Improve your cyber risk posture with Cybertrust External Asset Attack Surface Management

cybertrust

cybertrust.eu

Context

Two decades ago, the majority of organizations had a limited number of assets connected to the internet, primarily residing on on-premises servers. These assets were usually few in number and remained consistent over time, making them easy to monitor and oversee. And at the time, comparatively few vulnerabilities existed, so remediation was also a manageable task.

However, the manner in which we utilize the internet has undergone a significant transformation. Presently, developers continually generate fresh websites and applications to fulfill evolving business goals. Marketers extensively employ third-party scripts and services across various websites to enhance user experience and obtain comprehensive reports. Furthermore, unlike previous times, a majority of data is now hosted on cloud platforms such as AWS and Microsoft Azure.

Now that organizations have hundreds, if not thousands, of internet-facing assets it's become extremely difficult to keep track of the constant changes and ensure security. To an attacker, each connected asset can serve as a pathway to sensitive information.

As security teams struggle with the challenge of strengthening their systems, cybercriminals are amassing significant wealth through successful cyberattacks, continuously evolving in sophistication and capabilities. Operating on the underground network, these malicious actors collaborate in a nefarious marketplace, offering tools capable of exploiting vulnerable assets and accumulating vast reserves of resources to target businesses worldwide.

Major issues and risks organizations face

1. Lack of asset visibility
2. Unknown usage of Shadow IT
3. Lack of awareness and knowledge of risky assets
4. No single view of assets
5. Inability to prioritize
6. Labour intense auditing and compliance efforts
7. Inhouse shortage of cybersecurity expertise
8. Outpaced by cybercriminals

> “***70% of organizations don't know what assets their organization has****, despite governance IT frameworks providing guidance on IT asset management and numerous solutions on the market for managing IT infrastructure.*”
>
> — Source: Gartner 2022

Gain Visibility into the risks of your Digital Assets with Attack Surface Management

The attack surface is the collection of every internet-facing asset associated with a business that, if not properly secured, can provide entryways for an attacker looking to access sensitive data. Assets are things like web applications, servers, networks, firewalls, third-party tools, and certificates. In other words, everything internet facing that an attacker could use to breach a business makes up the attack surface.

So, attack surface management is a holistic, unified view and methodical way of keeping track of all internet-facing assets in a business to identify weaknesses that could leave it susceptible to an attack. Attack surface management breaks down into three recursive components:

1. **Discover** - Safeguarding the unknown is impossible; hence, the initial phase of attack surface management involves identifying and categorizing every asset connected to your business. Discovery must be an ongoing process since new assets can emerge and become operational at any given moment.

2. **Fingerprinting** - Once the discovery process brings your assets to light, the next step is to gain a comprehensive understanding of their characteristics and configurations to pinpoint potential vulnerabilities that might entice attackers. This thorough examination, often referred to as fingerprinting, entails identifying the technologies employed, the contents stored, and the associations with third-party entities. Furthermore, it involves uncovering vulnerabilities present at the firewall, server, or application layer. By cataloging this valuable information, you can gain a holistic view of where your risks materialize, enabling a clearer understanding of the bigger picture.

3. **Monitoring** - Developers frequently introduce modifications, while new vulnerabilities are consistently discovered. Consequently, it becomes imperative to maintain continuous monitoring of the attack surface to promptly identify any issues and prevent potential risks from slipping under the radar.

> “*Average of 68 new vulnerabilities a day disclosed in 2022.*”
>
> — Source: Tenable

Step by step approach to an improved risk posture

In order to protect your business, you need to have complete visibility into your digital assets and attack surface. Only then can you identify and mitigate the risks posed by cybercriminals. With this information, you can quickly identify and mitigate the risks posed by cybercriminals.

Cybertrust recommends the following **step-by-step approach** to testing and monitoring the security of your attack surface.

- ✓ Discover and identify your attack surface
- ✓ Analyze and reduce exposed services
- ✓ Identify, prioritize, and remediate asset vulnerabilities caused by outdated software and misconfigurations
- ✓ Discover web application issues, prioritize and apply best practices
- ✓ Use automated testing to discover errors that create security risks
- ✓ Use manual testing to find issues automatic methods can’t
- ✓ Generate approved reports for compliance

> *“With the increasing use of technology in our daily lives, cybercrime is on the rise, as evidenced by the fact that cyberattacks caused 92% of all data breaches in the first quarter of 2022.”*
>
> — Source: TheHackerNews

What to look for when choosing an Attack Surface Management Solution

With the help of the right solution, attack surface management isn't complicated. Here are the important things to consider when evaluating which solution is best for your business.

1. **Centralized viewpoint**
   Being able to see the status of your entire attack surface in one location is of the utmost importance. This allows you to monitor, prioritize and protect your assets with fewer things slipping through the cracks. Always remember that cybercriminals aren't just targeting your most secure and best-monitored assets, they're targeting anything they can find.

2. **Prioritization based on risk**
   Make sure you're always moving towards a risk-based approach to cybersecurity. Focusing on remediating vulnerabilities that pose no risk can distract you from what matters most.

3. **Continuous monitoring**
   If you're working off outdated information, you're leaving yourself vulnerable. Continuous monitoring is the key to identifying and eliminating attack vectors before they can be exploited. Regular scanning, discovering, and testing will help you stay ahead of the bad guys.

4. **Flexible integration with existing IT management tools**
   The "too many tools" problem is addressed if the solution can readily integrate with existing tools that are relied upon by others in security and IT.

5. **Contextual understanding of the relationship between assets**
   Security operations need a complete picture of what is happening with the elements of their attack surface to respond properly. Failure to do so can endanger either the security goals or business operations by doing too little or too much in response to a risk or threat.

6. **Tracking and reporting capabilities**
   We know executives don't want to wade through the details of every vulnerability fixed or target eliminated. Using simple, trackable risk scores and predictable methodology can help your teams get on the same page to reduce the cyberthreats that can devastate your business.

7. **People you trust**
   Tools are great, but having experts on hand can give you insights from outside your organization and knowledge base. Make sure you can work with your provider to develop a customized plan based on the principles laid out here and the unique requirements of your business.

How Cybertrust can help

Cybertrust gives you a 360° view of your online risk posture. See the real-time security status of your entire digital landscape and always stay ahead of hackers.

1. **All-in-one solution**
   We've brought together everything you need to manage your external risk in one platform, from Attack Surface Discovery to Website Monitoring to Penetration Testing. The Cybertrust Security attack surface management service offers a centralized dashboard that brings your top issues to the forefront.

2. **Organized for actionability**
   We compile the data we find in an easy-to-use dashboard that's designed to help you identify anomalies, inconsistencies and misconfigurations on your attack surface. Risk scores show you where your attention is needed most, so you'll never wonder where to get started.

3. **Continuously updated for changes**
   Our services are designed to monitor your attack surface on a continuous basis. You can schedule scans on a timeline that works for you, or you can run a scan on demand. Easily track changes over time in your dashboard to spot risks as soon as they arise.

4. **Experts ready to help**
   Cybertrust experts strives to be an extension of your security or IT team. Our experts are here to help you prioritize work, assess your security posture and understand every vulnerability.

5. **Pricing that scales**
   Our pricing is always straightforward and transparent. We charge based on the number of targets you want to monitor, with additional pricing for add-ons that give you full visibility into your security.

6. **Continuously improve your security posture**
   As your security posture strengthens, Cybertrust helps you not only maintain it but improve it, adopting internal or industry frameworks to ensure systems are continually improving through automated assessments. Automated queries continuously identify security coverage gaps and control drift, keeping security focused on new and emerging challenges.

Get started today and secure your attack surface

Are you one of those who's feeling stressed by your current state of cybersecurity asset management? Cybertrust experts are standing by to help you customize your security testing and monitoring strategy.

Cybertrust is a specialist in helping organizations to improve their cybersecurity strategy and risk posture in a sustainable way which can adapt along with the digital transformation of your organization now and towards the future.

Get in touch and schedule a free consultation today.

I cybertrust.eu
M contact@cybertrust.eu

Sustainable Cybersecurity

Cybersecurity sustainability means investing time, attention and capital in a way that mitigates risk, minimizes cost and maximizes effectiveness both now and in the long term.

With our consultancy services we can help to put these ideals into practice considering what sustainability looks like across the three pillars of security: people, process and technology.

cybertrust

SECURING THE WAY TO A SUSTAINABLE, RESILIENT FUTURE

Powered by CRONOS GROEP