CISO BRIEF

CYCOGNITO

Start with Attack Surface Visibility for Better Cybersecurity

Attackers Understand Your Attack Surface. Do You?

Attackers look for the path of least resistance in your attack surface so that they can break into your organization's high-value digital assets. They are looking for entry points that your organization doesn't see; this is your "shadow risk." To eliminate your shadow risk, you need ongoing visibility of your full attack surface, and there's only one proven way to get that: perform reconnaissance across your entire IT ecosystem, adopting an outside-in approach.

How much of your IT ecosystem – 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.

What is an attack surface?

Your attack surface is the group of your attacker-exposed assets, known and unknown, wherever they are: in the cloud, in third-party environments, or in your subsidiaries.

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 and your security teams are dealing with ever-increasing gaps in the information they need to secure your enterprise assets, where every small misconfiguration has the potential to open up access to your customer data, financial information and systems, application source code and intellectual property.

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 impact 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.

There are literally hundreds of solutions available to discover and document what assets are in your IT infrastructure. But these asset management solutions neglect a tremendous amount of your attack surface. 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 your partners use to connect with you, or the assets belonging to your own subsidiaries. And, they cannot identify assets that are abandoned, yet which remain a part of your attack surface and expose you to threats.

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.

Critical Information for Mapping Your Attack Surface

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

1. **What Are All My Assets?**
   What are all the assets, including partner assets, that are part of your extended IT ecosystem?

2. **Just How Important Is An Asset?**
   What business applications and data are on the asset, and who is the asset's likely owner?

3. **What Are The Risks?**
   Which threats are applicable to an asset?

4. **How Much Risk?**
   What is the chance of a cyberattack occurring?

5. **How Current Is My View?**
   How long has it been since the last update?

You Don't Know What You Don't Know

Having a cybersecurity plan in place is meaningless if your IT and security organizations are not aware of all of the assets and resources your organization needs to secure and protect. IT asset management and security assessment solutions seem like a natural starting point for establishing attack surface visibility but leave your organization with significant blind spots.

Use Attack Surface Visibility to Build Your Cybersecurity Foundation

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.

Establishing attack surface visibility from the attacker point of view enables you to improve your overall security posture. It provides the context you need to understand how your business operations would be impacted by a successful attack.

By understanding the extent of your IT risk exposure through attack surface visibility, your security teams will be able to circumvent attacks or counteract and minimize the effects. Full visibility to your attack surface from an attacker's point of view ensures that your enterprise has:

- *Comprehensive Assessment to continuously discover and detect attacker-exposed assets*
- *Situational Awareness to determine the extent of exposure and risk associated with threats across your entire IT ecosystem*
- *Focused Security and Compliance Initiatives that dynamically prioritize the resolution of security gaps that present the greatest risk to your enterprise so that your security investments are aligned with those risks*

In the end, it is all about information; who has it and who uses it to their advantage.

Contact CyCognito to learn how you can increase your attack surface visibility and identify and eliminate your organization's shadow risk.

CYCOGNITO
420 Florence Street
Palo Alto, CA 94301

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 brands to discover, enumerate, prioritize and eliminate their organization's shadow risk wherever it is, including cloud, partner and subsidiary environments. To learn how CyCognito can help you eliminate shadow risk, please visit CyCognito.com.