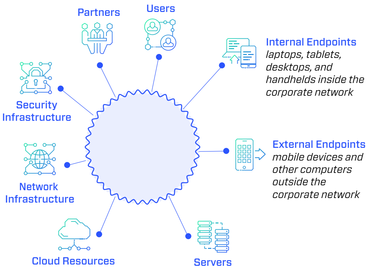
A Dynamic Attack Surface Requires Dynamic, Extended Security

It's time to focus on the bigger picture. An organization's attack surface is the total sum of all vulnerabilities in a device or network that an attacker can exploit to gain access and compromise the system or environment.

The aim is to keep the attack surface as small as possible and to actively manage all potential areas of vulnerability. But in today's hyperscale enterprise environment, where new assets are added as business demand requires, the strategy for managing the attack surface has become ever more unwieldy. Here, we review some of the considerations and best practices for managing your attack surface.

Surface Scope

An organization's attack surface includes all elements that can be used by an attacker to gain control of systems, networks, software, users, and assets.



The attack surface is complex.

The attack surface is constantly changing — new users, new systems or software, network changes, and security changes.

As much as 97% of all malware now uses a polymorphic technique to avoid detection by legacy AV. [1]

The attack surface is constantly growing.

Attackers Seek the Weakest Link

In order to gain access, an attacker will look to exploit the weakest link in the attack surface. In an ideal world, security teams would simply reduce their attack surface to virtually zero.

However, in today's hyperscale enterprise environment, where new assets are added as demand dictates, it's unrealistic to assume that enough action can be taken by the IT team to achieve this.

→ Organizations want to minimize their attack surface, but realize that the attack surface is constantly growing and changing. ←

Legacy AV is no match for unknown threats. Organizations cannot wait for the latest update or a threat to first be discovered, identified, and added to AV. Signature- and behavioral-based solutions that use a defined list are reactive and suited only to block yesterday's attacks.

Today the most dangerous threats are unknown—i.e., custom, brand-new (zero-day), or polymorphic exploits and payloads.

76% **of successful attacks** leveraged unknown and polymorphic malware or zero-day attacks.[3]

130 **breaches** per company per year.[2]

48% **of organizations** believed they could keep up with the new or emerging threats.[4]

To stay ahead of attackers, organizations need dynamic, proactive security that can identify previously unknown threats and harmful payloads before they can execute.

Other common attack surface tactics and how to defend against them

Memory Exploits

Potential file executions from possible unknown malware need to be analyzed in milliseconds before they have an opportunity to execute in the computing device's memory. A malicious payload may begin with a benign operation to fool security measures. Analysis should be rapid and deep enough to see downstream malicious actions.

Unauthorized Applications

Application control capabilities are a must as a next line of defense on purpose-designated servers and fixed-function devices. These need constant monitoring to prevent unauthorized apps from running or unauthorized use of a system.

Cloud Assets and Infrastructure

The cloud must not be a weak link in your attack surface. Cloud environments need to be protected from misconfiguration. The same security from on-prem resources needs to be extended to the cloud and provide consistent protection.

Reduce Your Attack Surface with AI-Driven Security Solutions

Try as they might, organizations will never be able to completely eliminate vulnerability. To manage the modern and dynamic attack surface, organizations need to ensure they have the right set of security controls in place that reduce the chance that an attacker can gain access.

With Cylance, organizations and their security teams rest easier, knowing that even if vulnerabilities go unpatched or they miss an update or two, their local, AI-driven endpoint security is helping to actively reduce their attack surface and proactively prevent breaches.

Learn more at cylance.com/why-cylance.

[1] Building an effective cyber defence against polymorphic malware
https://www.information-age.com/building-an-effective-cyber-defence-against-polymorphic-malware-123474759/

[2] Zero-days, fileless attacks are now the most dangerous threats to the enterprise
https://www.zdnet.com/article/zero-days-fileless-attacks-are-now-the-most-dangerous-threats-to-the-enterprise/

[3] The Cost of Cybercrime report, September 2017
https://newsroom.accenture.com/news/accenture-and-ponemon-institute-report-cyber-crime-drains-11-7-million-per-business-annually-up-62-percent-in-five-years.htm

[4] The Need for a New IT Security Architecture: Global Study on the Risk of Outdated Technologies
https://www.citrix.com/content/dam/citrix/en_us/documents/analyst-report/ponemon-institute-security-study-outdated-technology-risks.pdf