network, they should have more flexible sign-in requirements than if, say, they are suddenly logging in from a nation-state actor!

With a quick look at Gemalto's Breach Level Index report, the need for a new and comprehensive approach to security is clear. In 2017, only 4.6 percent of breaches reported were "Secure Breaches," meaning the data stolen was encrypted, and thus, worthless. Imagine, instead, the rest of the victims had taken Vinsot's advice and "built a better bank vault." In the first place, their ID and access management strategy might have prevented someone from getting in the front door. But even if they did get inside, there'd be nothing of value for them to take.

Passwords and perimeter-based protocols are dead. Why not try something new? You'd be crazy not to.



OVERWHELMED, UNDERTRAINED & OVERWORKED

SECURITY IN THE ERA OF ADVANCED PERSISTENT THREATS (APTS) AND BRING YOUR OWN DEVICE (BYOD) CAN FEEL LIKE A LOSING BATTLE, BUT A FOCUS ON PEOPLE, TRAINING, AND THE RIGHT TOOLS CAN KEEP YOUR ORGANIZATION SAFE WITHOUT STRESSING YOU OUT. WELL NOT TOO MUCH!

At its 2018 Security Analyst Summit, Kaspersky Lab announced it had discovered an APT called Slingshot. Analysis suggests it collects screenshots, keyboard data, network data, passwords, USB connections, other desktop activity, clipboard and more. "Slingshot managed to stay completely hidden for six years," says David Balcar, Security Evangelist for Kaspersky Lab.

HOW CAN IT SECURITY KEEP UP WITH STEALTHY ADVANCED PERSISTENT THREATS, MIND-NUMBING COMPLEXITY, TIGHT BUDGETS, AND A MASSIVE SECURITY TALENT GAP?

We interviewed David Balcar to get his perspective on where organizations should focus limited resources to get maximum security value.

Today, every environment is complex, according to Balcar. "A mom and pop store may think its IT environment is simple, but it likely does some credit card processing, gets email on multiple devices, or has an outside service managing its point-of-sale systems.

"Every time you add a service or capability—such as BYOD, hyper-convergence or Software as a Service (SaaS)—you add complexity and increase your attack surface and risk of attack exponentially," says Balcar." BYOD could add 10,000 new mobile devices that can get hijacked or infected with malware." It's difficult for a limited IT security staff to find the time and talent to keep up, and it only takes one APT to get through. ▶▶▶

APT'S LOVE COMPLEXITY, ACCORDING TO BALCAR, WHICH MAKES THE JOB OF DEFENDERS THAT MUCH HARDER.

"Many of these nation-state-sponsored hacking groups have hundreds of people writing software that can penetrate the most complex networks multiple ways. Once they get in they have access to very sophisticated tools that can help them stay hidden for a long time."

But while hacking is getting more sophisticated, it's also getting easier. "Anyone can go online and download code that came from an advanced nation-state leak such as Wikileaks Vault 7 and the ShadowBrokers" says Balcar. "WannaCry used at least two exploits from a nation-state leak to attack hundreds of thousands of computers around the world for several weeks.

"There are sites on the Dark Web that build ransomware for you with an interface rivaling production software. Then they'll help you push it out to victims and collect the bitcoins for about $175. Many provide 24-hour support."

UNFORTUNATELY, WHILE APT'S ARE MULTIPLYING, TOP-NOTCH SECURITY TALENT IS IN VERY SHORT SUPPLY, SO BALCAR ADVISES THE 80/20 RULE.

"The trick is to find people who can handle the essential pieces of the security puzzle, put them on a team to bring all that knowledge together, and give them tools they need to fill in any talent gaps and make training easier. Then each player must spend 80 percent of his or her time protecting the company and 20 percent actively learning about all the new threats and tools so they know how to protect the organization against those attacks." Says Balcar.

He adds that leadership is key, "You need leadership that supports security team training and is willing to fund the training/tools you need to help defend against and respond to those threats."

WHEN IT COMES TO SOLUTIONS, COVER AS MUCH GROUND AS YOU CAN WITH A SINGLE PANE OF GLASS.

Look for best-of-breed tools that cover a lot of security ground with a single pane of glass, says Balcar. "Kaspersky offers an all-encompassing security solution called Threat Management and Defense (TMD). It's a combination of technologies and services, including Kaspersky Anti Targeted Attack platform (KATA), that detects and responds to the most sophisticated threats in the environment.

"With every install, TMD has found something new, even when the network was already protected by next-generation firewalls and other advanced security solutions."

TMD includes Kaspersky's cybersecurity services for instant response, penetration testing and training and Kaspersky's impressive threat intelligence. "We have research teams like the Kaspersky GReAT looking for threats and we get that threat intelligence into KATA on a constant basis, along with information on how to protect your network and respond to an attack."

YOU ALSO NEED HELP FROM EMPLOYEES. THE IT TEAM CAN'T BLOCK EVERYTHING.

"From the person at the front door to the CEO, everyone must be on the same page when it comes to security awareness, training and what to do if they suspect a breach or malware."

Help desks are important players. "In most organizations, the help desk is the first group to notice a security issue, but you must train them on what to look for."

Train the rest of the staff as well. "People don't like to tell the security team when they do something wrong because they worry about getting shamed. It has to come from the top that you're all a family and everyone must be involved, take security seriously and report incidents such as stolen phones right away. I know companies that give flowers and Starbucks gift cards to people who report spam."

LEARN TO THRIVE IN AN ENVIRONMENT OF ZERO TRUST.

APT's will only get worse "Cyber criminals now target supply chains, so you can't even trust your hardware." Trust nothing but find ways to build back that trust. "Encrypt all your data at rest and in transit so if it's stolen there's a certain trust level that it won't be decrypted."

CLOUD SECURITY

ACROSS THE FIVE STAGES OF CLOUD ADOPTION

ACCORDING TO RIGHTSCALE'S STATE OF THE CLOUD REPORT, 96% OF ENTERPRISES ARE USING THE CLOUD IN SOME CAPACITY AND 80% OF ENTERPRISES HAVE ADOPTED A MULTI-CLOUD STRATEGY.

When deployed effectively, the public cloud is a powerful and disruptive model. It brings positive operational transformation and greater competitiveness. But poor implementation is equally disruptive. Softchoice has worked on countless cloud initiatives at all stages of adoption with our clients. Through that, we've identified fives stages that allow you to methodically approach your migration.

We've called them stages for a reason. While you progress through the stages, the journey isn't exclusively linear. You may find yourself weaving in and out of stages as you move workloads to the cloud and will likely repeat some of all of these stages as you continue your migration. More importantly, each stage must be underpinned by comprehensive security.

STAGE ONE: GAP ANALYSIS - APPLICATION AND SECURITY DEPENDENCIES

Your journey into the cloud begins with a Gap Analysis of your current IT systems. This will give you a detailed inventory of the applications, or production workloads, in your data centers. This information is crucial for generating a cost estimate and preliminary budget. Conducting a thorough Gap Analysis will also help you understand which applications are in need of an update prior to moving to the cloud. Secure deficient applications before you move. You need to understand the vulnerabilities and dependencies of systems before swapping them to hosted infrastructure. This involves knowing which applications depend on which workloads. It also means taking responsibility for patching, monitoring and fixing your code for on-premise business systems before moving them.

STAGE TWO: GET MOVING - GOVERNING ACCESS TO CLOUD APPLICATIONS

At this stage, you choose one meaningful workload with cross-functional implications to migrate to the cloud. There are two reasons to get moving before a more formal plan is developed. You quickly build real-world experience. And, it helps further develop the use case for the cloud and to get quicker buy-in. Your cross-functional team should be made up of Security, Finance, and Lines of Business. This is when you will build your governance policies, which is all about controlling spend and workload visibility. Ask yourself and cross-functional partner's questions like:

- Who owns this application/workload?
- How do we bill for it?
- How does someone request setting up a new workload?
- How are applications decommissioned?

Make identity and access management a best practice. IT leaders need to embrace the practice of 'least privilege' whereby administration rights are based on the absolute minimum requirements the individual needs to do their job and nothing more. From there, you can broaden access on a role or a situation-based need. You also want to consider multi-factor authentication services, which come ready-to-go with Azure and AWS. This makes it easy for users to quickly engage with your cloud applications while ensuring the right people have access, and no one else.

Combine this with the documented policies on how cloud resources are requested and retired can help avoid costly "compute sprawl" and ensure those who stand up and manage workloads are ultimately accountable for the costs incurred by their work. To succeed in this area, you must define roles and responsibilities. Define who will be responsible for infrastructure procurement, assign authority to turn on cloud services, and determine who will assess your security posture in the cloud. ▸▸▸

STAGE THREE: PLANNING - UNDERSTANDING YOUR CLOUD PROVIDERS SECURITY RESPONSIBILITIES VS. YOUR OWN

Businesses too often treat their cloud projects like the moving of servers or infrastructure between locations. Moving to the cloud is not a simple lift and shift of your applications. Your adoption plan must take into account the technical requirements of all software, the effects operations in the cloud will have on their performance, and how to meet your business SLAs and regulatory requirements. Build your cloud plan based on your applications and their suitability for the cloud. Again, this is where a deep understanding of your applications, and their dependencies, is needed. Start by profiling your applications. Determine which are dependent on each other, which pose the greatest risk, and which are the strongest candidates for the cloud. Pay close attention to risks, complexity, dependencies, operating costs and suitability.

Thorough planning around security is essential to success, even for minor cloud projects. While cloud service providers such as Microsoft and AWS provide some security resources, it's best to treat these as the foundation on which to build your security capabilities. Keep in mind: the cloud does not replace your own responsibilities. Get familiar with the shared responsibilities between you and your service provider. What aspects of security they take off your plate and which they leave varies based on the provider and service type (IasS, PaaS). It cannot be stressed enough how important it is to fully understand your accountabilities.

STAGE FOUR: MIGRATION - SECURITY AUTOMATION

Achieving the agility and time-to-value that you're turning to the cloud for also requires the use of sophisticated scripting and automation tools. Luckily, the cloud offers automation tools that far exceed the ones that exist for on-premise virtualization solutions. You also want to consider how much automation you can leverage to take as much human error out of the equation. For example, you can automatically ensure end-user machines continually align with a configured security policy. You can also apply technical protection to a document contained in a certain folder.

STAGE FIVE: OPTIMIZATION - DISASTER & RECOVERY PLANNING

The work doesn't end when your applications are in the cloud. Once you have successfully moved to the cloud and achieved some degree of operational normalcy, it's now time to go a step further and refine your deployment. In the on-premise world, compelling events for change might happen annually, or more likely, once every three years. In the cloud, there may be a new opportunity to reduce waste, or some technological challenge to address, or even a challenge that's become simplified, in any given week.

Pay attention to encryption and key management. If disaster strikes, you better have a plan. Not only should you have a clear disaster recovery and backup strategy in place, you need to pay close attention to encryption and key management. Assume for a moment that all your data is hosted and encrypted on the cloud. Now imagine your encryption keys are stored in an application in your server room, separated from the systems that depend on them for security purposes. Failure of that on-premise hardware means that your data remains safe and sound - and completely useless - encrypted at rest, with minimal hope of recovery in the cloud.

THE WAY TO FAIL IN THE CLOUD IS TO RUSH HEADLONG INTO IT WITHOUT ADEQUATE ATTENTION TO SECURITY.

Every one of the stages requires a strong security address. Each design should include comprehensive security. Best practices to safeguard the cloud must be at the forefront of all discussions.

CONCLUSION

Cloud native services come with a wealth of enterprise-class security features. But don't make the mistake of relying solely on them. They need to be augmented with third-party, best of breed security solutions; to protect data before it is transmitted to the cloud: to safeguard it while it is in transit; to control the many avenues of access to that data; to detect potential incursions, and to harden applications. Start realizing the full potential of your cloud migration by visiting our IT Leader's Guide to Maximizing Cloud Value and learn, in depth, the 5 stages of cloud adoption.

FRESH APPROACH REQUIRED

Some attempt to move to the cloud by designing their application and security architectures in the traditional way. They fall back on legacy best practices and designs. They may be comfortable with these principles. But they won't work well in the cloud. Those that do it this way waste time and money. Why? The cloud works quite differently from traditional IT.

THAT'S WHY IT'S A GOOD IDEA TO ENGAGE WITH KNOWLEDGEABLE PARTNERS LIKE SOFTCHOICE. OUR CLOUD SPECIALISTS CAN HELP YOU FIGURE OUT:

✓ How to get started in the cloud

✓ How to validate the cloud and gain buy-in.

✓ How to devise the right plan and the right architecture

✓ Which third-party security applications should be used to support the cloud

✓ How to continually optimize your cloud.

FOR MORE INFORMATION, VISIT :

softchoice.com/research-studio/increase-it-agility/cloud-adoption

WANT MORE ARTICLES LIKE THIS?

Explore past issues of the Ultimate Security Guide

www.softchoice.com/security-hub

softchoice
ISSUE #4 SPRING 2017
THE ULTIMATE SECURITY G
THE AGE OF RESPONSE: HOW AI ENABLES NEAR-INSTANT REACTIONS TO DIGITAL THREATS
WHO IS ACCOUNTABLE FOR A HYBRID CLOUD SECURITY BREACH?
HOW HACKERS CHANG WAY WE BUILD AND P NETWORKS AND WHY MUST ADAPT...OR G
softchoice
ISSUE #5 WINTER 2017
THE ULTIMATE SECURITY GUIDE
THE SIMPLE SOLUTION TO ENDPOINT SECURITY IS RIGHT UNDER OUR NOSES
THE NEW ARCHITECTURE
BE AN ATTACK HUNTER NOT GATHERER

GOING HOLISTIC:

A CONVERSATION WITH OUR SECURITY EXPERTS

SOFTCHOICE SECURITY ARCHITECTS MIKE COIT AND MIKE STINES OUTLINE THEIR APPROACH TO MAKING IT PROFESSIONALS' LIVES EASIER. GO BEYOND TACTICAL SOLUTIONS AND EXAMINE THE BIGGER SECURITY PICTURE.

> "I HATE MY ANTIVIRUS ENDPOINT VENDOR. WHO ELSE IS OUT THERE?"

In a typical day, Mike Coit and Mike Stines will have back-to-back conversations that begin like this. As presales security architects with Softchoice, "the Mikes" spend their time helping IT leaders breathe easier around all things security

When the person on the other end kicks things off with such a specific pain point, they're often looking for a tactical solution. But when they want to buy product X to solve problem Y and end the conversation, they're missing the bigger picture.

In the security world, "one problem tends to lead to another," says Coit. The initial complaint is often a symptom of a wider issue.

"We try to discover more about the customer and what they already have in place." The resulting conversation may expose gaps in that IT professional's current environment. Sometimes it reveals they already have what they need in-house.

As vendor-agnostic architects, the Mikes see their role as much more than moving organizations onto licensed products. Instead, it's about helping IT professionals understand the moving parts within their business and how they interact from a security perspective. From there, it's about translating those insights into educated, actionable recommendations.

"In this role," Coit explains, "we tend to have to think wider."

THE VALUE OF HOLISTIC THINKING: IT'S ABOUT REDUCING RISK.

Shifting customers toward a holistic approach to security isn't always easy. How much convincing is necessary? That depends on the company, the vertical and the level of "security maturity" in question.

Some organizations hesitate to embrace a holistic perspective because they don't know they need more than basic protection. Others realize the need for many layers of security, but what stops them is cost.

Implementing something like a security information and event management (SIEM) tool is neither simple nor inexpensive. The prospect is sometimes overwhelming.

When it comes to articulating the need to go beyond a tactical approach, "it's a matter of risk management," says Stines. Every organization must weigh the cost to improve security against the risk of exposing the business.

"We ask ourselves 'have we helped the customer reduce their risk exposure?" When that customer has only fulfilled a tactical need, "the answer is usually 'no.'"

REALISTIC ADVICE TAKES REAL-WORLD EXPERIENCE.

The Mikes agree that the most worthwhile security conversations dig deeper into the story of the business. It helps, then, that both are twenty-plus-year veterans in enterprise IT. That experience operating in actual business environments gives their client discussions real-world context.

"You learn a lot about a business, how it operates, where the pain points are," says Coit. His experience includes everything from desktop and application support with a book publisher to network administration for one of Canada's largest banks.

"It helps me relate to customers from an educated perspective."

Meanwhile, Stines believes his decades of experience in day-to-day data center operations management gives him insight into "what a 'day in the life' is like" for clients. That on-the-ground experience allows him to add better value for customers through realistic recommendations.

When it comes to common customer needs and challenges, "it's not alien to us."

YOU'RE NOW IN CHARGE OF SECURITY. DON'T PANIC.

For anyone who finds themselves at the reins of IT security, the Mikes have a simple message: Don't worry. "Any organization that does this does not need to reinvent the wheel," says Stines.

Their advice for building a security game plan? Start with an existing cybersecurity framework, such as HIPAA or NIST. Look at your current state and measure it against those best practices. Identify and rank the gaps. Build your policies from there.

They also emphasize the message that your cybersecurity plan is not a "one-and-done" evaluation. "IT security is not a 'cookie-cutter' operation," says Stines. "But it is a structured, repeatable method." The problems facing your organization change, as do the needs of the business. Your plan must adapt to changing circumstances.

The Mikes also stress that security is not something you "bolt-on" after-the-fact. Instead, it needs to factor into every stage of the business lifecycle.

"Security isn't meant to be a disabler or a roadblock to innovation," says Coit. "If it does get in the way, there are important reasons for that." As Stines adds, "it comes back down to risk management. What is the cost of not making this change?"

FOR THOSE CONSIDERING A DIY APPROACH TO IMPROVING THEIR SECURITY POSTURE?

Many organizations will take this path. But even in those situations, there are opportunities to validate the approach with an expert. We offer many free assessments that help organizations detect gaps in their security infrastructure and reduce costs through consolidation.

> "IT NEVER HURTS TO GET A SECOND OPINION."

softchoice

SECURITY CONSOLIDATION ASSESSMENT

Simplify your environment. Save money.
Strengthen your security.

KNOW YOUR SECURITY LANDSCAPE

Most organizations are using 30-40 security solutions, greatly increasing cost and complexity, while not necessarily making them more secure. With internal resources stretched thin, finding the time and expertise to take inventory and develop a more cohesive security strategy feels simply beyond reach.

Our free Security Consolidation Assessment will help you identify opportunities to consolidate vendors, improve overall security and plan intelligently for today and tomorrow's threats.

REQUEST A CALL WITH A SOFTCHOICE SECURITY EXPERT TO LEARN MORE ABOUT THE SECURITY CONSOLIDATION ASSESSMENT.

https://www.softchoice.com/research-studio/security/expert-led-services