How ethical hackers can help to increase your attack surface visibility

BY ANNA HAMMOND · FEBRUARY 21, 2022 · LAST UPDATED ON MARCH 6, 2025

200 years after the first design for a Panopticon, some security experts still dream of safeguarding the security of an entire institution from a single, centralized viewpoint.

They are looking in the wrong direction. Cybersecurity teams who want to achieve comprehensive attack surface visibility should be looking to the future, not the past. Today, crowdsourced cybersecurity is rapidly becoming the most viable way to maintain a clear overview of security threats.

Understanding your attack surface visibility

What is an attack surface?

Your attack surface is the totality of connection points available to a malicious hacker seeking unauthorized access to your devices, systems, or networks. The hacker will be trying to steal or compromise your digital assets. These assets might include customer and financial information, intellectual property, and other sensitive data. Systems functionality is another area of attack through ransomware and Denial of Service Attacks (DoS).

What is attack surface *visibility*?

Attack surface *visibility* describes how complete an overview a security team has of its cybersecurity risk. Maintaining strong attack surface visibility is critical in risk prioritization and mitigation.

The volume of digital assets produced continues to grow rapidly. Meanwhile, devices, systems and networks have become increasingly interconnected with the advent of cloud computing.

As a result, attack surfaces are expanding at a rate Edwin Hubble might have recognized, leaving you feeling you need a tool as powerful as his eponymous telescope to keep an eye on what is going on.

Challenges in gaining visibility

The daunting frequency of cyber attacks and their astonishing economic impact ($3.92 million on average in 2021 according to IBM), make it essential to formulate an executable strategy to maintain attack surface visibility for your entire IT ecosystem over time.

Two of the most common strategies for increasing cybersecurity visibility include automated vulnerability scanners and pentests. Both however present problems for *continuous* security testing.

Automated solutions are too narrow in the scope of what they test. Yes, they can reliably offer visibility of your digital assets and of *known* vulnerabilities. However, they have no capacity to expand into the gray areas of your attack surface. Unfortunately, this is where malicious human hackers will be seeking most actively to discover exposed assets and *unknown* weaknesses.

And while a pentest *can* test for a greater range of security risks, they are costly and only offer a single snapshot in time. They can't affordably assess changes in infrastructure or threats at the pace at which they mutate.

So how can you square this circle of protecting against threats you aren't aware of? Is there a tool that can do this?

Benefits of continuous security testing

One answer to this perplexing question is to ask experienced hackers how they would try to break through your organization's cybersecurity defenses.

The rather obvious drawbacks of enlisting criminals to enforce your cybersecurity, however, can be overcome. Fortunately, there exists a global community of white hat or ethical hackers willing to hunt down weaknesses in your attack surface without running off with your digital assets.

If that sounds almost too good to be true, these hackers are strongly motivated professionals who are appropriately rewarded for their work.

Moreover, this preventative ethical hacking can be made incredibly secure for your organization as part of a crowdsourced bug bounty program managed by a platform provider.

Crowdsourced cybersecurity brings a number of benefits to continuous security testing:

Continuity – A bug bounty program can run continuously in order to reveal both known and new vulnerabilities on your attack surface over time.

Affordability – Crowdsourced ethical hackers only earn a reward or payment if they expose new, actionable and in-scope bugs. This makes bug bounty programs very cost-effective.

Scalability – Using a dedicated bug bounty *platform* allows you to quickly broaden the scope of your security testing as the need arises.

Proactivity – Ethical hackers are the good guys who can think like bad guys. They proactively create new approaches to discovering unknown vulnerabilities and report what they find responsibly to the stakeholder. And they do so *before* malicious hackers can make the same discoveries.

Attack surface management

The process of managing attack surface visibility and risk prioritization is a complex one that your organization will develop over time. Nonetheless, there are some attack surface management best practices that help ensure you minimize your risk of suffering a damaging attack.

To summarize, consider the four key steps to establishing good cybersecurity:

- Assess (or "discovery phase")
- Test
- Validate

- Patch

One of the advantages of hosted bug bounty programs is that their benefits extend beyond just the discovery phase into all four areas.

For example, crowdsourced ethical hackers both assess and test your defenses. And if you are using a bug bounty *platform,* the SaaS provider will often provide triage services to validate the hackers' reports. This can save you a great deal of time spent on doing your own validation.

Moreover, some bug bounty platform providers also provide (optional) recommended solutions to help you patch discovered vulnerabilities. This is also a huge time-saver and a great learning resource for your cybersecurity team.

Bug bounty programs are adaptive and scalable

Once you've established comprehensive attack surface visibility, and have mitigated risk through testing and patching, you should assume that cybersecurity needs to be adaptive and cannot be safeguarded from the viewpoint of a single point in time.

This is the best-practice approach of many leading industry frameworks. Following **Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA)** lead, they assume that risk and trust are dynamic and ever-changing.

Bug bounty programs align perfectly with this way of thinking. They can be run and reconfigured indefinitely ensuring your security posture is up-to-date and appropriate for evolving risks. Scalability is built-in through the platform and testing is on-going 24/7 by real human hackers.

Closing thoughts

Maximizing attack surface visibility requires a comprehensive approach, that can be executed and adapted over time.

A bug bounty program directly addresses this need while providing uniquely proactive testing from white hat hackers who constantly try new ways to discover weaknesses in your attack surface. It's on-going, affordable and very secure when undertaken through a bug bounty platform, like Intigriti.

Intrigued by what you have read? Want to know more about bug bounty programs? Get in touch to **request a demo** with a member of our team today.