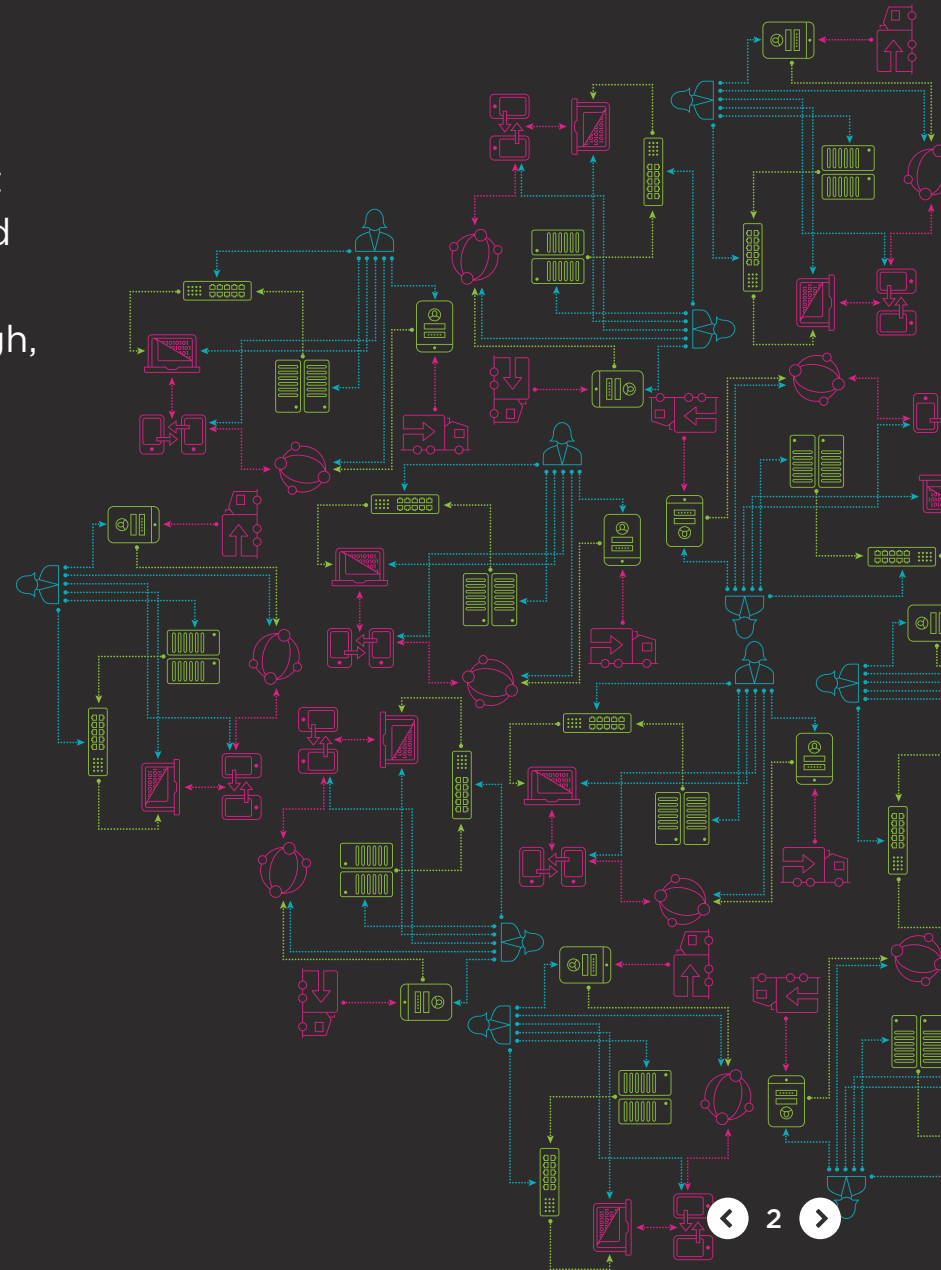


INTRODUCTION

If you were to look at a map that showed computer security as a whole, from a high enough vantage point it might look like art. The blend of arrows, symbols and colors bunched up against serious-looking acronyms would take on an abstract quality. But get close enough, and the overwhelming detail and scope of this map would seem like an endless and incomprehensible maze of information.

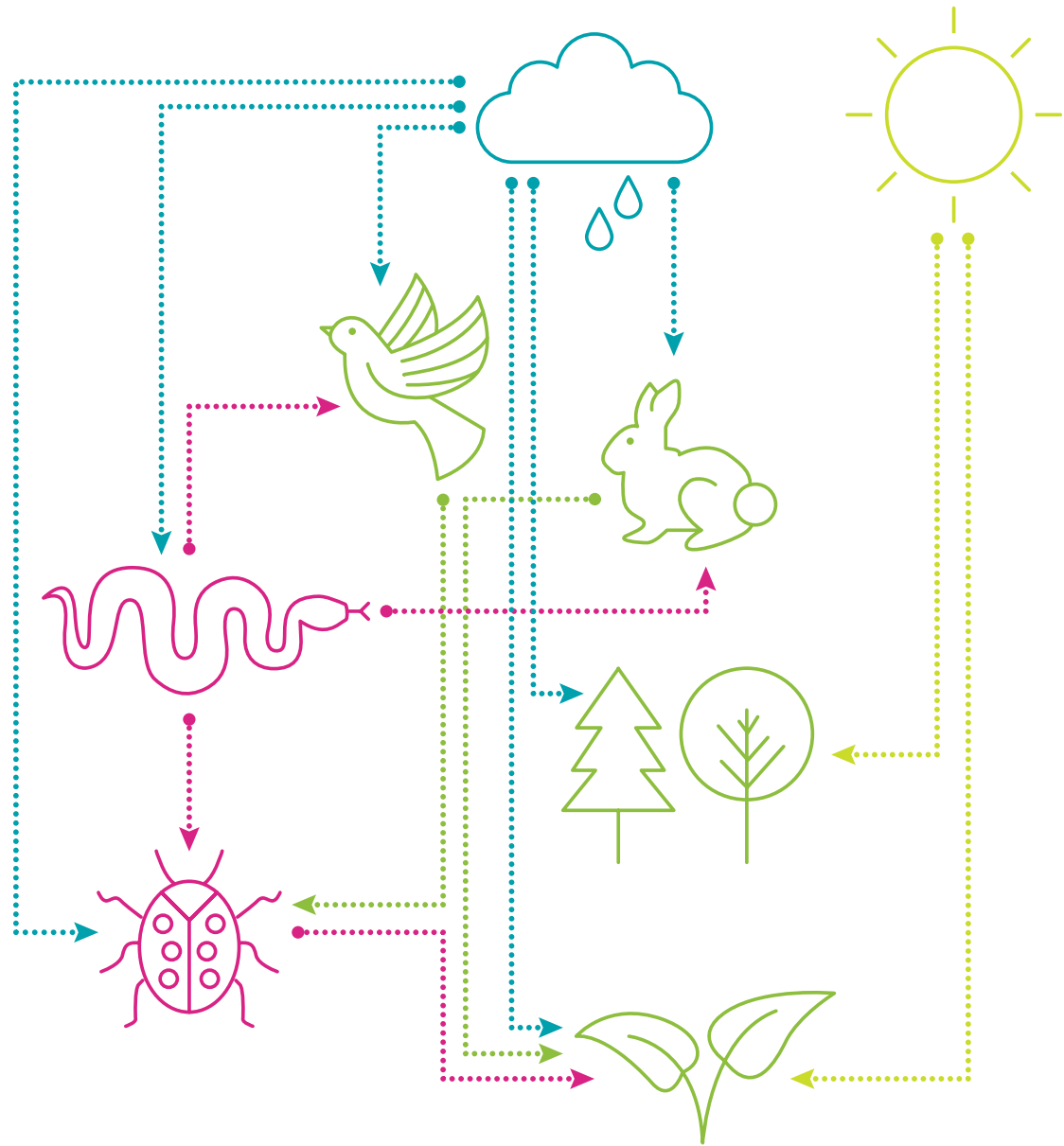
*How to sort out this truckload of information?
How to even begin?*

Categorizing the information by the OSI model is a good place to start.



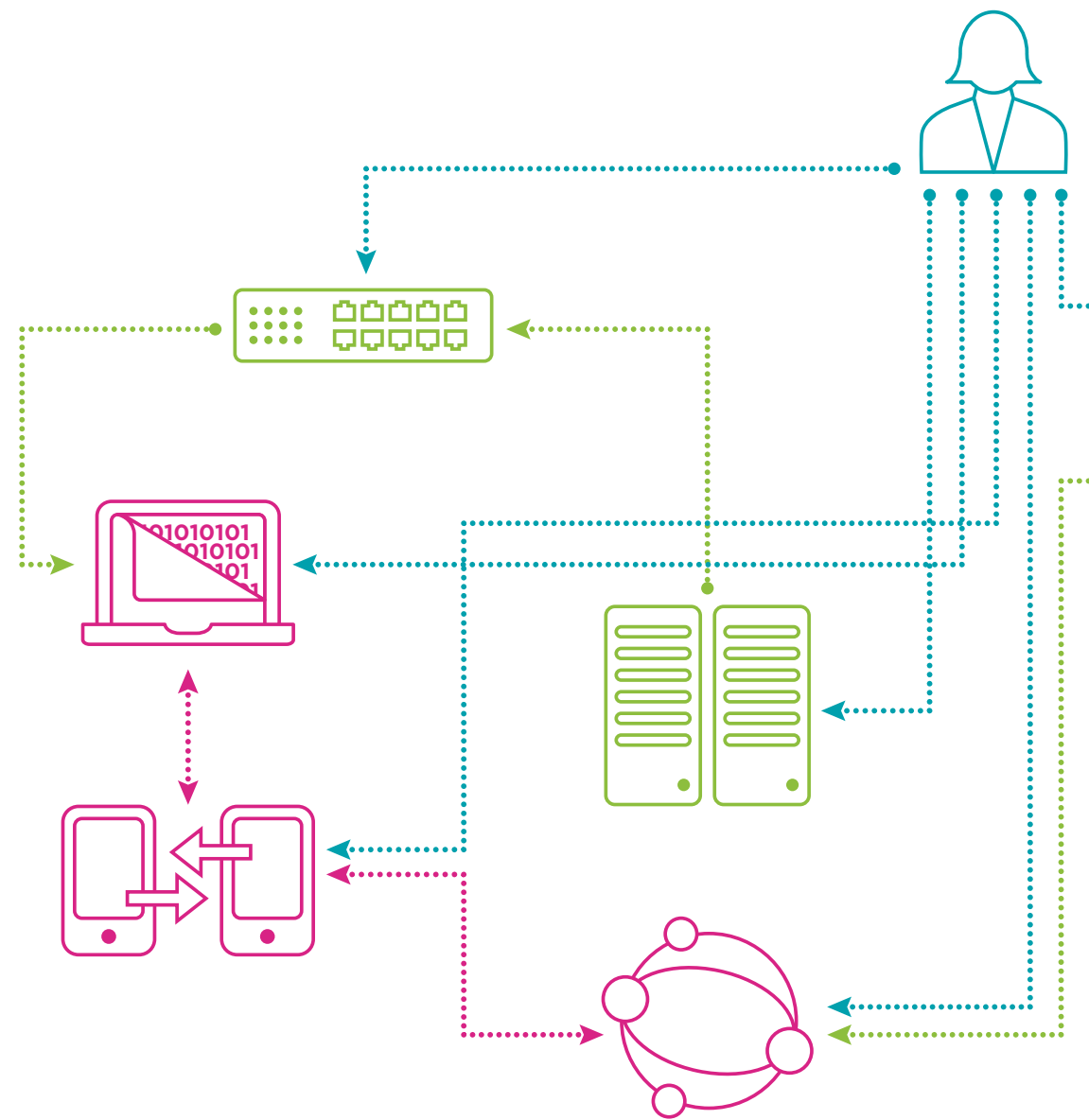
Before delving into the categorizing of seven kinds of security, it will probably help to have an image in your head to picture the world of security.

Imagine an ecosystem: one of trees, birds, bugs, grass, etc. The security ecosystem, if you will, is just like the ecosystem in your backyard. It is a study of interdependence, limited resources and finding just the right balance among all the players in the game to make everything work optimally.



As you can imagine, this is a tall order.

And like an environmentalist studying a complex ecosystem, it requires specific knowledge, expertise, tools and dedicated effort to find that perfect balance.







What does this security ecosystem include?

According to the **OSI model (Open Systems Interconnection)**, a conceptual model of the structure, technology and interactions of systems, we can define layers, or kinds, of security.




The Open Systems Interconnection model (OSI model) is a **conceptual model** that characterizes and standardizes the **communication functions** of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into **abstraction layers**.

The original version of the model defined seven layers.

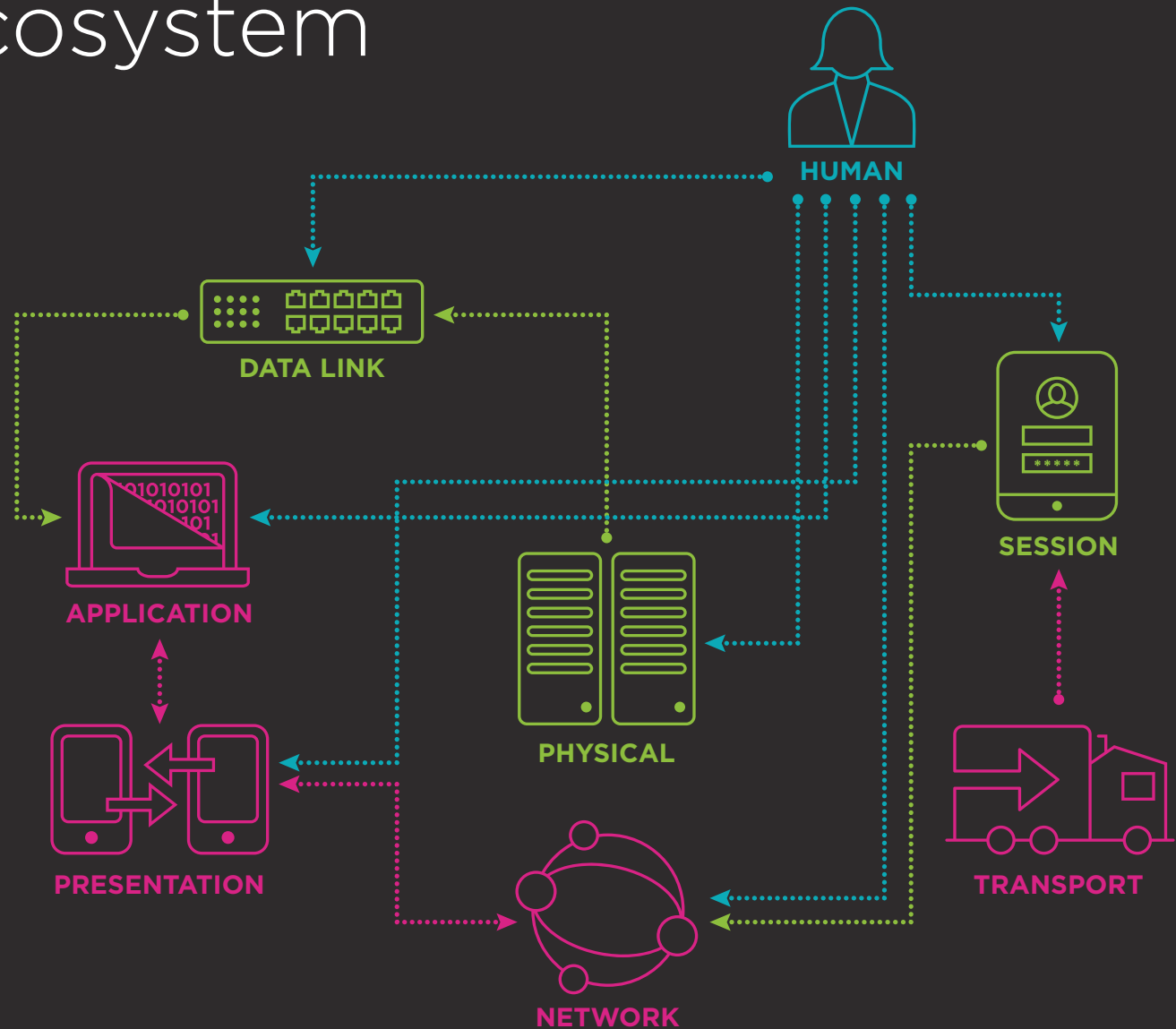
What are the 7 layers in this security ecosystem?

1.		PHYSICAL	This is the lowest layer where the hardware shares the same physical, real-world space as the user. This is where we put locks on doors to keep systems safe.
2.		DATA LINK	At this layer, the data is just one level above the bare metal and silicon of the hardware. Here, the data moves from software to hardware and back. Security at this layer keeps the traffic going and the data where it's supposed to be.
3.		NETWORK	Think traffic control, speed limits, detours and stop signs. This is where network addressing, routing and other traffic control take place. Security at this layer protects against flooding attacks and sniffing or snooping attacks to keep criminals from accessing logins and passwords sent over the network.
4.		TRANSPORT	Think of the post office getting mail from point A to point B reliably and without anyone tampering with the contents, but instead of bills and postcards, you're dealing with data, and instead of houses and apartments, you're dealing with computers and networks. Denial-of-service attacks also occur here, as well as man-in-the-middle attacks (bad guys trying to intercept the data between point A and point B).

What are the 7 layers in this security ecosystem? (continued)

5.		SESSION	This represents the continuous exchange of information in the form of multiple back-and-forth transmissions. The session layer controls the dialogues (connections) between computers. Examples of attacks are denial-of-service and spoofing.
6.		PRESENTATION	The presentation layer is just below the application layer and transforms data into the form that the application accepts. For instance, feed HTML code to a web browser, and you'll get a webpage. Give it to your phone's texting application, and you'll get a lot of computer text that makes no sense to your friend.
7.		APPLICATION	This is the layer closest to the end user and the most troublesome these days. Commonly, web browsers and email clients are attacked at this layer. It's how people interact with computers and devices.

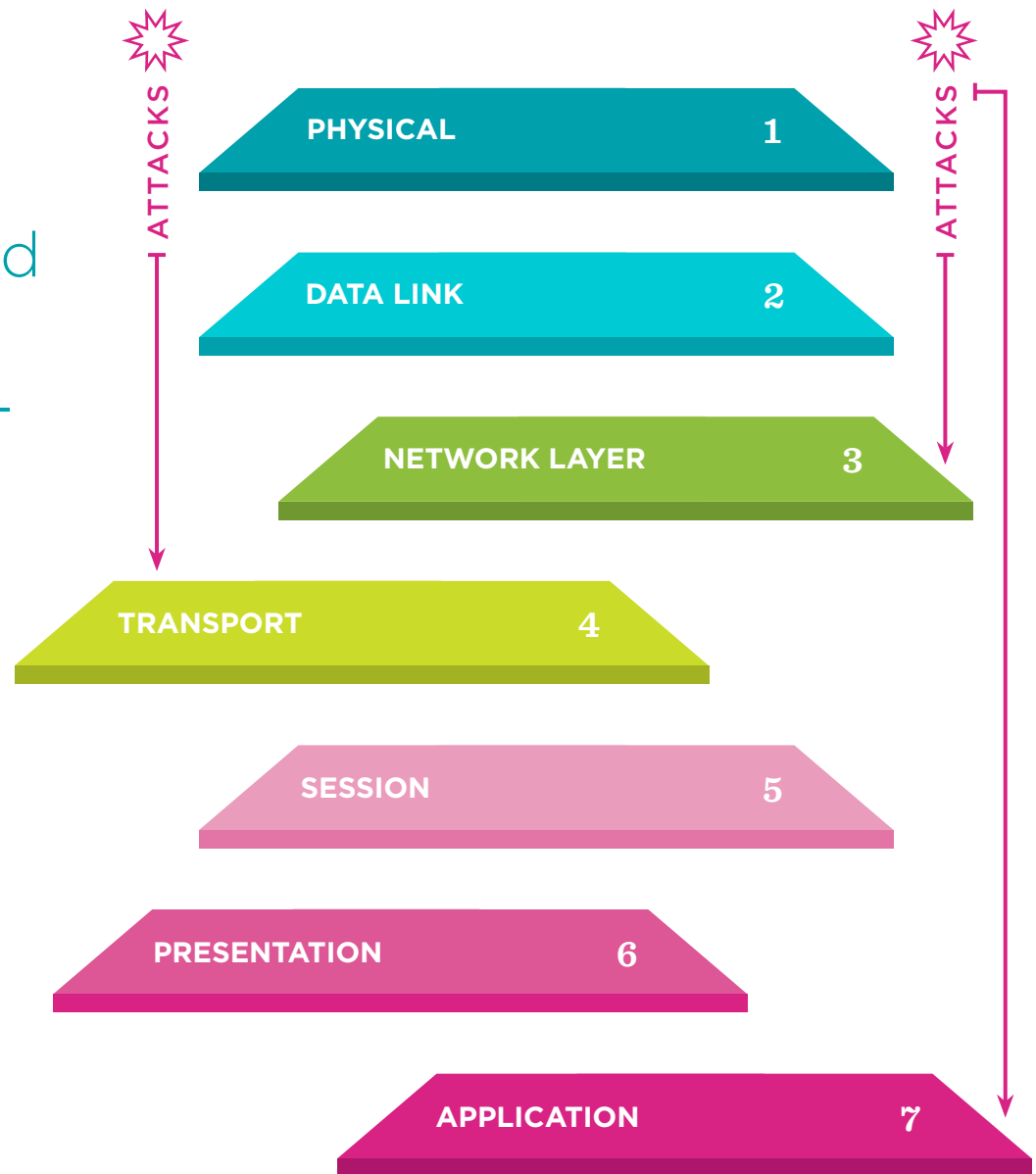
What does this security ecosystem look like?



These layers represent how systems, software and networks interact and contribute to the attack surface (attack surface — the areas where attacks can occur).

Each layer is vulnerable to direct and indirect attacks.

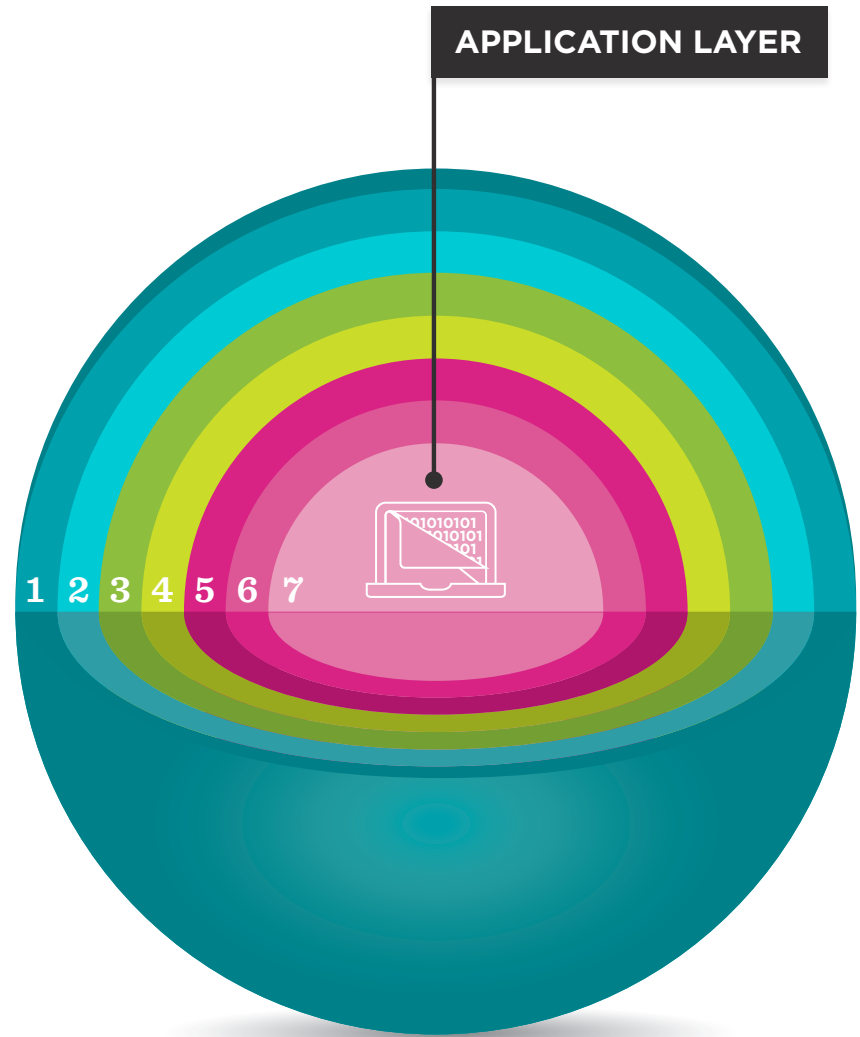
The layers must be continually adjusted so the ecosystem is protected and the attack surface is minimized, without blocking the normal flow of business.



The prevalence of applications means security ecosystems are stressed.

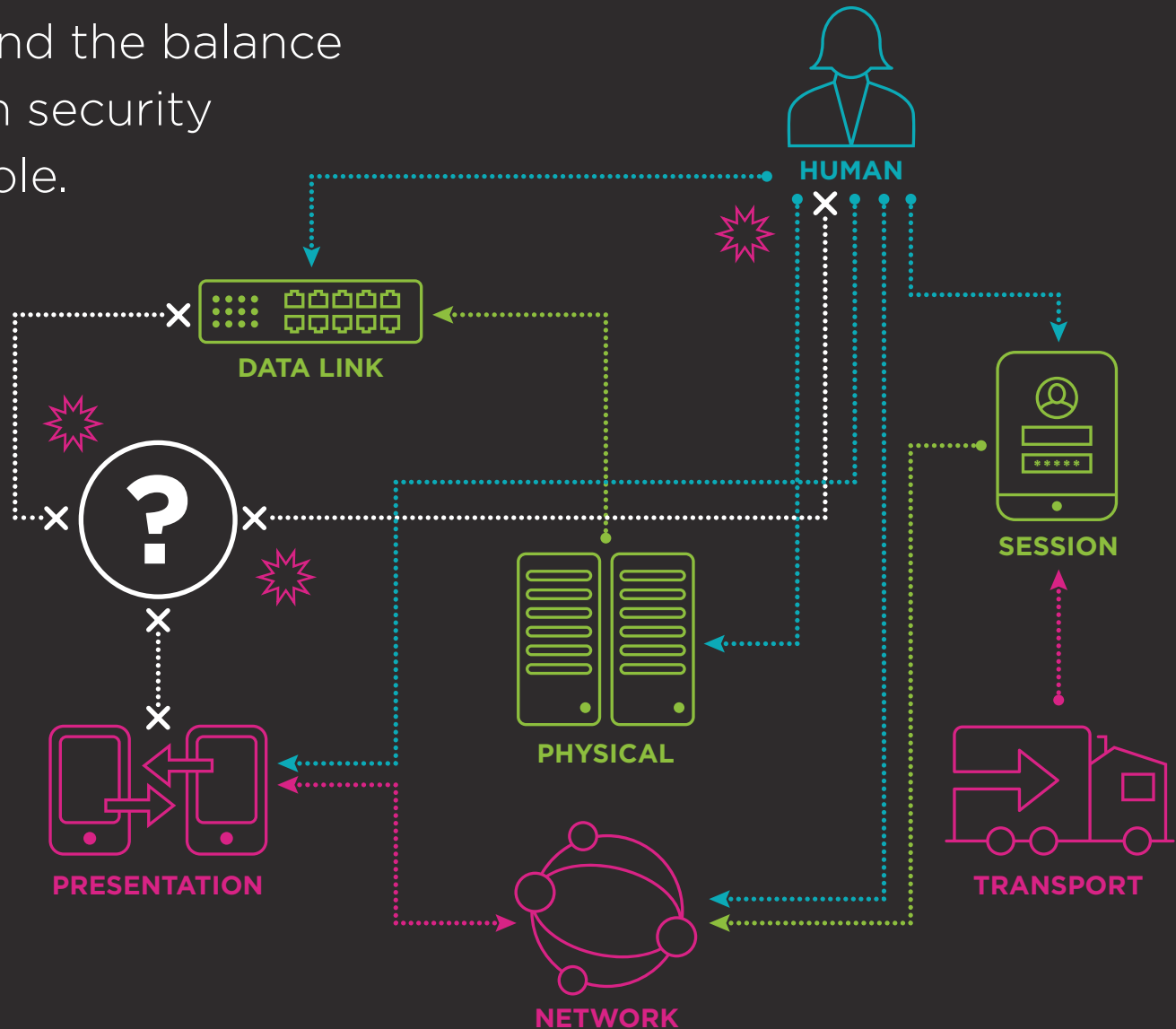
As it turns out, seven is an important number.

The seventh layer, the application layer, is the growing risk in this layer cake of potential insecurity. Addressing this risk is not an easy task as application security requires protecting all applications through design, development, upgrade and maintenance.



This adjustment requires a good understanding of the interaction between the layers, the resources needed and the balance required to maintain security and protect the whole.

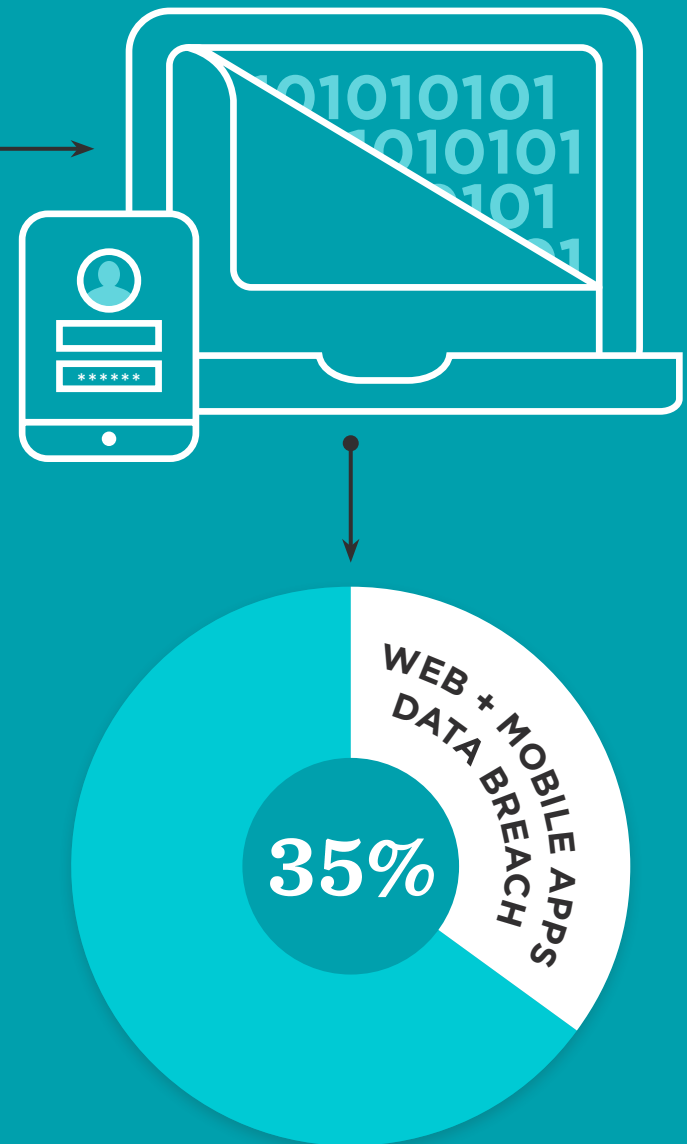
If you remove one piece or restrict resources, or if a piece fails, the entire ecosystem can become unstable or insecure.



The newness and very nature of how Internet-enabled applications work, making it possible for companies to interact effectively and efficiently with the outside world, also mean they are at greater risk of cyberattacks.

Which is why web and mobile applications currently account for more than a third of data breaches.

Source: 2014 Verizon Data Breach Investigations Report



Consider that in 2014...

THERE WERE 8 MAJOR BREACHES THROUGH
THE APPLICATION LAYER



RESULTING IN MORE THAN

450 Million
personal or financial records stolen



According to Akamai's "State of Internet Security" report, "application-layer attacks are growing much more rapidly than infrastructure attacks." Unfortunately, with companies in all industries relying more and more on applications as a source of innovation and business efficiencies, attacks against the application layer will only continue to grow. We can already see it in the growth of application-based vulnerabilities on the web.

According to Risk Based Security's VulnDB for 2015, there have been...

595

reported new web application vulnerabilities

OF THE 595 REPORTED



198

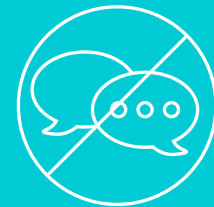
**HAD NO KNOWN
SOLUTION OR PATCH**



291

**WERE CONSIDERED HIGH SEVERITY
BY THEIR CVSSv2 SCORE**

Common Vulnerability Scoring System



18

**THE VENDOR DIDN'T
EVEN BOTHER TO RESPOND**

Four real-world breaches...

1

Target was breached through a sophisticated attack-kill chain, which included exploiting a vulnerability in a web application used to interface with vendors.

The breach resulted in the theft of data, including names, email addresses, credit card information, mailing addresses and phone numbers, for 70 million customers.



TARGET.

2

JPMorgan Chase was breached through a web application built and hosted by a third-party developer. The web application was deemed non-business critical because it promoted a charitable road race and was not related to business activities.

The breach resulted in the records of 76 million households and 7 million businesses being stolen.

JPMORGAN CHASE & CO.

3

Community Health was breached through a software component with a well-publicized vulnerability. The insurance company was unable to find all instances of the component in its application ecosystem and, as a result, could not patch the vulnerability.

The breach resulted in more than 4 million patient records lost.



4

TalkTalk was breached through a common SQL injection vulnerability.

The breach resulted in the theft of names, addresses, birthdays and financial information for potentially all of the company's 4 million customers.

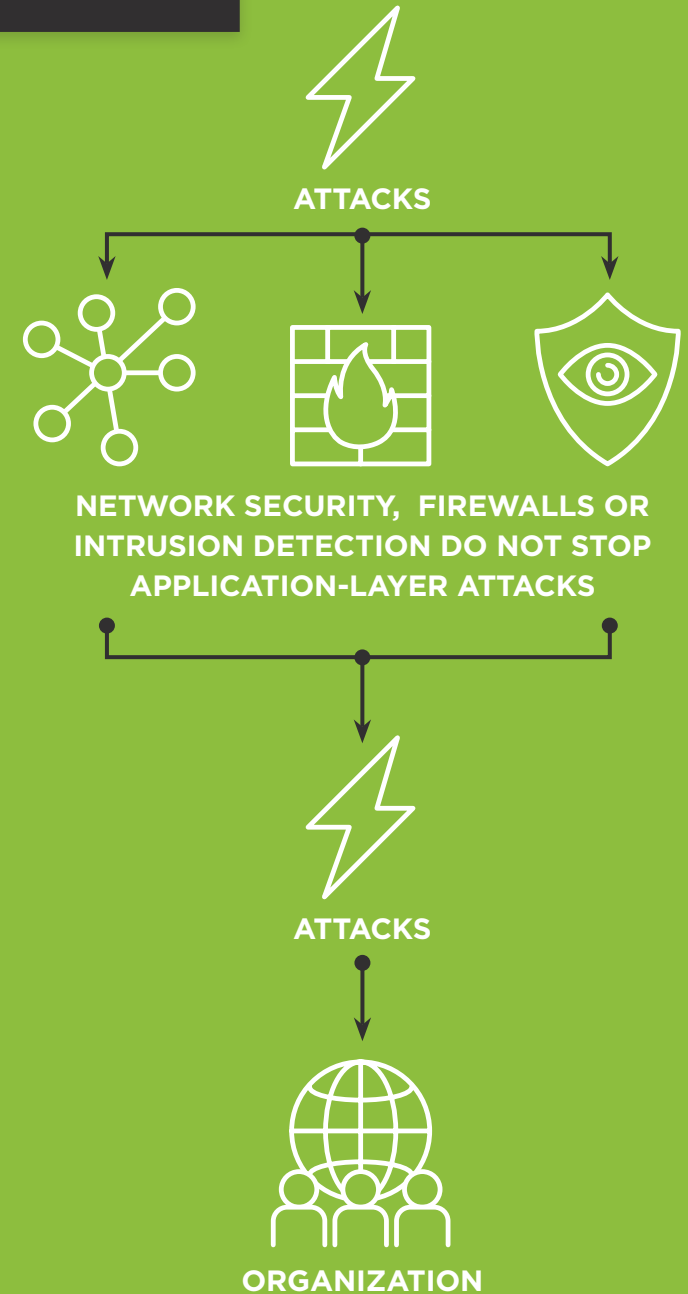
TalkTalk

Many organizations assume that their existing security measures, such as network security, firewalls, intrusion detection systems or data leakage prevention tools, protect them from application-layer attacks.

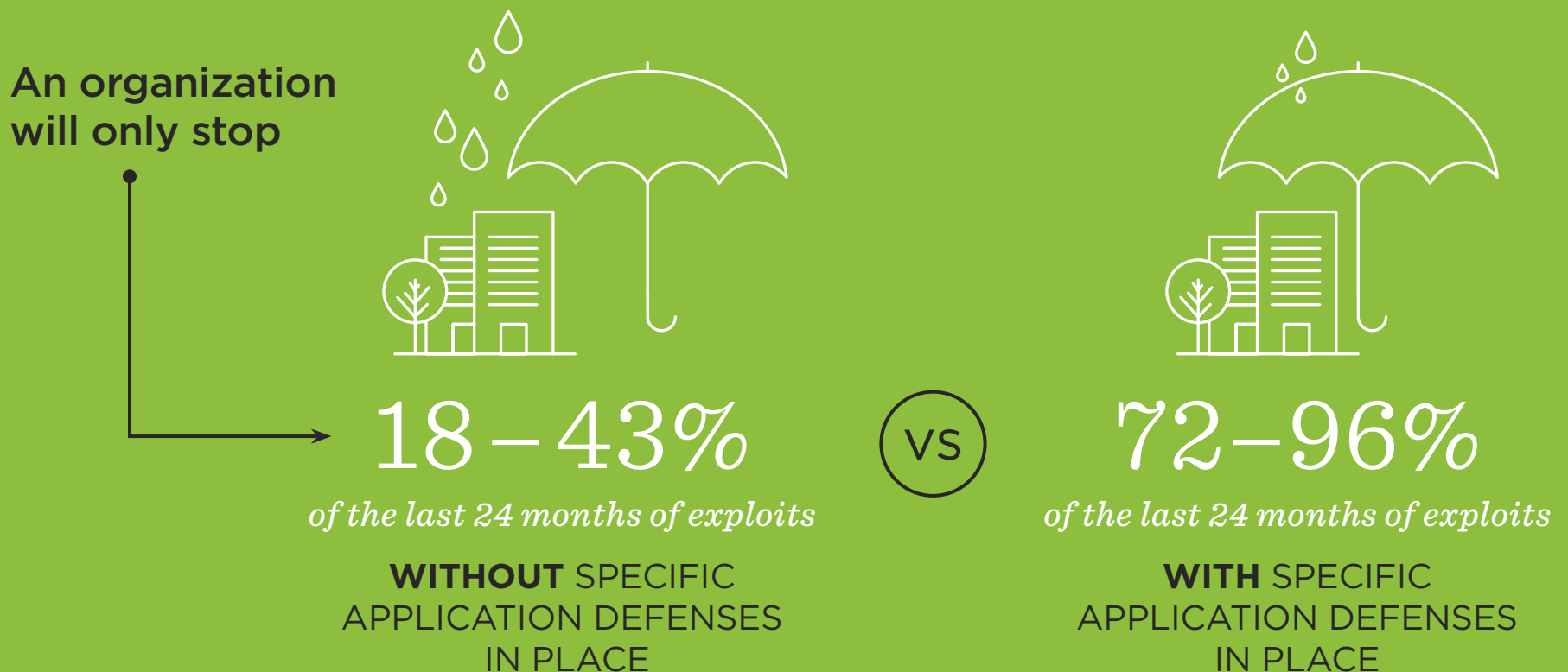
This is old-world thinking.

The idea that lower layer security measures protect higher layers simply isn't true.

THE REALITY



According to research by **Picus Security**, which tests live exploits against various infrastructure protection devices for security effectiveness...



If you're like most people, phrases like:

“major breaches”

“high severity”

“no known solution”

“didn't have a vendor response”

“only stop 18% to 43%”

... are the stuff of which ulcers are made. If it wasn't already apparent, applications may be the invading species in the world's backyard.

They're growing faster than kudzu too. →





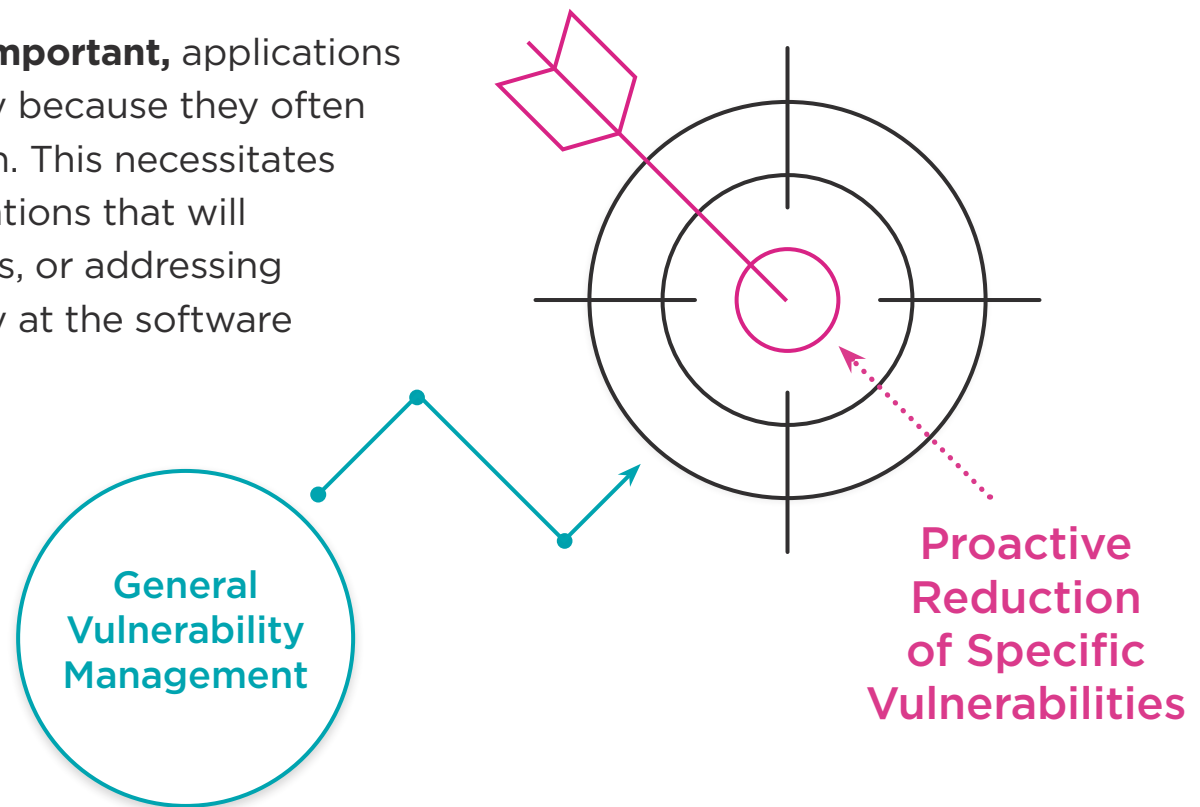
A security ecosystem is fragile by default. Its optimal functioning depends on a delicate balance of controls, interactions and vulnerabilities.

Since applications tend to tie together multiple systems across the network and across many types of users, application security requires more focus and attention than it has received in the past as it impacts every layer of the security ecosystem.



The introduction of application security shifts the focus from general vulnerability management to proactively reducing specific vulnerabilities in applications.

While both perspectives are important, applications present a more alarming reality because they often face attacks that have no patch. This necessitates thoroughly researching applications that will be purchased from third parties, or addressing application design and security at the software development phase.



CONCLUSION

When a major shift is introduced to an ecosystem, like dropping a python in a mouse cage, or like adding Internet-facing applications, it will be difficult to find harmony again. It's incumbent on a business to assess how to adjust the seven types of security in the environment to reduce risk. Every interaction matters to the attack surface, and applications bring many more and new types of interactions on all layers. Introducing application security addresses these interactions and benefits the entire security ecosystem, on every layer.

LOVE TO LEARN ABOUT APPLICATION SECURITY?

Get all the latest news, tips and articles delivered right to your inbox.

LEARN MORE
**How to Convince
Board AppSec
is Your Most
Productive Spend**