4 Hidden Security Gaps for Remote Work

IDENTITY
ENDPOINT
VPN
DATA

impelix

Intro

"Many gaps lay in wait for companies who are instituting fully remote workforces."

"I wrote this to share the insights I've gathered from our own journey."

From the founding of Impelix a decade ago, we knew that being a distributed workforce would be in our DNA. Whether working from home, a coffee shop, or 30,000 feet in the air, we wanted everyone at our company to be able to do their job.

Early on, I began to recognize the unique challenges this presented us: gaps, lying hidden, created by our work-from-anywhere workforce. To mitigate them, I set about putting various solutions in place, ones that weren't anywhere near as robust or elegant as we have today.

Many of the gaps I identified back then still lay in wait today for many companies who now, a decade later, are instituting fully remote and distributed workforces.

Fortunately, much progress has been made in the development of cyber security solutions that address remote work. I've tested and deployed them to mature our work-from-anywhere model, remaining committed to it even as Impelix substantially grew.

For companies that are now exploring this new territory, I've written the following series to share the insights I've gathered from our own journey.

Thomas Whang
CTO

Contents

impelix

Hidden Security Gap

Identity 1

To prove identity, two pieces of information are required at minimum: a form of identification and a form of authentication. Traditionally, this is usually some sort of user ID for your identification and a password for authentication. This is known as single-factor authentication (SFA).

The primary method of security here is the password complexity. Unfortunately, humans perform very poorly when generating strong passwords. Additionally, since we are bad at generating complex passwords, we will also tend to reuse the same passwords.

Gap: using weak, reused passwords to access apps, many in the cloud, from outside the trusted network

With the majority of us working from home nowadays, to perform our job, we must authenticate to applications that reside in the cloud and in our organization's data center from outside of the secured and trusted network. Doing so opens up one more attack surface for bad actors to target. If the account information is compromised, this will likely allow the bad actor access to multiple applications and/or systems within the organization.

In our early days, to mitigate this specific type of security gap, we implemented a very strict password policy along with an aggressive password rotation policy. Then came along two-factor authentication (2FA).

Instead of just a password required to authenticate, we needed another authentication factor. Originally, we started with SMS; however, it's now considered inadequate. Eventually, we moved to a software token-based solution.

Stop gap: strict and aggressive password policies, plus software token-based 2FA

2FA mitigates the credential theft situation. Without the second factor, a bad actor is unable to gain unauthorized access into the application or systems. This also allows the IT team to reset the user's password without exposing the organization due to a compromised password.

impelix

Hidden Security Gap

Identity ①

Modern IAM: 2FA and Beyond

Today's solution for Identity and Access Management (IAM) is very robust. Along with 2FA, other notable features include 1) Single Sign On (SSO) and 2) adaptive capabilities (where are you acting from, what type of device, are you human or not).

- 2FA
- Single Sign On (SSO)
- Adaptive capabilities

If you haven't enabled 2FA/MFA in your organization, I highly recommend that you take the time to evaluate an IAM solution. Given the extraordinary times we are currently in, our partner Okta has developed an emergency remote work program for any organization to adopt SSO with MFA at no cost for six months.

As we adjust the way we work, we should also assess and adjust the security necessary to keep our people safe and our companies safe. Let's all do our part, both physically and in cyber.

impelix

A Rise in Off-Network Risk

With the sudden and dramatic shift from our normal office commute to a work-from-home environment, significant new challenges have sprung up. How do you maintain the same level of endpoint security when all your assets are now off-network? Being off-network has dramatically increased the attack surfaces of most organizations, making them ripe targets for bad actors. Across many of our clients, we have seen a dramatic uptick in phishing scams, ransomware and malware attempts.

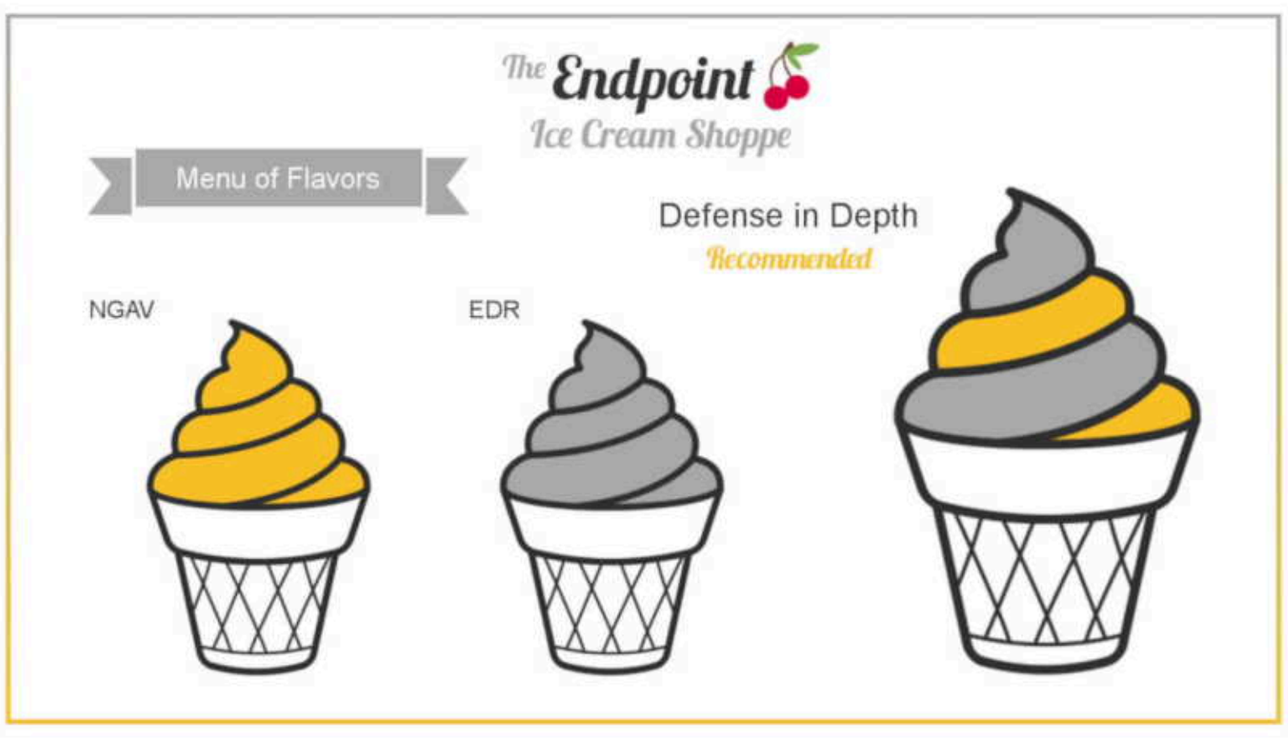
Across many of our clients, we have seen a dramatic uptick in phishing scams, ransomware, and malware attempts.

How can we combat this barrage of attacks?

Endpoint: The First Line of Defense

The first line of defense would be securing the endpoint. Endpoint protection comes in many flavors, but for the purpose of this post, I'll focus on two: Next-Generation Antivirus (NGAV) and Endpoint Detection and Response (EDR).

So you may be asking yourself, what is the difference between NGAV and EDR? Aren't both describing the same thing? They're both ice cream, sure, but they're different flavors. I'll show you the differences in "taste" and why you need to combine both to serve up a "Defense in Depth" swirl.



Next-Generation Antivirus

As the name suggests, it takes the concept of antivirus—with which all of us are familiar and have been using for 20+ years—and brings the technology into the 21st century.

What makes it "Next Generation"? It's the enhancements in detection and prevention. The legacy antivirus engines used virus definition files that included signatures of known bad behaviors. Unfortunately, signature-based antivirus engines weren't designed to handle the type of malware of today like polymorphic or multi-stage, just to name a couple.

> The biggest advantage NGAV brings is the ability to identify both known and, more importantly, unknown malware and prevent it from causing any damage.

NGAVs use additional techniques to detect and prevent malware compared to legacy antivirus engines. Many will incorporate some combination of artificial intelligence, behavioral detection, machine learning algorithms, and exploit mitigation. The biggest advantage this brings is the ability to identify both known and, more importantly, unknown malware and prevent it from causing any damage.

Endpoint Detection and Response

If NGAV is capable of identifying and preventing known and unknown malware, doesn't that mean the endpoint is secure? Not exactly. The answer is yes, but … there is still risk. If you notice, NGAV only talks about malware and preventing malware. What about all the other ways that an endpoint can be compromised? This is where EDR comes in.

EDR can secure the endpoint above and beyond just malware-based attacks. It's ability to analyze different types of tactics and techniques from the bad actor's actions provide an additional layer of security to the endpoint. EDR can detect and prevent actions like lateral movement, privilege escalation, and command and control communication to name a few.

With the additional capabilities, you get extra benefits (think sprinkles on top of your ice cream). Those can include:

- Process-level activity visibility
- File-level activity visibility
- Stitching of related attack activities
- Containment of host (with remote response capabilities)

Complete Endpoint Security: A Swirl of NGAV & EDR

If you are currently using a legacy antivirus solution, I implore you to upgrade to an endpoint solution technology that incorporates both NGAV and EDR capabilities. Remember: don't pick a flavor, combine them.

As you can see, a good endpoint security solution will combine the capabilities of NGAV and EDR to provide a comprehensive package to secure the endpoint—a Defense in Depth swirl. Many of the endpoint solutions incorporate additional functionalities, giving you more robust capabilities in visibility, intelligence, application and operating system vulnerability, and more.

I'd urge anyone who is already using these new endpoint security solutions to get very familiar with all the different features. There may be some hidden benefits that you've missed—possibly even displacing other tools you may have.

Hidden Security Gap

VPN 3

The VPN Tradeoff

The default (and outdated) remote access solution deployed today is VPN. It provides a secure connection for your remote workers to access your internal resources. But what about internet or SaaS traffic? (Office 365, Salesforce, etc.)

You're forced to make a tradeoff: do you choose performance or security? Which is really a choice about who gets to be happy ...

You're forced to make a tradeoff: do you choose performance or security?

If you choose performance via split-tunneling, your users will be happy. However, you won't be, on account of restless nights worrying about the risk of their unfiltered internet access.

If you choose security via force tunneling, your users won't be happy with the poor performance from backhauling their internet-bound traffic. Neither will your network team with the increased bandwidth consumption at the data center. And your nights will still be restless because of all the complaints.

It seems you're damned if you do, damned if you don't. Of course, that's with yesterday's solution, VPN. But what about tomorrow's?

Heck Yes, We Can

Is it now possible for everyone to be happy? Can you really have your cake and eat it too with both security and performance? Heck yes, we can!

impelix

Hidden Security Gap

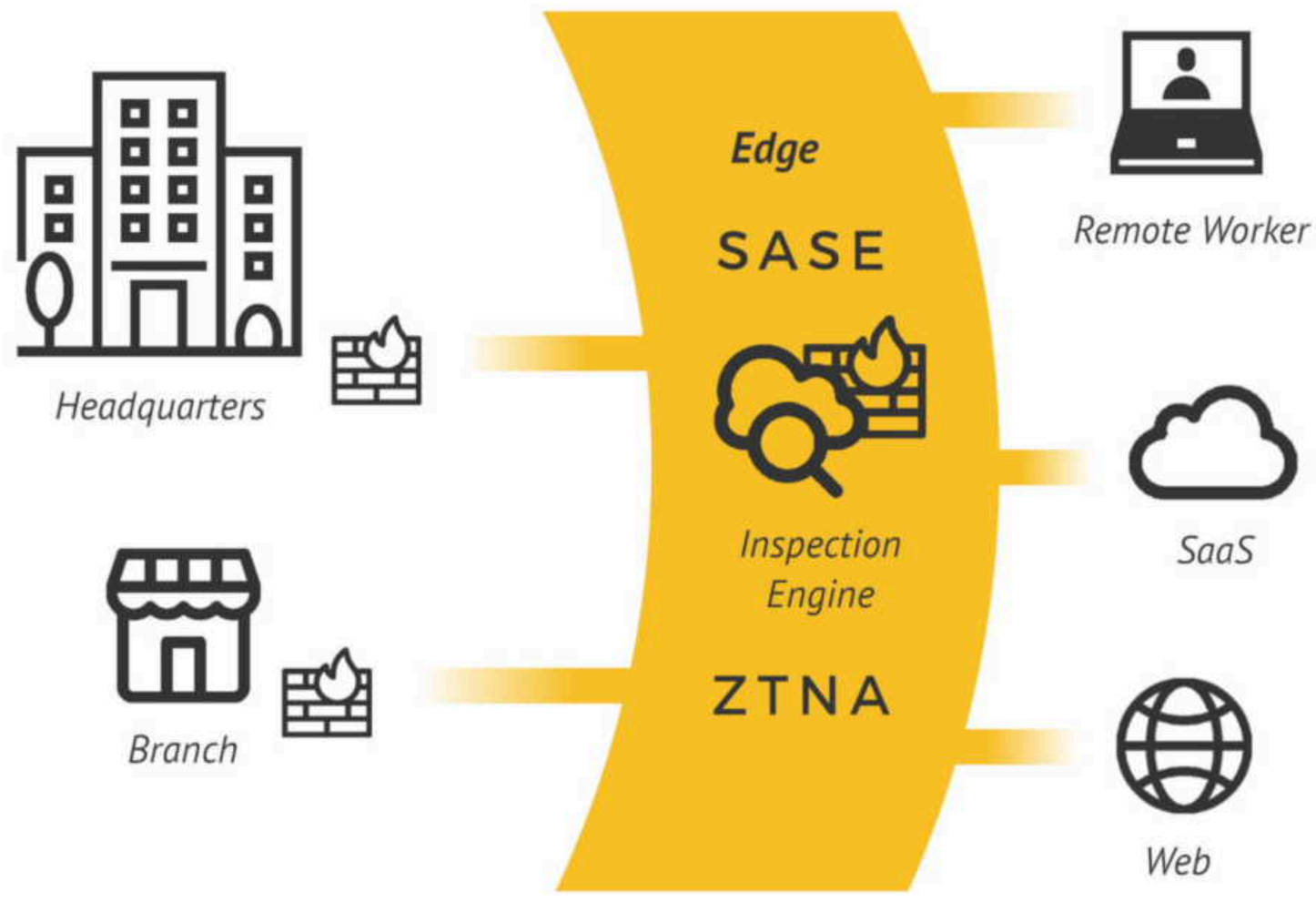
VPN 3

Solutions now exist that provide excellent security without compromising performance. These are based within the SASE concept and its core directive to move inspection engines to remote users, not the other way around, thereby inspecting traffic as close to the source as possible. In this model, it's at the Service Edge that all security policies are enforced: Malware/Threat Protection, SSL Decryption, Data Security, and more.

Security policies enforced at the Service Edge:

- Malware/Threat Protection
- SSL Decryption
- Data Security
- And more!

You get performance (no backhauling traffic) and security (NGFW functions at the Edge).



Private Access from the Edge

Here's the icing on the cake: you can use this same Edge for private access to your corporate environment. What?!

impelix

Hidden Security Gap

VPN 3

Yes, this Edge also serves as your VPN gateway infrastructure. Say goodbye to your legacy VPN infrastructure. Say hello to the remote access VPN killer. These VPN killers can provide granular access down to the specific applications for each user. Can you say Zero Trust?

Say goodbye to your legacy VPN infrastructure. Say hello to the remote access VPN killer.

A SASE-based security infrastructure can provide secure access to the Internet for your remote users and a replacement of VPN connectivity that's more agile and granular, accomplishing Zero Trust Network Access without any of VPN's cumbersome infrastructure. Plus, because these next-gen solutions are cloud delivered, performing a proof of concept requires mere days, not weeks or months.

Goodbye, VPN

If you've continued to rely on VPN in the transition to WFH, you've most likely been forced to make a tradeoff. For many, it has come with increased risk to maintain an office-like experience for employees now working from their couches and kitchen tables. It doesn't have to be that way.

Next-gen, cloud-based solutions are now available, capable of delivering a secure web gateway and ZTNA at the Edge by moving inspection engines out of the corporate data center to wherever remote users are located. So long, legacy tradeoff!

Have your cake. Eat it. Then lick the icing off your fingers while you wave goodbye to VPN.

impelix

Hidden Security Gap

Data ④

Why Data Security?

You're probably thinking your data is safe because you have an identity infrastructure, an endpoint security solution, and VPN. Well, I've got bad news for you: your data is not safe as you think.

Why not? Because Digital Transformation, that's why—the Harry-and-Marv "Wet Bandits" of the modern attack surface.

Companies, large and small, are consuming cloud-based software services at an alarming rate. Every time an employee connects to a SaaS provider, sanctioned or unsanctioned, there's the potential for data to be leaked, lost, or encrypted.

Every time an employee connects to a SaaS provider, sanctioned or unsanctioned, there's the potential for data to be leaked, lost, or encrypted.

So, what's the difference between sanctioned and unsanctioned?

Sanctioned Applications or Providers

This term refers to cloud services that have gone through an organization's risk and business management process and have received approval for organization-wide or department-wide use.

impelix

Hidden Security Gap

Data ④

Unsanctioned Applications (a.k.a. Shadow IT)

This term refers to SaaS applications or cloud services consumed by employees or departments without the knowledge of the central IT organization, thereby creating higher risk.

Sanctioned Data Leakage and Loss

A lot of emphasis is placed on the riskiness of Shadow IT for good and obvious reasons. However, even with data residing in sanctioned application providers, there's plenty of risk for leakage and loss, in large part due to the inability to control a user downloading, interacting with, or encrypting it. Once the user is authenticated, they have free reign. Essentially, the data has been leaked.

With the ability to download all data from the sanctioned application, a user can upload it to any number of cloud storage or SaaS providers outside of the organization's IT purview. The data has now been lost. The organization, at this point, has lost all control and visibility of the data. Uh-oh.

All hope is not lost, though.

impelix

The Solution: SWG & CASB in SASE

The solution is in the cloud, in the form of a Secure Access Service Edge (SASE). Two major features of SASE, Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB), provide NGFW-like functions through Data Loss Prevention (DLP) capabilities applied to internet-bound traffic.

SASE delivers data security without compromising performance, the ultimate combination.

With SASE, data can be inspected and policies can be enforced at the service edge. You're empowered to monitor data movement and enforce any data security policy regardless of the user's location or type of access. It delivers data security without compromising performance, the ultimate combination.

Data security with SASE:

- Traffic inspection at the edge
- Monitoring of data movement
- Enforcement of data security policies
- Applied regardless of user's location or type of access
- No compromise of performance

Hidden Security Gaps for Remote Work

Conclusion

In closing, this series was meant to help you see the gaps lying in wait in our "new normal" of an entirely remote workforce. I hope I did that for you! I also hope these insights, born out of my own experience, have helped you and your organization be safer. If you gained any nugget of information that helped you, I've done my part.

Stay safe everyone ... in the cyber world and the physical world.

Thomas Whang
CTO

Drive onward

impelix