

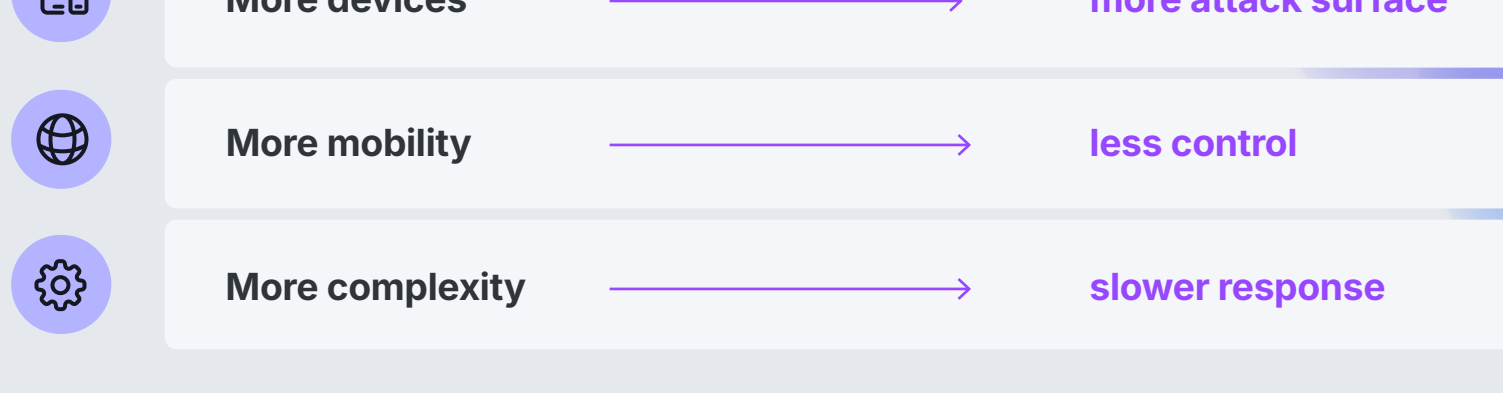


Security gaps are expanding. Here's how to close them.

Hybrid work, mobile devices and advanced threats have broken perimeter security. A layered approach is the way forward.

WHY LEGACY FAILS

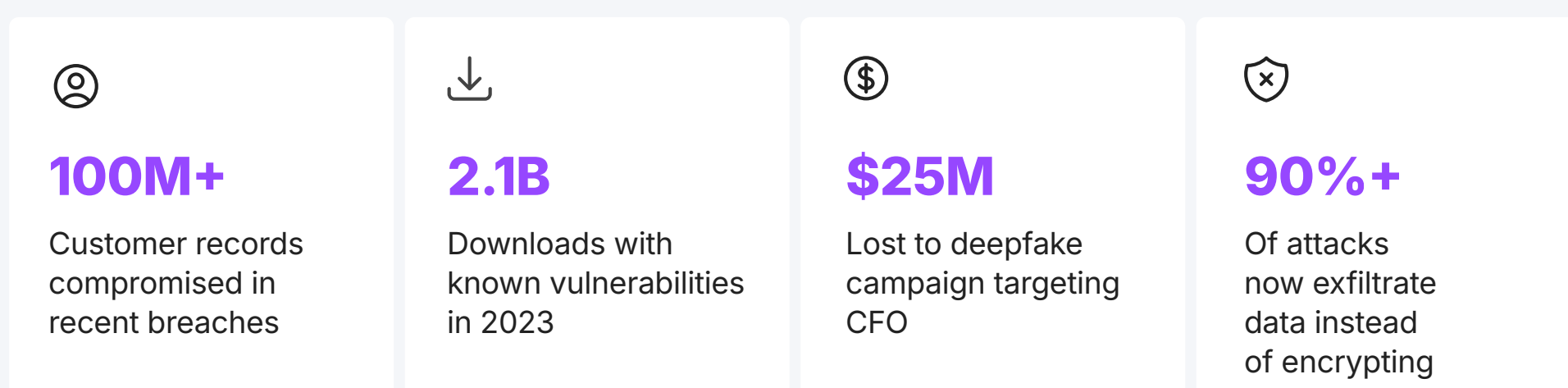
The **perimeter** is gone. The **risk** is not.



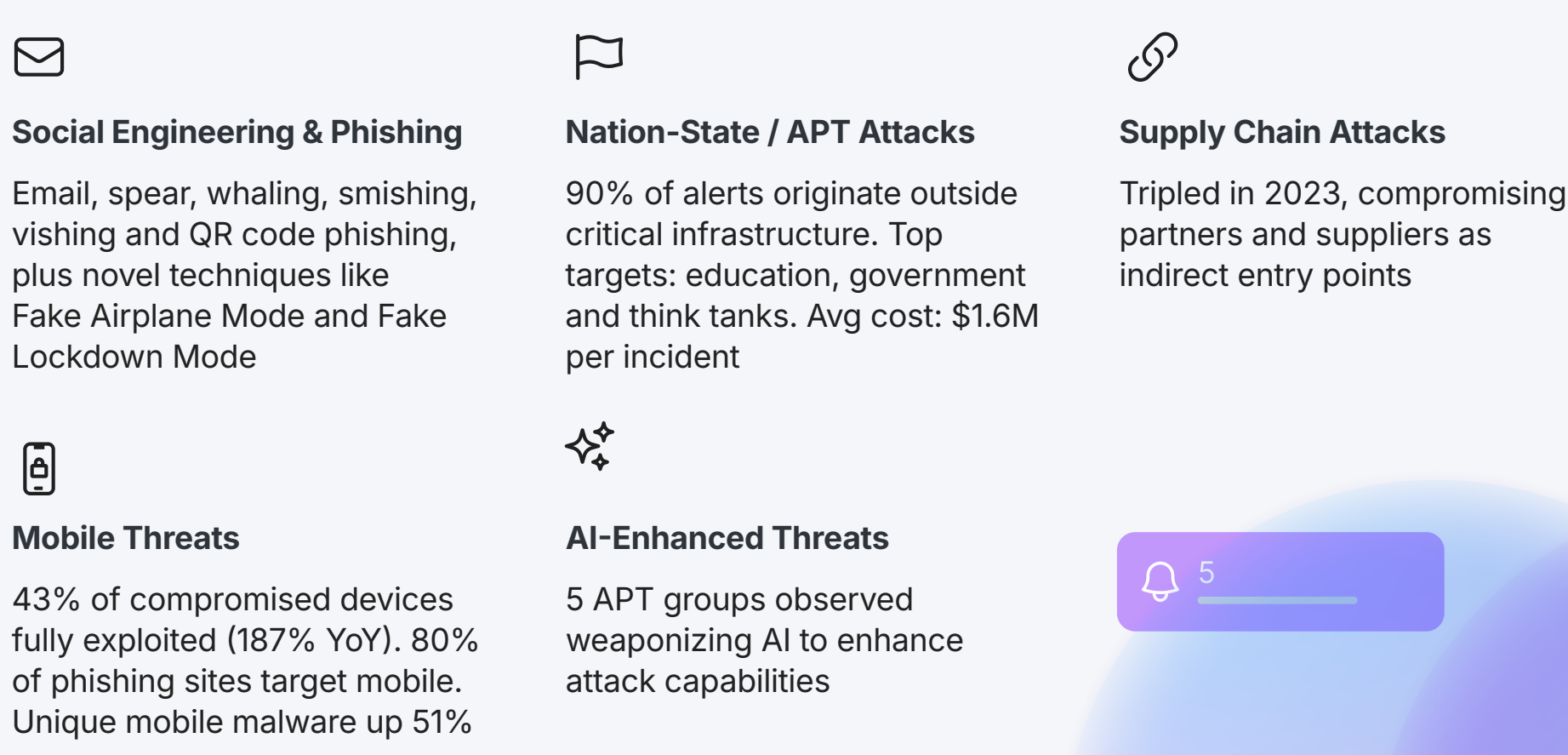
Cloud services, remote work, BYOD and untrusted networks have eroded the boundaries that legacy tools were designed to protect.

THREAT LANDSCAPE

Today's **threats** are sophisticated, converged and relentless.



KEY THREAT CATEGORIES



NATION-STATE THREATS

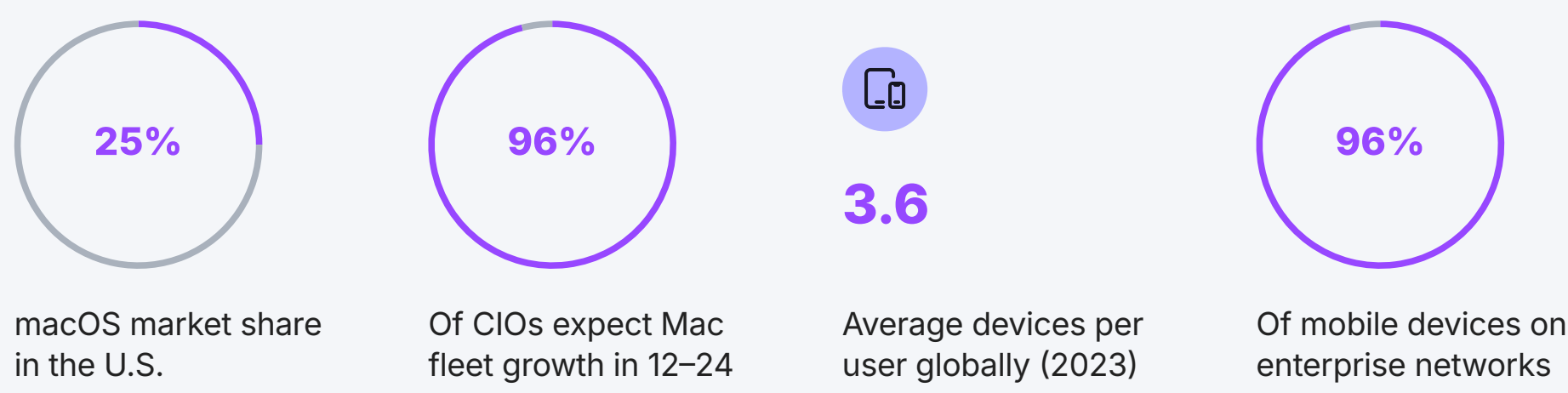
Targeted attacks by the numbers.



WHY ONE SIZE DOESN'T FIT ALL

The **device landscape** has **changed**.

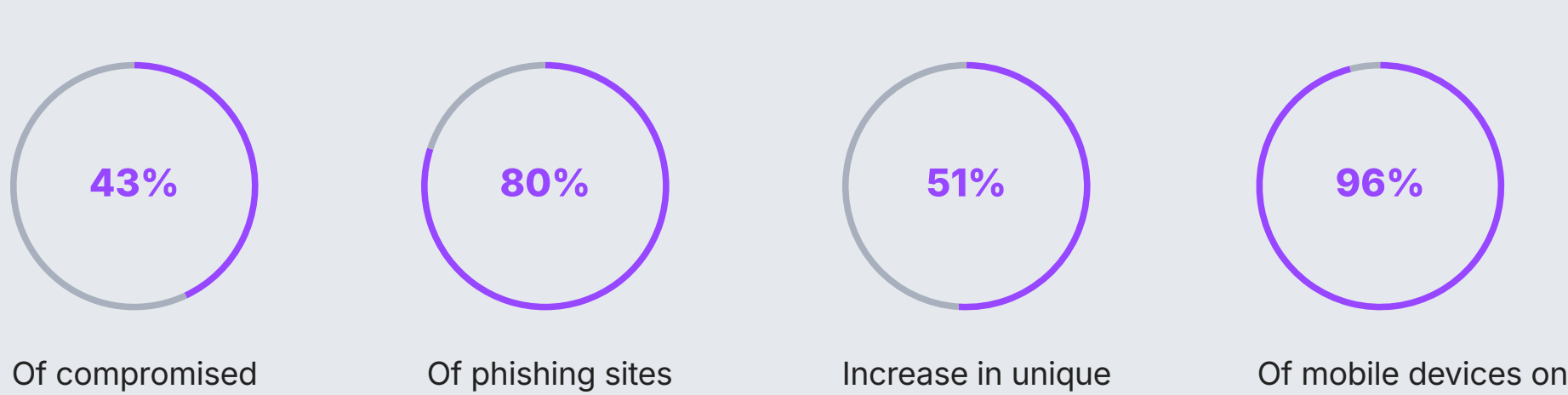
Legacy solutions designed for static, office-based desktops can't secure today's dynamic, multi-device environments.



MOBILE: UNCHECKED RISK

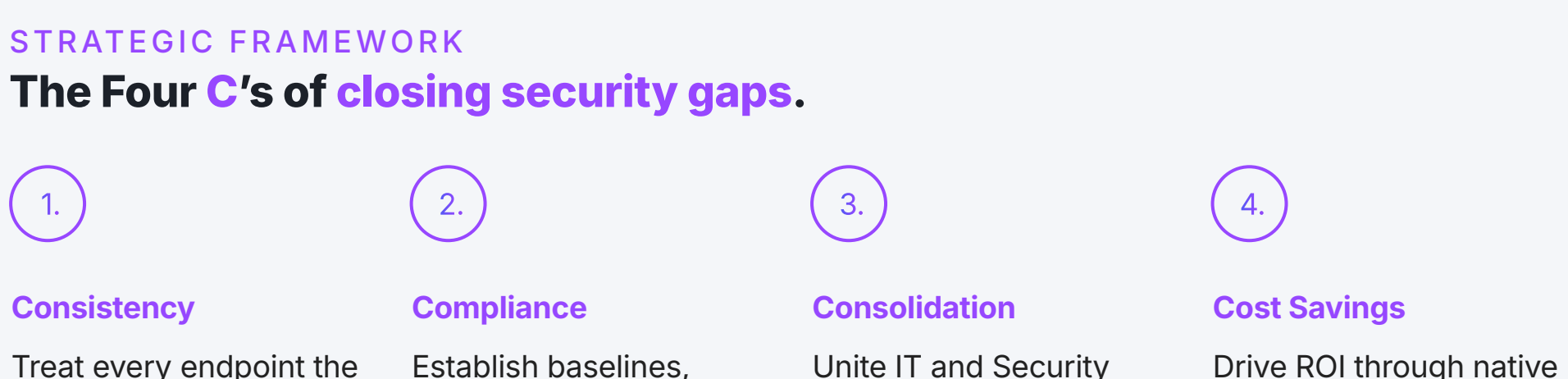
Mobile is the front door no one's guarding.

The average user has 3.6 devices. That's 4x the attack vectors per person, often with no specialized endpoint protection.



STRATEGIC FRAMEWORK

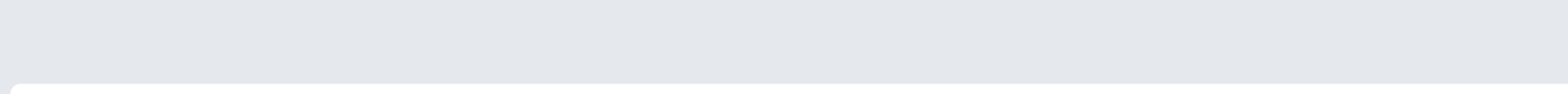
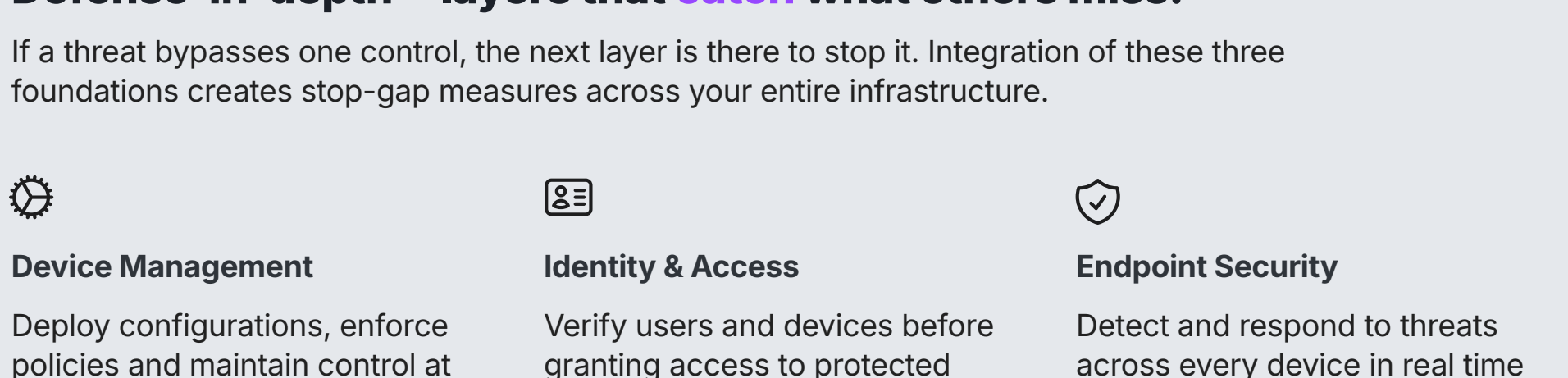
The **Four C's** of closing security gaps.



LAYERED SECURITY MODEL

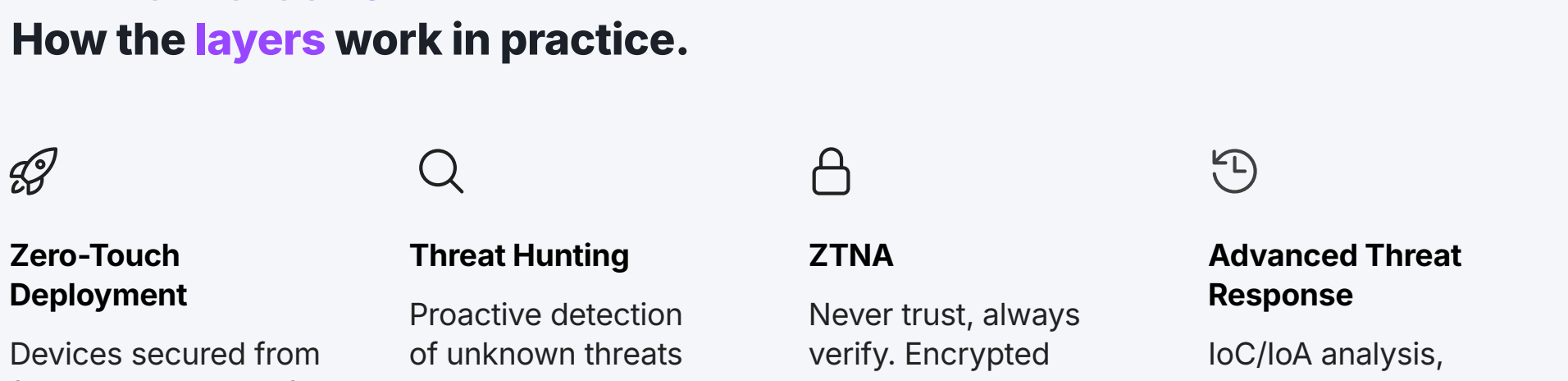
Defense-in-depth = layers that catch what others miss.

If a threat bypasses one control, the next layer is there to stop it. Integration of these three foundations creates stop-gap measures across your entire infrastructure.



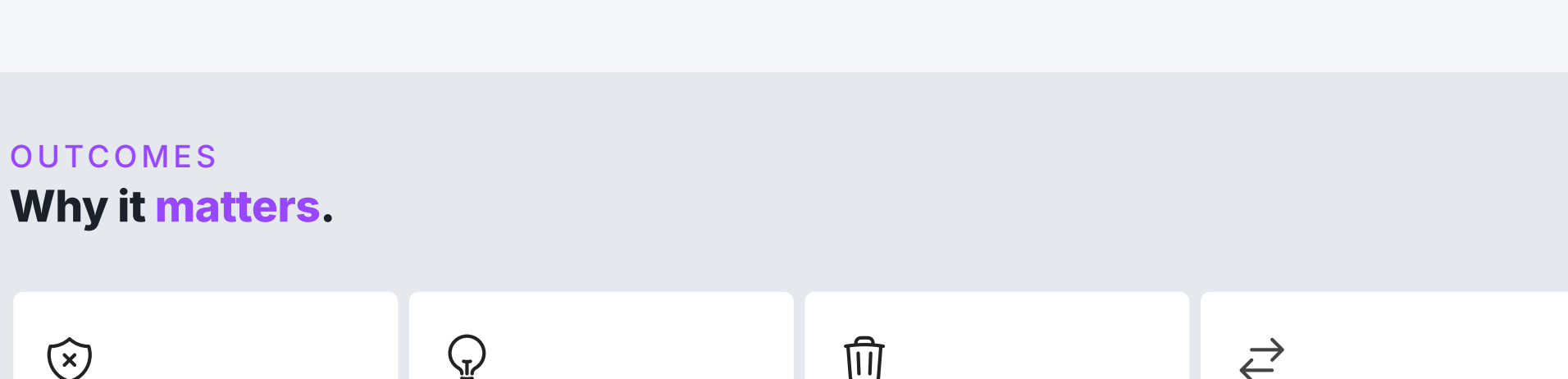
KEY TECHNOLOGIES

How the **layers** work in practice.



OUTCOMES

Why it **matters**.



Explore the full framework for building integrated, layered security across your organization.