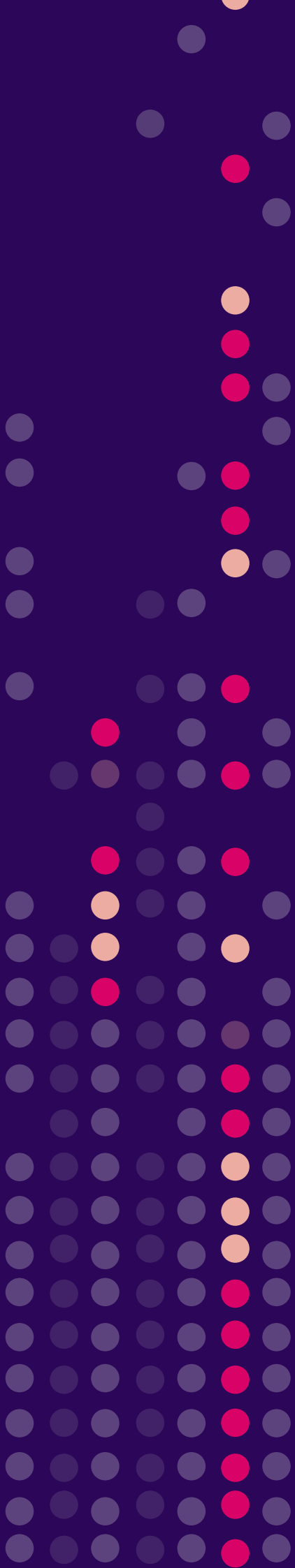
zilla SECURITY

EBOOK

A look inside the security risk of outside identities



A Look Inside the Security Risk of Outside Identities

Understanding security from the inside out

Remember when "going into work" didn't mean going into the spare bedroom/home office and closing the door behind you to muffle the sounds of playing children and barking dogs? Which isn't to say that working from home is a bad thing. Thanks to technologies such as videoconferencing, cloud-based applications, and mobile apps, workers have been able to maintain and even improve productivity while working from home. In a recent Gallup poll, 90% of workers said they want to continue working from home part time even after the Covid pandemic subsides.[1]

As helpful as work-from-home (WFH) initiatives have been for companies, the WFH movement has also turned network security inside out. Internal employees are accessing the corporate intranet from external locations, business applications are as likely to sit in a third-party cloud as in the corporate data center, and employees are increasingly using "shared devices" such as personal laptops and smartphones to access sensitive applications and data. Add to this a growing reliance on virtual teams that include contractors, part-time employees, and partners, and it becomes easy to see why many companies struggle with enforcing security policies and managing compliance beyond their four walls.

In the past, security teams were able to apply more stringent security measures to external parties. But in a world where even the people on the inside are often on the outside, businesses find themselves granting too-broad access privileges to external identities. Cybercriminals know this, and they know that external identities often have looser security guardrails in place, which makes them easier to compromise and exploit. Not surprisingly, some of the most serious network breaches in recent years have come from compromised external sources.

90%

of workers

want to continue working from home, even after Covid risk subsides

Why are external IDs a bigger security risk now more than ever?

There are three driving forces behind the increase in external ID security risks. These are the cloud, the composition of virtual teams, and Covid.

The widespread adoption of cloud-based services and mobile apps has caused an explosion in the number of application programming interfaces (APIs). A typical enterprise may have hundreds of APIs (or more) in play to connect applications, databases, networks, users, and devices. APIs are a critical part of our digital world, but they also represent a possible security risk by providing a poorly secured means of entry into otherwise secured systems. Tellingly, more than 90 percent of developers rate API security and privacy as one of their most important considerations when developing new applications.[2]

Virtual teams have become the new normal as enterprises look to attract and retain the best talent. Millennials in particular value work/life flexibility that includes working from home and business hours beyond the traditional 9 to 5. In addition, the rise of the "gig" economy means that more workers are joining the workforce as freelancers, contractors, and part-time employees. This shift away from the traditional, office-bound employee means that even internal employees frequently find themselves outside the lines of traditional security mechanisms such as firewalls and identity protection.

As we all know, the Covid pandemic accelerated the timetables for the remote workforce migration. At the peak of the pandemic, some enterprises moved as much as ninety percent of their workforce to a fully remote arrangement. While many workers are now returning to the office, employees still want the flexibility of working from home, at least on a part-time basis. IT teams will need to find ways to enforce security policies and monitor compliance across a constantly moving workforce and continually shifting landscape of devices and identities.

90%

of developers

say API security and privacy is top of mind

If you don't pay attention to external IDs, hackers will

Hackers are like fleas in winter. They'll hop on anything or anyone so long as it takes them inside—often hiding for months before they're discovered. Security professionals know this and have multiple safeguards in place to protect employees as they enter and leave the network, from multifactor authentication to real-time threat detection systems. You can think of these safeguards as a kind of virtual flea collar for office workers. But the network is only one doorway, albeit an important one, to critical applications and data. What about applications hosted on clouds, vendor systems with "back door" access to your network, and even the APIs that travel back and forth between applications and external users? What kind of protection do they have against hackers?

These fleas are more than a small source of irritation. Once inside, they can cause devastation. You only have to read the news to see what can happen when hackers take advantage of under-protected partners, vendors, and APIs. One of the biggest hacks in history occurred when Target's HVAC partner was compromised, allowing cybercriminals to slip inside Target's network and steal millions of customer records, ultimately costing the retailer millions of dollars in fines.

When the game-streaming platform Twitch (owned by Amazon) was attacked in 2019, the source of the attack was determined to be a misconfigured server that allowed a third party to sneak into the network and steal valuable data. Last year, Nieman Marcus announced that millions of customer records had been stolen by an unauthorized third party; a breach that took the company nearly a year to discover. Unfortunately, no business is immune to being targeted because of the myriad entryways into their business. But businesses can protect themselves from being attacked by paying more attention to what's happening outside their network.

A steady drumbeat of security breaches in the news

"A devastating Twitch hack sends streamers reeling"

"1.1 million credit cards exposed in three-month hack"

"Target to pay $18.5 million for data breach that affected 41 million consumers"

Test your security strength: 5 questions

How can you tell if your business is at risk from external identities? As a rule of thumb, if you're not worrying about them, you probably should be worried. Recognizing that external identities represent risk and mitigating that risk through real-time visibility and proactive measures are critical components for a sound security strategy. If asked today, would you be able to answer these questions:

1 **Who is accessing our network from the outside?**

Partial visibility into active users is one of the biggest reasons that companies are blindsided by external attacks. Your Active Directory only tells part of the story. What about your partners and vendors and their partners and vendors? And then there are your known users who may be using unknown IDs from a different device when they're working remotely. If you want to protect your network, the first step is to know who you're protecting it from.

2 **Does our permissions model give us the flexibility to address a wide range of different users?**

We get it: configuring hundreds of different security policies is hard work. So, organizations tend to use "blanket" access privileges for everyone. This is exactly what hackers want you to do, because they can then find an external account with minimal security that has maximum access to everything including sensitive files and controls. There is no shortcut to a strong security strategy; you need flexible permissions rules that can be automatically configured and consistently enforced.

3 **Do we have "orphaned" external accounts?**

An orphaned account is one that no longer has an active user: e.g., an old vendor, a former employee, a retired application, or even a customer who no longer accesses their rewards account. Orphaned accounts tend to live in the shadows where companies don't see them. Hackers, however, know how to find them and actively look for them because they're often lacking the latest security updates and/or not being monitored by anyone.

4 **Are there non-human identities outside the organization (e.g., APIs) that pose a security risk?**

Just as organizations need to know who is accessing their applications, they also need to know what is accessing their applications. APIs, for example, have become an increasingly popular target for hackers because many APIs are only partially secured. As a result, malicious code can be passed along in APIs that aren't being monitored or external parties can use APIs to access the network and move laterally to steal sensitive data.

5 **Can we maintain security compliance inside and outside our network?**

Healthcare organizations, financial companies, and retailers that collect customer financial data are familiar with the various security compliance measures that regulate their industry. Monitoring and testing compliance is relatively straightforward when you're working with a single, secured network—but what happens when users, applications, and data are spread across multiple clouds, regional offices, and personal devices? It's a question that regulators are asking with more frequency—and one that companies will need to answer.

Zilla Security has the answers you need

If you feel like you have more questions than answers after testing your security strength, you're not alone. According to one recent study, 93 percent of business networks could be compromised by an external attack right now.[3] So, what can you do to protect yourself from external identity attacks? Talk to Zilla Security.

Zilla's security solutions give businesses the visibility they need to identify orphaned accounts, track external users, pinpoint vulnerable APIs, and more. And Zilla also provides automation to help security teams manage, customize, and control their security policies in today's inside-outside world. Cyber-criminals are counting on businesses to maintain their plain vanilla security strategy. If you want to beat them, add Zilla to your plain vanilla and keep the bad guys outside.

Learn more at zillasecurity.com

Learn More

Sources

1. Saad, Lydia and Ben Wigert, "Remote Work Persisting and Trending Permanent," gallup.com, last accessed March 10, 2022 (https://news.gallup.com/poll/355907/remote-work-persisting-trending-permanent.aspx)

2. "RapidAPI's New State of APIs Survey Finds Majority of Software Developers Increased Reliance on APIs," businesswire.com, last accessed March 10, 2022 (https://www.businesswire.com/news/home/20211208005267/en/RapidAPI%E2%80%99s-New-State-of-APIs-Survey-Finds-Majority-of-Software-Developers-Increased-Reliance-on-APIs-Participation-in-the-API-Economy-Grows-In-Importance-Across-All-Industries).

3. Brooks, Chuck; "Cybersecurity in 2022 — A Fresh Look at Some Very Alarming Stats," forbes.com, last accessed March 10, 2022 (https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=25e5af026b61).