Attack surface management best practices: Intigriti's top tips

BY ANNA HAMMOND · JANUARY 12, 2022 · LAST UPDATED ON MARCH 6, 2025

While the cultural stereotype of a hacker sitting in front of a monochrome CRT tapping obscure terminal commands makes for interesting fiction, the damage real hackers do is far less entertaining.

In this article, Intigriti discusses attack surface management best practices that help organizations stay one step ahead of malicious hackers. We'll explain how using crowd-powered security testing is an effective way of discovering and fixing vulnerabilities before bad actors do.

What is an attack surface?

Your attack surface is the totality of connection points open to a malicious hacker seeking to get into your devices, systems, or networks. Poorly maintained or untested attack surfaces are red rags to highly motivated "black hat" hackers seeking unauthorized access to your networks and devices.

These malicious hackers are intent on doing damage, stealing data or—increasingly—locking control of systems through ransomware. Through attack surface management, you decrease the chances of falling victim to a successful attack. In other words, prevention is better than cure.

The risks of poor attack surface management

First, there's the quantifiable harm done in terms of money and time. Hackers commonly steal valuable information (financial, intellectual property, customer records, etc.) or install ransomware to extort money. With the median cost of cybercrime incidents in Europe now at €50,000, the stakes for organizations are huge.

Second, less easy to quantify but equally important, is the reputation hit to a hacked organization. The loss of trust can be devastating for a business and their mission, especially when hackers weaponize their assets against them. In recent years, the Equifax breach and "Climategate" are illustrative of how damaging this can be.

In both cases, businesses that take steps to manage their attack surface will help minimize these risks.

Standard security practices aren't enough

Cybercrime has grown by a daunting 60% since 2013, according to McAfee. Plus, in 2019, Accenture and others estimated that $5.2 trillion in value would be lost over the following five years due to cybercrime. Much of the context for this unprecedented growth is the fast-evolving application landscape. The proliferation of devices and software has inevitably led to more security vulnerabilities being exposed.

In such a context, standard attack surface management practices, like firewalls, endpoint security scanning and software patching, are a must. However, a dependency on these *reactive* security measures

has an inherent weakness: they only test for *known vulnerabilities.* Meanwhile, malicious hackers grow ever more inventive, and with a $5.2 trillion incentive, you can assume bad actors are constantly working to discover *unknown attack surface vulnerabilities.*

A race to the unknown

To defend against these evolving threats, you must be *proactive* in discovering unknown vulnerabilities on your attack surface *before* malicious hackers potentially could. This requires the ability to think like a "black hat" hacker to pre-empt their attacks.

Thankfully, there is a strong global community of **"white hat" ethical hackers** who can help you do just that. The 2021 Intigriti **Ethical Hacker Insights Report** defines an Ethical Hacker as a "security expert that specializes in the testing of computer and software systems or processes to evaluate, strengthen and improve security."

Just like malicious hackers, they're driven by the overriding goal of breaking through a target's system defenses. However, an ethical hacker always operates within the law and discloses vulnerabilities only to the companies they work with instead of exploiting them.

Key Steps in Attack Surface Management

Break attack surface management into two steps: assessment and management.

Assessing your attack surface

Understanding which areas of your attack surface represent real risk is the first step in securing your infrastructure. To implement best practices, you need a clear idea of every device/software and user/login on your network, as well as the level of risk they represent in terms of exposing your digital assets.

This assessment must also include all third-party integrations. Many organizations have rapidly adopted tools like Slack, Microsoft Teams, Trello, Zoom, etc., during the pandemic. It's critical to know what information they would expose to a successful attacker.

For enterprise-level organizations, maintaining an up-to-date list will be a challenge in itself—but it is necessary. Given the proliferation of highly incentivized bad actors, it's best practice to take the approach that what you're not monitoring will eventually become an exploited attack vector.

It's also important not to fall into the trap of focusing solely on the technological to the exclusion of human error. By **some estimates**, identity-based attacks are responsible for 81% of data breaches. Make sure you have **the complete picture** of what you need to secure—but remember to consider humans as well as devices!

Managing your attack surface

While it's impossible to detail every security measure or tool available in an article of this scope, the following core steps should be implemented by organizations of all sizes:

1. Keep all software on all devices up-to-date

2. Provide security awareness education for staff
3. Require standard protocols like two factor authentication and unique passwords
4. Run automated security measures such as endpoint protection and firewalls
5. Perform penetration tests (pentests)
6. Run bug bounty programs.

Remember that endpoint protection is only effective against attacks based on known vulnerabilities and methods. Likewise, pentests focus on one moment in time, and fall short of providing an on-going assessment of your evolving network. They also require significant budget.

Best practices will require on-going security measures that can prepare for unknown threats. This is precisely why bug bounty programs are critical to reducing your attack surface.

Bug Bounty Programs

Bug bounty programs provide several unique advantages over all other security measures. For example, they bring:

1. Trusted human experts that can think like malicious hackers

To uncover both known and unknown weaknesses before malicious hackers can exploit them in your infrastructure, you need all the skills and inventiveness of a "black hat" hacker without their malicious intent. "White hat" hackers, incentivized by bounties, provide this expertise.

2. The power of crowd-sourcing

Another name for bug bounty programs is "crowd security testing", and it makes perfect sense. Once you launch a program, you'll have **large numbers of expert minds** simultaneously trying to discover weaknesses in your IT security—but without any risk.

As Thomas Colyn, an award-nominated security specialist and CISO of DPG Media, **makes clear**: "I can use the creativity of thousands of ethical hackers' minds through Intigriti [bug bounty programs]—and that is far stronger than using automation or general algorithms to discover difficult to find vulnerabilities."

3. On-going tests

IT systems and solutions change frequently. Bug bounty programs provide on-going testing of your systems' security in a way one-off testing cannot. You can't run a pentest after every patch, but you can be sure your bug bounty team will be looking for new vulnerabilities.

Colyn again spells out the benefits: "At each moment, someone is trying to find a vulnerability, which is one of the biggest differences between pentesting and bug bounty."

4. Time-saving triage

Few organizations have dedicated IT security departments. Those that do are frequently overstretched. Bug bounty platforms, like Intigriti, allow you to leverage customer support and a triage team. These

expert agents are constantly on-hand to review and screen incoming vulnerability reports so that you are only notified about what is relevant, valid and in-scope.

5. Scalable security

Running an on-going bug bounty program allows you to rapidly scale your IT infrastructure and security testing simultaneously. Security teams become aware of vulnerabilities and potential fixes much faster than with standard security measures.

6. Public or Private—you choose

If the thought of going public with a bug bounty program is overwhelming, private bug bounty programs like those optionally offered by Intigriti are a great way to get started with crowd security testing without public exposure.

Closing thoughts: Attack surface management is an ongoing responsibility

From small businesses to enterprise-level companies, every modern organization needs an effective attack surface management strategy in place. A key part of this strategy will be to recognize that protecting your digital assets from highly incentivized “black hat” hackers is an on-going task.

Bug bounty programs provide an effective method of continuously responding to ever-evolving security threats. Engaging the skills of “white hat” hackers to safely target your system defenses with the same level of inventiveness as the “black hat” hackers should be a cornerstone of your attack surface management strategy. The good news is it’s easier than ever to get started thanks to bug bounty platforms like Intigriti.

Want to learn more about bug bounty programs?

If you’d like to know more about integrating bug bounty programs into your security best practices, we’d love to hear from you. Get in touch to request a demo with a member of our team today.