

5 Top Priorities for Attack Surface Management

Internet Attack Surface Management as a concept is gaining traction in enterprises across all industries. While relatively new, in many ways, it's a logical extension of what we've already been doing inside the corporate network for decades.

Traditional Security Practices

Traditional security teams strive to have a complete picture of the assets that constitute the digital world inside the corporate network; servers, applications, desktops, users, etc. IT governance policies specify best practices for each of these asset types, and security solutions monitor adherence and help automate ongoing maintenance of the environment as it pertains to security.

A close working relationship between security teams and other groups such as IT operations, application development, and operational risk has always been required to deliver the best security outcomes. In addition to these proactive security initiatives, most organizations deploy security monitoring solutions that look at the bigger picture. These solutions continually assess adherence to standards and draw attention to the activity that could indicate an active threat requiring investigation and response.

Today, most of these principles can be extended outside the firewall to ensure you're managing your entire attack surface.

External Threat Practices

The difference between the security landscape today and that of the past is that digital transformation initiatives have resulted in a vast array of digital assets across web, mobile, and social channels that are exposed on the internet, outside the protection of traditional security defenses.

However, as we mentioned, the management requirements of this internet attack surface are very similar to traditional security practices. Just like inside the network, we:

- Need to know what we own, and its adherence to governance policies.
- Must engage in regular maintenance.
- Should have excellent relationships with other departments to ensure that we're able to respond promptly to reduce our exposure.

Top Priorities:

1. Map your attack surface
2. Minimize your attack surface
3. Get compliant
4. Protect your customers
5. Get the most out of your other security programs

On top of these practices, regular security monitoring is required to assess adherence to standards and to identify and alert security teams if assets are compromised. But unlike traditional security practices (except for phishing emails), we also need to identify instances of impersonation and brand infringement used by cybercriminals to compromise employees and customers and take action to remove them.

While some organizations have developed a mature external threat program, others are just starting on the journey, evaluating the scope of their program and identifying where to start. For those organizations, we have identified five activities that will help build a solid foundation for any external threat program.

1. Map your attack surface

Today, it's crucial to understand what belongs to you and what you look like to customers and attackers. An organization's internet presence is comprised of known, unknown, unsanctioned, and often poorly maintained internet-facing assets.

Shadow IT, M&A, and a lack of standard commissioning processes mean that security teams have an incomplete view of their attack surface and its weaknesses. Regardless of their efforts, they can't protect what they don't know about. Attackers perform reconnaissance to find and exploit unknown, vulnerable, and unmonitored internet-facing websites, applications, forms, and underlying infrastructure. According to [Verizon](#) and others, 70% of all successful breaches today originate on the internet.

2. Minimize your attack surface

Once you've mapped your organization's attack surface, it's time to reduce it to make yourself a smaller target for hackers. First, your team must develop an accurate CMDB of internet exposed assets, enriching the information through tagging by country location, business unit, and owner. This exercise will enable you to improve your security posture systematically by addressing specific types of weaknesses, including:

- Frameworks
- Certificates
- Mobile apps
- Third-party components
- EOL infrastructure
- Critical CVEs
- Open ports

3. Get compliant

It no longer matters if an asset resides on the network or beyond the firewall. If it belongs to your organization, maintaining compliance with internal standards and third-party regulations is imperative. Already, organizations are facing fines for breaches that originate outside the firewall.

In the case of British Airways, their website was breached by the card-skimming crime syndicate Magecart, which appended their malicious JavaScript to steal credit card information from thousands of customers. Because of their lack of visibility outside their firewall, they were the subject of the first post-GDPR fine proposed to be £183m, which represents 1.5% of BA's 2017 revenues. To put this in context, the largest pre-GDPR fine levied by the UK's Information Commissioner's Office (ICO) was £500,000.

Going forward, more regulations will be put in place to protect customers from threat actors targeting businesses. Organizations must be able to stay within GDPR, OWASP, and internal compliance guidelines to remain compliant and avoid potentially devastating penalties.

4. Protect your customers

Your customers interact with your business outside your firewall and, as indicated by the massive GDPR fine against British Airways, you're responsible for their safety and online experience. This obligation includes protecting them from threats that belong to you but reside outside the network such as browser-based threats like cyptominers, malicious Injects, and Magecart.

However, this responsibility extends to assets that don't belong to you as well. These rogue assets are meant to mimic your brand and target your customers. Even though your organization did not develop them, they're nonetheless a part of your attack surface. These include typosquatting domains and subdomains, fraudulent mobile apps, phishing sites and pages, and infringing social media accounts.

5. Get the most out of your other security programs

As we mentioned, the first step in delivering a mature attack surface management program is to gain visibility of all assets that exist on the public internet. Then, curate that data such that it can be used by either the security team or the broader organization. Finally, monitor or audit those systems to ensure that any changes are accounted for and appropriately managed.

Organizations require rich internet data to be accessed automatically by their other security tools to add "outside the firewall" context to other security functions. By making this data available to existing systems and processes, organizations can bring internet visibility to a range of additional security and IT operations tools to enrich the information they deliver, accelerate response or mitigation and improve the organization's cyber effectiveness.

Some common applications are:

- **Pen-testing:** Having visibility and an always up to date inventory of exposed assets and their risks, pen-testing teams can focus their efforts on addressing the areas of the overall attack surface with the highest levels of risk.
- **Vuln-scanning:** Finding unknown assets and assets with weaknesses that indicate that they are a priority for scanning. As with pen-testing, you can only scan those assets your security team has visibility over.
- **SIEM enrichment:** A SIEM can only see as far as the edge of the corporate network because the data that feeds it comes from devices and applications hosted on the network. For malicious activities that originate on the open internet, SIEM correlation and detection may find the effect of a threat but often has no information with which to determine the cause. This is where outside the firewall visibility comes into play.

Due to cloud server migration, hosting and other digital media initiatives, millions of assets appear on the internet every day, and they're entirely outside the scope of firewalls and endpoint protection. A business's attack surface extends from the internal network to the farthest reaches of the internet, where attackers have all the visibility. Security teams are now responsible for defending this enormous swath of digital real estate with the same scrutiny as their internal networks.

Fortunately, despite this drastic increase in what security teams are now tasked with protecting, basic tenants of cybersecurity haven't changed. With the right tools, security teams can apply the same rules that keep their internal networks safe to their entire attack surface.

This is the first installation in a series exploring attack surface management and its application. Stay tuned as we explore setting up an attack surface management program and what your organization can do to get yours off the ground and fully optimized.



RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

✉ sales@riskiq.net

☎ 1 888.415.4447

Learn more at riskiq.com

Copyright © 2019 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 09_19