CYLANCE

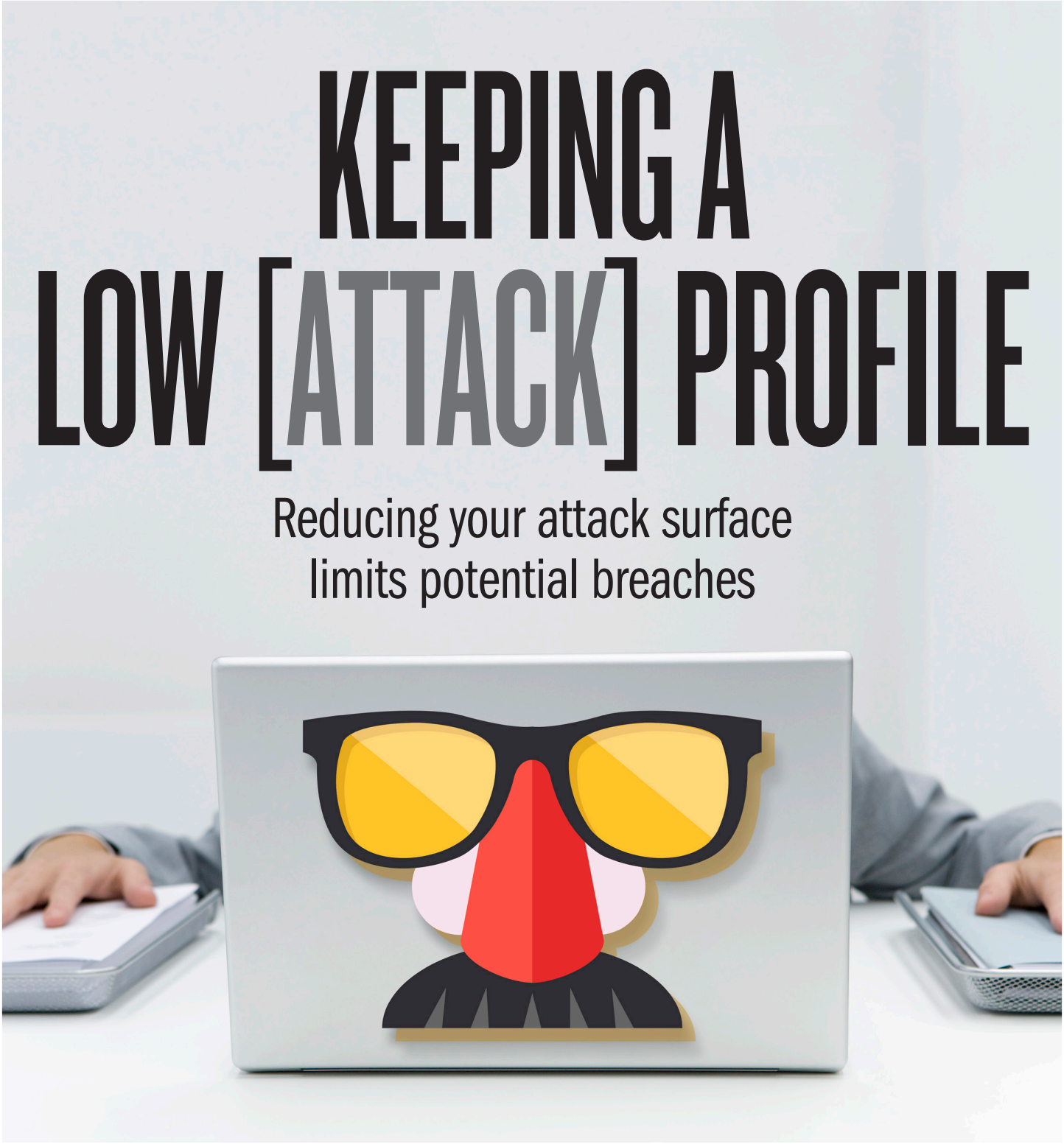
ExpertFocus

Brought to you by Cylance

February 2019

KEEPING A LOW [ATTACK] PROFILE

Reducing your attack surface limits potential breaches



Enhance cybersecurity by reducing your attack surface

CISOs understand that the smaller a company's attack surface, the fewer areas need to be protected. Keeping a low profile lets you make better use of your resources. Esther Shein reports.

One might think that large, high-tech enterprises that are often the targets of cyberattacks would be the most knowledgeable and experienced in cybersecurity. After all, those in technology-driven industries must know more than those in non-tech fields that are less often targeted, right? While one might think that, they would be wrong.

Before David Lagacé arrived at the 50-year-old Montreal-based telecommunications infrastructure provider Telecon in mid-2018, security was done on an ad hoc basis. It was not the primary focus of the company, which was founded in 1967, he says, adding, "If we had time to do security, we would."

With 3,200 mostly mobile users and some 2,500 endpoints and devices to manage across Canada and the U.S., Telecon's attack surface is broad. Because of the company's prior stance, Lagacé, senior manager of IT security for information technology, knows the company has been on borrowed time. "You're only as lucky as your next infection," he notes wryly.

In his first 90 days on the job, Lagacé discovered software patches had not been applied, so once those were done, he made sure systems were put on a regular patching schedule. Telecon also did not have any vulnerability scanning capabilities so that IT could check for any new common vulnerabilities and exposures (CVEs), report them, and get the operations team to mitigate any issues.

Ideally, security teams would patch all known vulnerabilities and update hardware and software on a regular basis, effectively reducing their attack surface to virtually zero. Of course, that is not realistic in today's hyperscale enterprise environment, where new assets are added as demand dictates, making it a challenge for IT to keep up. Many organizations today are also managing hybrid environments, adding to the complexity.

To manage the dynamic attack surface, organizations need to ensure they have the right set of security controls in place to reduce the chance that an attacker can exploit the attack surface. These security controls should prevent zero-day payloads from executing; identify newly discovered malicious behavior; prevent common and uncommon attack vectors; and take decisive, automated response actions without the need for human intervention.

Most of all, these security tools need to be resilient, requiring minimal updating without degrading their abilities to protect the environment.

When Lagacé arrived on the scene at one of Canada's leading network infrastructure providers, he found the company vulnerable to the same types of challenges companies without Telecon's technical savvy face every day.

Today's attack surface considerations

As a managed security service provider (MSSP), Plano, Texas-based Critical Start knows a lot of responsibility rests with

"Just buying security tools doesn't make you secure."

– Rob Davis, CEO, Critical Start

the company when it comes to protecting a client's attack surface. CEO Rob Davis says there are several issues officials consider, starting with the efficacy of a given product, the costs related to implementing and managing it, and its detection response capabilities.

The primary vectors for an attack surface are malicious executable software that someone manages to get on a desktop and macros in a Word document, Davis says. His staff also looks for "people exploiting unpatched software and programs and operating systems, and launching memory exploits or injecting code into memory exploits."

Stolen credentials is another concern. "A lot of times [attackers] store credentials and use them in ways you don't expect, and masquerade as you," he notes.

In the past 10 years, more endpoints have been added to the enterprise attack surface, increasing the complexity of managing a security environment. "What's really changed from an attacker's perspective is it is easier, and it takes less expertise, to launch an attack," Davis says. While the techniques have not changed all that much, he adds, it is much more lucrative to launch a cyberattack today.

"Attackers can find scripts online and it's very easy and cheap to launch an attack. It's easier to monetize with cryptocurrency and easily sell credit card numbers on the dark web," he says.

The cost to defend against attacks has gone up significantly, especially as the attack surface has grown, Davis says. "Everything was much more centralized, but now, instead of having one castle you have a hybrid infrastructure — part in a data center, part in the cloud, in multiple clouds and SaaS apps in clouds, and people working in multiple places and traveling — so there's infrastructure sprawl."

Since achieving rock-solid security is impossible, shrinking the attack surface is a critical goal for Robb Reck, CISO at identity platform provider Ping Identity. "Step one in managing the attack surface is knowing what you have, where it is, and understanding when there are changes to that surface," he says.

Rather than trying to hide all your assets behind a firewall and allowing broad access to it via a virtual private network (VPN) or network-based access list, Reck supports the Zero Trust approach and provides application/resource-level access to specific individuals and groups.

"This means that we're very granular about what access they get, from what type of device, and most importantly, who the person is, with a high level of assurance," he says.

Trying to get clients to move from a "detect and respond" methodology to a "provable prevention" methodology is paramount for Sig Murphy, consulting director for the western United States at Cylance Inc. of Irvine, Calif. Those are the two camps in the security industry, he notes. The detect-and-respond camp "has for years touted that CISOs need to purchase more and more technologies so that they can layer these together [and] hope for effective security." The kicker is, tools all have their own languages, training programs and certifications, and require numerous people to run them, Murphy says.

"Provable prevention, on the other hand, is a strategy that states, 'Stop what you can before it can perform badness, then deal with the rest,'" he says.

"What I worry about is the ripple effect and multiple effects that could occur if certain portions of infrastructure were taken out" by a rogue nation-state.

– Malcolm Harkins, chief security and trust officer, Cylance

Today, security professionals also must contend with industrial control systems (ICS), adds Davis. "That's all the boring stuff that runs power plants and generation, water systems and dams, that make the whole world work. Historically, that's been offline and there was no way to get to it."

Now, people want to monitor those systems and automatically update firmware to be more efficient, so everything is connected, and attackers are going after them, he says.

Add to the equation the shortage of cybersecurity professionals, which means it has become harder to retain them. Meanwhile, "your budgets haven't changed a whole lot," Davis says. "I'm glad I'm not a CISO right now."

Sleepless nights

Another aspect of the attack surface that most organizations worry about is their employees, which has two dimensions to it: an individual making an unintentional mistake or an insider attack, when there is a deliberate act by an employee to take data and do something malicious with it, observes Malcolm Harkins, chief security and trust officer at cybersecurity provider Cylance.

That sentiment is shared by Cameron Zink, senior systems engineer at Portland, Ore.-based Campbell Global, which manages natural resources investments. "Most of the not-quite-security-incidents but alerts we get are users who have leaked credentials, meaning they have fallen for a phishing attempt or something like that, along with our publicly available services, which we try to keep to a minimum," he says.

For example, Campbell Global has remote desktop servers that users can log into from both inside and outside the company, as well as data hosted by third parties. IT uses a Dropbox-like hub to hold data that is shared with those external third parties. "But we're still responsible for the security of that data, so keeping a close eye on things that are shared and who has access to what is a large part of what we monitor in order to make sure our attack surface stays as small as possible," Zink explains.

Since Critical Start provides security services to clients, Davis says he worries about "the number of companies that think they can buy their way into good security and somehow that will make them secure. Just buying security tools doesn't make you secure." Enterprises need to be training staff on how to operationalize and monitor those tools effectively, he says, since "most companies buy too many tools and don't use them or monitor them properly. This continues to frustrate me like Groundhog Day — doing the same thing over and over again and expecting different results."

Harkins worries about individuals getting planted inside financial organizations and knocking out large market exchanges almost simultaneously. "Think of the macroeconomic impact that would have on the world. It would be enormous," he says. "What I worry about is the ripple effect and multiple effects that could occur if certain portions of infrastructure were taken out" by a rogue nation-state.

Then there is concern over "the Ted Kaczynski [type] who happen to be smart enough … [to] weaponize something from a computing perspective," he says. "If someone can go into a hotel in Las Vegas and

> "We're clamping down on shadow IT, but it's a continual process to get people to buy into going through IT to get things done."
>
> *– David Lagacé, senior manager of IT security for information technology, Telecon*

take out a window and shoot people, how far away is that from someone doing the equivalent of a mass shooting but … saying 'I'm going to wipe out a wide swath of computer infrastructure because I can.'"

Lagacé says employees bypassing IT is a big issue at Telecon. "People deploying apps or projects that aren't aware of what they're doing, for example, [or] putting web servers on the Internet that are not patched," without going through the proper channels, could increase Telecon's attack surface, he says. "We're clamping down on shadow IT, but it's a continual process to get people to buy into going through IT to get things done."

Murphy's big concern is over certain IoT devices that attackers can target and defeat — or increase the arms race.

"I think we're going to see ransomware as a tactic spread to Internet-connected things in the near future," he says. "Can you imagine sitting down to drive your vehicle and being presented with a dialog box stating that you must pay a ransom to start your vehicle?"

On the arms race side, Murphy believes malware developers will begin to utilize artificial intelligence (AI) to create newer and more effective strains of malware. "We're seeing an evolution by malware makers toward Malware-as-a-Service (MaaS) by groups like MealyBug … and others," he says. "So it's only a matter of time until some of these groups start using effective AI for the harvesting [and] spreading of their wares."

Tried, but not true

With all these concerns at the forefront, many cybersecurity professionals are making valiant efforts to protect their enterprises' growing attack surfaces. But as is often noted, hindsight is 20/20. Sometimes, the tactics employed simply don't work. "One thing we tried that was problematic was building a single template for security," recalls Zink. "When we were building out services, we had this idea that we could make one secure server then just use that as a guide for how we built all others."

All servers were configured with same with same firewalls and access rules, he says. "When we used that template of one way of configuring everything, we found it broke a lot of things we were working on." This left some vulnerabilities open on certain servers and it also left some things functioning improperly because they needed additional rules IT hadn't built into a template, he says.

"Instead of being able to generate things from a template to follow, we have about a dozen now to ensure everything's locked down for the service being offered," Zink says.

Reck found that moving datacenter-native security controls into the cloud does not work. "Controls based on a single ingress and egress from an environment work poorly in a datacenter, and not at all in the cloud," he says. "Rather than trying to shift your favorite legacy security control into the cloud, [you] need to adopt cloud-native solutions that work internally to the workloads and accounts."

Critical Start's Davis says they learned to plan for failure with their clients. "Nobody has an infinite amount of budget for security, so you can't do everything you want," he says. "We've learned the best place [to spend] money is on good protection and good, responsive tools at the endpoint level."

> "So it's only a matter of time until some of these groups start using effective AI for the harvesting [and] spreading of their wares."
>
> *– Sig Murphy, consulting director for the western United States, Cylance*

He says he finds it amazing that companies do not do this more often. "They have good protection tools … but they don't plan for failure so when something does happen [they] can detect it quickly and respond quickly."

For example, a large insurance provider Critical Start worked with had a large security operations center (SOC) with perimeter protection and firewalls, "but any time something goes wrong they have no ability to investigate even the smallest thing," recalls Davis. "It takes a lot of time and during that time, an attacker is within the organization and can accomplish what they want — steal information [or] install a Trojan. This is an example of people spending to establish a SOC, but if they don't have right tools and they're not training in the right way and it's not well managed, it won't be effective."

Many of the clients Murphy talks to are frustrated with cloud-hosted apps that are not properly secured. "The big example of this in 2018 [was] the move by business email compromise (BEC) actors toward a malware-less entry vector," he says. In this model, the threat actors do a bit of reconnaissance to craft a phishing email with a link that masquerades as the victim's email provider, such as Office 365 or Gmail, and the user is presented with a login prompt when clicking on the link.

The user enters their credentials, and then is forwarded to a bogus external document. "They scratch their head thinking, 'this wasn't the document that I was looking for… weird,'" Murphy recounts. "But the attacker has harvested their email credentials and can now log in and masquerade as them. The attackers then spread out inside the victim's environment through additional spear phishes and then also target third parties."

In 2017, 78 percent of U.S. companies were victimized by BEC attacks, Murphy says.

What security professionals want

One of the main features Zink always looks for in a software product is visibility. "The more visibility and information and logging we can get out of our tools, the better," he says.

Lagacé says he prioritizes usability over cost. However, "if I can put something in place quickly and at a low cost, that's a definite winner," he adds. "Otherwise, I have to look at the requirements, like ease of use," and offerings that are effectively plug-and-play.

Davis says he advises people to have software with good endpoint protection, detection and response capabilities to reduce the risk to the organization's attack surface.

"The biggest problem with most security tools is the massive delta between the potential value of the tool, and the actualized value," notes Ping's Reck. "It's easy to buy a new tool and see it sit half implemented. I look for partners that make the implementation of their technologies as seamless and turnkey as possible. If they are able to sell a solution instead of a set of tools, that goes a long way."

This approach will be crucial with the shift in recent years toward services, and specifically, APIs for doing business, he says. "Instead of the typical visible applications, the move to APIs is already underway, and it allows data to flow behind the scenes. This can improve security when done right."

But all too often, the shift is done

> "By building in our controls at all these levels, we reduce the risk of a rogue service getting stood up unprotected."
>
> *– Robb Reck, CISO, Ping Identity*

invisibly to the security team, thus exposing the services to risk, he says. "Building a security model that incorporates identifying and securing APIs in the cloud world is essential to the future of security."

Security needs to be built into all levels of an organization's entire infrastructure — meaning the accounts, security groups, operating systems and applications it runs, says Reck. "By building in our controls at all these levels, we reduce the risk of a rogue service getting stood up unprotected, and in the event that it does happen, this model also will reduce the impact of the issue, by ensuring that one hole doesn't expose the entire environment."

The attack surface is only going to expand and the number of devices to defend against is growing exponentially, thanks to the IoT, says Davis. And people are still the easiest attack surface, so they need constant training and protection.

If Zink had his druthers and could simplify and automate protection of Campbell Global's attack surface, there would be significantly fewer false positives and false alerts in the security monitoring. The firm would also have users who are better about protecting their information and credentials, he says. "Really, those would be the two biggest changes between where we're at and where we'd like to be in a perfect world." ■

For more information about ExpertFocus from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an eBook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

ExpertFocus

Cylance has redefined endpoint security. Our products and services aim to predict and prevent, rather than reactively detect, the execution of advanced threats. Deployed on over 14.5 million endpoints, we protect clients worldwide including Fortune 100 organizations and governments.

For more information, go to https://www.cylance.com/en-us/index.html

Corporate Information Technologies works with companies to create a Culture of Security. We replace the rhetoric and TSA version of security implemented by most companies and MSP's by implementing our Foundational Security Framwork. Is your Cyber Security up to the challenge?

Corporate Information Technologies - www.corp-infotech.com


Cybersecurity is a numbers game.
It's time to embrace zero.
Nothing is worth more than your peace of mind.
Zero anxiety about cyber threats is achieved through deploying a proactive strategy of defense. Our AI-driven security solutions help you prevent attacks before they can damage your devices, your data, or your reputation.
To learn more, visit cylance.com/zero
CYLANCE