CYCOGNITO

WHITE PAPER

ATTACK SURFACE VISIBILITY

The Foundation of Effective Cybersecurity

ATTACKERS UNDERSTAND YOUR ATTACK SURFACE. DO YOU?

Attackers are looking for the path of least resistance in your attack surface so that they can break into your high-value digital assets. To stay ahead, you have to think like an attacker too. That requires ongoing visibility of your attack surface, and there's only one proven way to establish attack surface visibility: perform reconnaissance across your entire IT ecosystem, adopting an outside-in approach.

How much of your IT infrastructure — your digital attack surface — is susceptible to an attack? The extent to which you are open to attack depends on the depth and breadth of knowledge you have about what is connected, what is running and where it is. In order to protect your assets, you have to understand what you have, right down to the last connected device.

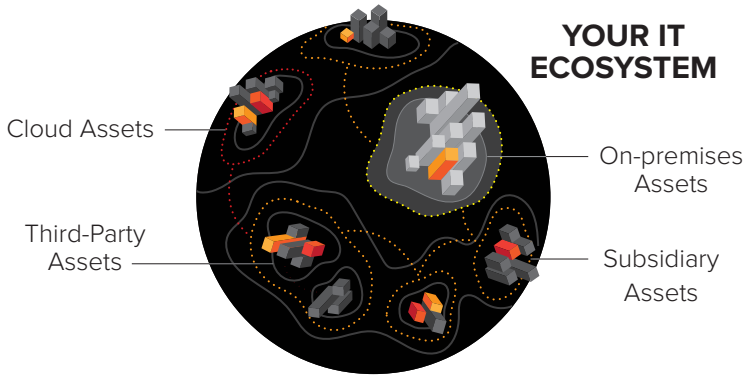

Figure 1. What is an attack surface? An attack surface is the set of ways in which an adversary can illicitly gain entry to servers, applications, data, and partner assets and potentially cause damage.

And of course, there are challenges... your cloud-based infrastructure and applications... the DevOps team members who are bringing up new resources as fast as they can type... the partners and subsidiaries that you connect with... and the flood of attack vectors and vulnerabilities that are constantly being discovered — over 16,515 Common Vulnerabilities and Exposures (CVEs) reported and added to the MITRE list in 2018.[1]

Increased IT Complexity Impacts Security

Applications and systems that used to sit within a well-defined perimeter have now shifted — in part or entirely — to a cloud infrastructure, with edges that are amorphous and changing daily, if not hourly. The implications of this change are profound, as you deal with ever-increasing gaps in the information you need to secure your enterprise assets, where every small misconfiguration has the potential to open up access to customer data, financial information and systems, application source code and intellectual property.

1 https://www.cvedetails.com/browse-by-date.php

As a chief information security officer (CISO), both you and your security team need to be able to answer these questions as part of your assessment about the exposure of your IT assets to compromise:

What are our shadow risks — the blind spots that attackers target, but we don't know exist?	How can we view cyber risk across our entire IT infrastructure, including partner connections and integrations?	What part of our IT portfolio, from on-premises to cloud, is most susceptible to compromise?	From an attacker's point of view, what assets are most attractive?	What's the impact to our organization if a particular attack vector is exploited?	How do we prioritize our risk mitigation efforts to get the greatest reduction in risk?

Asset Inventory: How Much Can You See?

Your attack surface is made up of digital assets you have or use, so to understand your attack surface, you have to understand your assets and how they are connected to your infrastructure, partners and other networks. Even more importantly, you must understand how those assets relate to your business: who owns them and in which business processes are they used. This information is fundamental to determining the criticality of any associated risks and requires a level of insight that goes well beyond a listing of IP addresses and ports.

IT Asset Management Tools are Siloed

There are literally hundreds of solutions available to discover and document what assets are in your IT infrastructure: from network discovery to on-premises asset management solutions to cloud asset inventory/management tools, to solutions that work for hybrid environments such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS). They find assets and build a database about the hardware, software, network and communications infrastructure, servers, and applications connected to and running within your IT environment.

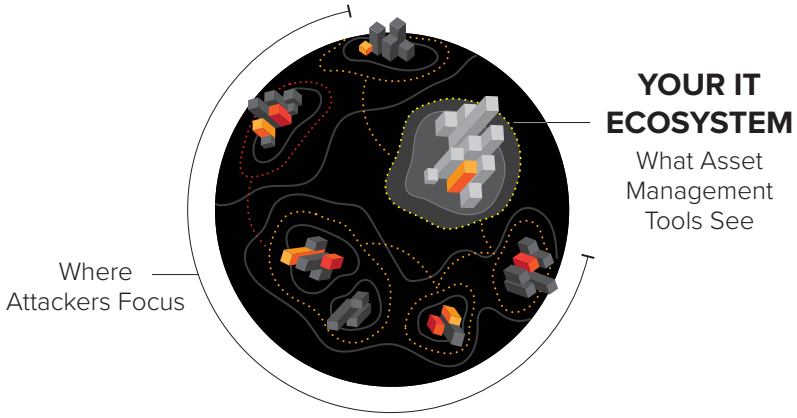

Figure 2. Asset management and security assessment solutions see portions of your IT ecosystem but do not provide comprehensive coverage. Worse, they entirely miss assets in your IT ecosystem that belong to "others" such as partners and subsidiaries as well as assets that are unknown to your IT teams.

Asset management solutions neglect a tremendous amount of your attack surface entirely. For example, they cannot discover the cloud environments that your lines-of-business and functional teams are using but which your IT teams don't know about. They do not explore the assets associated with connections and integrations your partners have with you or the assets belonging to your own subsidiaries. And, they cannot identify assets that are abandoned yet remain a part of your attack surface and expose you to threats.

So, what are you really getting by using a combination of IT asset management solutions? A collection of siloed data that represents an incomplete snapshot of your IT infrastructure and assets; a snapshot that is out of date by the time it is assembled.

Security Solutions Also Provide a Partial View

Security solutions do not address the problem well either. They miss the same elements that IT asset management solutions do, such as assets from unmanaged, unknown, abandoned, partner and subsidiary environments. For example, vulnerability assessment products look only where they are configured to look and they assess IT assets using a list of devices or IP address ranges configured by an administrator. At best, the source of the information used by those administrators comes from IT asset management, configuration or network discovery solutions that do not produce a comprehensive picture.

As with IT asset management solutions, relying on results from vulnerability scanning tools or penetration tests leaves your security team with outdated and incomplete information that doesn't represent the true picture of your infrastructure.

The common thread amongst all of these approaches is that they each cover a piece of the problem, but do not offer complete insight into all of your IT resources and assets no matter where they are situated.

Leveraging existing information sources — such as IT asset management solutions or IT security solutions — to help map an attack surface simply doesn't work. There are too many blind spots. Attack surface mapping and visibility can only come from performing ongoing reconnaissance, much like attackers themselves do.

You Don't Know What You Don't Know

In the end, what seems like a natural starting point for establishing attack surface visibility — IT asset management and security assessment solutions — leaves your organization with critical blind spots. And without full attack surface visibility, it is impossible for your security team to defend your business from cyberattack. Having a cybersecurity plan in place is meaningless if your IT and security organizations are not aware of all of the assets and resources they are supposed to be securing and protecting. The ability to build and implement a comprehensive security strategy is predicated on having reliable and continuously up-to-date information on all the assets that comprise the entire universe of your assets, no matter where they reside.

Critical Information for Mapping the Attack Surface

There are five key dimensions that you must address to create an actionable attack surface map. The critical insights you need are:

01 **What Are All the Assets?** A complete asset inventory, as discussed, is not possible with traditional solutions because they leave too many blind spots. A meaningful inventory must also include assets (e.g., systems, infrastructure and cloud-based resources) that are part of the organization's extended IT ecosystem including:

Unmanaged assets: Cloud-based resources or applications including: IaaS, PaaS and SaaS; semi-autonomous subsidiaries with connectivity to the rest of the enterprise; third-party IT business partners.

Abandoned assets: Cloud-based applications, source code repositories, development tools, digital certificates that are not in use and have not been decommissioned.

Unknown assets: Assets put into use independent of the IT organization by individuals, business units, or subsidiaries, and not tracked or discoverable by current tools in use. For example, imagine a self-provisioned marketing platform used in a branding campaign.

Misconfigured assets: Any assets with logins that are not properly configured, using defaults and/or missing parameters. While misconfiguration of cloud assets is commonplace, this category includes legacy systems — even mainframe computers — unintentionally exposed to attackers.

02 **Just How Important Is That Asset?** Besides the issues around unmanaged, abandoned and unknown assets, you and your security team need business context about the assets. This context needs to include not just information about the operating system software running on the asset, but what business applications or data are hosted there and the likely owner of the asset. Establishing an association between each asset and its business purpose helps you understand the criticality of each asset to the business as a whole. For example, knowing that an asset is used in finance processes or contains source code for a business application enables you to prioritize issues associated with that asset.

Armed with this information, your security management and security operations center (SOC) teams are able to incorporate the importance of assets into overall strategy.

03 **What Are The Risks?** Building on the first two items, you need to understand which threats are applicable to your assets. Knowing how attack vectors are interwoven into your on-premises infrastructure, applications and cloud-based applications and resources is essential. Every asset, no matter what it is, could have one or more vulnerabilities or other flaws associated with it, and each of them needs to be quantified by its business impact.

04 **How Much Risk?** Insurance companies insure individuals, businesses, and property against accident or catastrophe based upon the quantifiable risk of a loss occurring. They leverage hundreds of years of experience and data to quantify this risk. In the case of enterprises, and the chance of a cyberattack occurring, measuring risk requires understanding the extent to which an asset is exposed to one or more threats. Each vulnerability or attack vector must be assigned a risk score, which defines the impact it will have if used in an attack. Individual assets may have one or more such issues that apply to it. The combined score represents the total risk that applies to that asset.

05 Continuous Asset Insight

In order to maintain attack surface visibility, you need updated information about your IT ecosystem, including connections to partners and subsidiaries and the many sources of shadow risk discussed previously. Unless this information is updated continuously, your organization will be blind to the kinds of changes that occur daily in modern IT environments: new assets brought online, older assets deprecated or abandoned, and unmanaged assets incorporated into critical business processes. These attack surface visibility gaps impact your ability to manage your organization's overall risk.

An Information War

Your security team is waging an information war against cybercriminals and state-sponsored hackers. The one thing attackers desire most is information, but it is not your data or IP that is most valued, as most people would think, rather it is the information necessary to gain access to your infrastructure and then steal valuable data and IP from your company. It is this information that represents a huge advantage for hackers over those trying to defend against them.

In the words of Sun Tzu, "To know your enemy, you must become your enemy." For an attacker, knowing your company — their enemy — is absolute necessity. The information needed by each side in this adversarial battle is the same, but used with different intent as the table below shows.

		Enterprise Security	Hackers
Information Source	Assets and infrastructure	Needed to ensure that all assets are known and can be assessed	Needed to build an understanding of infrastructure and ascertain the presence of assets, their accessibility and connectivity
	Asset Importance	Needed to establish the value of an asset to the business and the overall impact if compromised	Needed to determine high-value targets with data that can be resold or used for other purposes
	Attack Vectors	Needed to understand the type and number of risks associated with each asset	Needed to understand which exploits are available and the best choice for a particular asset
	Exploitability	Needed to quantify the total risk of each asset's attack vectors	Needed to quantify the amount of work required to compromise a targeted asset

Once attackers target your organization, they will continuously probe your assets and defenses over an extended period of time to determine the weakest points in your infrastructure. Essentially, they are documenting the attack surface of your IT assets, connectivity and security tactics, from on-premises to the cloud.

Like hackers, your security team should use the information defined in the five dimensions above to enable visibility into the entire attack surface across all of your assets and infrastructure.

Attack Surface Visibility

Assessing risk is the foundation of IT security. Many security industry best-practices models, including the Gartner Continuous Adaptive Risk and Trust Assessment (CARTA) strategic approach, identify the need to continuously discover, monitor, assess and prioritize risk as the basis for establishing and maintaining a good security posture.

Attack surface visibility provides the foundation that your IT and security personnel needs to determine which assets present the biggest risks to the business. Using this information, corrective action can be taken to resolve any high-impact and easily exploitable vulnerabilities and attack vectors, and reduce or eliminate their risk.

Attack surface visibility from the attacker point of view enables you to improve your overall security posture by providing the context needed to understand the extent to which your business operations would be impacted by a successful attack on one or more assets. Instead of following reactive security plans and policies, your security teams can define and implement a stronger approach that is centered on eliminating the greatest threats and risks to your entire enterprise. Attack surface visibility is really a game-changing capability as it prevents the typical piecemeal approach of “find a vulnerability, fix a vulnerability” that wastes resources and precious budget.

By understanding the extent of your IT risk exposure through attack surface visibility, your security teams are able to circumvent attacks or counteract and minimize the effects. Attack surface visibility in combination with thinking like an attacker ensures that your enterprise has:

Comprehensive Assessment

- Able to fully discover and document any attacker-exposed assets no matter their location
- Able to immediately detect any new assets (e.g. virtual, physical, SaaS, IaaS) brought online, their location, owner and status
- Able to continuously update the state of your IT infrastructure

Situational Awareness

- Able to document attack vectors for any IT asset across your entire IT portfolio from on-premises to the cloud
- Able to determine the extent of exposure and risk associated with a threat or combination of threats by individual asset, by line of business, across the entire enterprise
- Able to derive and view all attack vectors that apply to a particular asset or set of assets used by an important line of business

Focused Security and Compliance Initiatives

- Able to visualize threat and risk characteristics dynamically
- Able to prioritize resolution of security gaps that present the greatest risk to your enterprise
- Able to gain insight into compliance with internal policies or with external security standards such as the Payment Card Industry Data Security Standard (PCI-DSS) or the Health Insurance Portability and Accountability Act (HIPAA).

In the end, it is all about information; who has it and who uses it to their advantage. Seizing the initiative from hackers by knowing your attack surface better than they do will significantly increase the difficulty of a successful attack. In fact, it may actually cause hackers to retreat.

CYCOGNITO

420 Florence Street
Palo Alto, CA 94301
cycognito.com

CyCognito provides solutions that identify and eliminate shadow risk: risk that IT and security teams are blind to, but sophisticated attackers actively target. The CyCognito platform is a fully automated next-generation security risk assessment solution that enables leading companies to discover, understand, prioritize and eliminate their organization’s shadow risk wherever it is, including cloud, partner and subsidiary environments.