Attack Surface Reduction

Bring down cyber risks and improve your security posture for seamless business continuity.

Understanding attack surface dynamics

Today's businesses are constantly becoming more digital and implementing new cloud technologies. Even further, businesses are serving customers globally, enabling employees to work remotely, interacting with vendors through different IT systems, and so on.

These factors contribute to an increase in the number of entry points to your IT systems, like web applications, email systems, third-party integrations and cloud services.

A total of all these entry points is referred to as 'attack surface.' Some of them have a vulnerability. A vulnerability could be as simple as a weak password or outdated software in use or the lack of the right encryption protocols.

As the number of entry points increases, the attack surface also grows. An attacker is always looking to get into your systems through one of the entry points by exploiting any vulnerability.

Any business with a large attack surface needs to be aware of and actively manage it to gain control. Hence, a business must see its entry points as an attacker would – and based on that knowledge, proactively reduce the security gaps and minimize the attack surface.

The need to minimize the attack surface

Businesses need to take stock of their attack surface to be aware of the different assets they have. Some will be familiar and managed, however there is a high chance of unknown and rogue assets as well.

Having such assets on the company network poses a huge risk for any organization. For instance, there could be data breaches arising out of an employee's unknown personal device connecting to the company network and accessing corporate applications.

This device may be exposed to risks – which any hacker might exploit to exfiltrate sensitive customer data or any other information.

This is just one downside of having an unmanaged attack surface, there are more:

- Difficulty for security teams to detect and respond
- Compliance risks due to unknown assets that don't comply
- The company's ability to protect data is lowered and hence might lead to lower trust among customers

In addition, a breach can cause heavy financial losses. Therefore, businesses must focus on reducing their attack surface.

Insights on attack surface and related cyber crime

- Attack surface monitoring is a top 10 priority for 98% of organizations
- Yet only 9% of organizations have tested 100% of their attack surface
- 68% of organizations have experienced an attack from an unknown, unmanaged asset
- 70% of attacks are perpetrated by external threat actors
- 1 in 10 of all detected internet-facing assets had an associated unpatched vulnerability

Source: Attack Surface Management Statistics, 2023

T Systems

Let's power higher performance

How T-Systems can help you in attack surface management

With the right tools and expertise, we help your business to reduce the attack surface. The following describes our proven and globally tested method to systematically reduce attack surfaces, which we've successfully implemented with numerous clients:

Holistic Assessment and Discovery

As a part of thorough assessment, we scrutinize your network and systems to discover various types of assets: known, unknown, rogue, etc. This process results in the development of a comprehensive inventory.

Asset Mapping and Analysis

We then analyze company assets. All assets are categorized according to their functions and criticality to business operations. Asset mapping also includes how assets are interconnected to each other. This helps us to understand resource allocation and to plan strategically.

Recommendations and Remediation

After identifying critical assets and potential security gaps, we prioritize vulnerabilities as per their criticality. Our experts guide you through the remediation process that focuses on correcting misconfigurations, updating software, addressing software bugs, fixing patches, closing security gaps, and more. We also offer recommendations that help you improve your security posture and avoid potential threats in the future.

Automation

We use advanced automation tools for asset discovery and vulnerability management. This helps us expedite the process and at the same time achieve greater efficiency in scanning of systems and large networks. Our accuracy levels are higher with the help of these automated tools.

Monitoring and 360-degree Visibility

After remediation and recommendation, we establish continuous monitoring – which allows visibility and high vigilance to detect and respond to potential security threats in real-time to ensure swift action.

Security Program Effectiveness

We offer mechanisms to measure the effectiveness of the attack surface reduction program. We help you to get a view of the attackable surface that has been reduced over the period along with the number of risks that have been decreased. This helps your business to make more informed security related decisions in the future.

Continuous Improvement

Our strategy for continuous improvement involves feedback loops and periodic reassessments, adapting to evolving threats in real time. By embracing a dynamic approach to reducing the attack surface, we ensure that your security measures adapt to the changing threat landscape. Stay one step ahead with our commitment to ongoing enhancement and adaptation.

How your business can benefit

- Enhanced security posture
- Reduced risk of data breaches
- Improved regulatory compliance
- Cost savings by decreased attack frequency
- Efficient and faster incident response
- Better reputation and greater customer trust
- Increased productivity
- Competitive advantage with solid security

Get a customized solution from our security experts to reduce the attack surface of your business.

Start a conversation with us today.

Expert Contact
Andreas Pecka
Head of International Expert Sales & Presales Cyber Security
a.pecka@t-systems.com

Published by
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
E-Mail: cyber.security@t-systems.com
Internet: www.t-systems.com

T Systems

Let's power higher performance

Last update: 01/2024 | Designed by: Creative Factory, TSIN