

**TRUADVANTAGE POWER HOUR WEBINARS & WORKSHOP**

- "Knowledge is Power"

# The Ever-Evolving Cybersecurity Landscape





# ABOUT TRUADVANTAGE



**100 +**  
Organizations Served



**2001**  
Since providing IT



**97.2 %**  
Client Satisfaction



**14**  
Awards last 3 Years



**200+**  
Google Reviews

## #1 RANKED IT & CYBERSECURITY TEAM IN THE BAY AREA



TruAdvantage is a Bay Area based, award-winning IT firm that specializes in managed IT, managed Cybersecurity, cloud solutions and strategic IT planning. Our passion is to bring enterprise-level productivity, simplicity, scalability, and security to over 100 small to medium businesses who have chosen us as their IT partner.



# Free to our Audience:



Currently, we are offering a completely Free Security Audit and Penetration Test. Take advantage of it here: <https://www.truadvantage.com/cyberaudit/>



Please send your questions to [Kayvan@truadvantage.com](mailto:Kayvan@truadvantage.com)



Join our future Power-Hour Webinars and Workshops:  
[TruAdvantage.com/power-hour](https://TruAdvantage.com/power-hour)



To have a quick chat regarding this webinar, our IT services, or our free IT Audit please schedule a quick chat here: [www.truadvantage.com/QuickChat](http://www.truadvantage.com/QuickChat)



# Speaker



**Kevin Davy**  
Sr. Systems Engineer,  
Barracuda



# Cybersecurity Landscape



2000

Device  
Hackers  
Perimeter  
Attacks



2007

Desktop/Laptop  
Script Kiddies  
Controlled  
Access  
Intrusive



2014

Mobile  
Criminal  
Ecosystem  
Wide Access  
Disruptive



2022

IoT (Internet of Things)  
Hacktivists  
Hybrid Cloud  
Destructive

IoE (Internet of Everything)  
Non-State Actors  
No Perimeter  
Devastating



2023

Metaverse  
Criminal  
Ecosystem  
Malicious A.I.  
Colossal



# Crime has Changed.

---













## Twitter in data-protection probe after '400 million' user details up for sale

© 30 December 2022

## PayPal warns 35,000 customers of exposure following credential stuffing attack

Published Jan. 19, 2023

DATA BREACHES

## Yum Brands Discloses Data Breach Following Ransomware Attack

KFC and Taco Bell parent company Yum Brands says personal information was compromised in a January 2023 ransomware attack.

HACKED AGAIN —

## T-Mobile discloses 2nd data breach of 2023, this one leaking account PINs and more

Hack affecting 836 subscribers lasted for more than a month before it was discovered.

DAN GOODIN - 5/1/2023, 7:40 PM

## Sobeys cybersecurity breach brings \$25M net earnings hit



Alicja Siekierska

December 15, 2022 · 2 min read

## Hackers demand \$15 million ransom from TransUnion after cracking "password" password

## MailChimp discloses new breach after employees got hacked

By [Lawrence Abrams](#)

January 18, 2023 04:11 PM





It is estimated that organizations suffered a ransomware attack every **11 seconds in 2021.**

By 2031, it is anticipated that a new attack on a customer or business will occur **every 2 seconds.**





# Evolution of Ransomware

---





# RANSOMWARE

is a type of malware that infects your system, then locks or encrypts your data, allowing attackers to ask for a ransom. The attackers will offer to provide the decryption key only if you pay a certain amount of money within a short time.

```
uu$:$:$:$:$uu
uu$$$$$$$$$$$$$$$$$$$$uu
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$$$$$$$$$$$$$$$u
u$$$$$$$*   *$$$*   *$$$$$u
*$$$$*     u$u     $$$*$
$$$u       u$u     u$$$
$$$u       u$$$$u   u$$$
*$$$$u$$$$$   $$$uu$$$$$*
*$$$$$$$$*   *$$$$$$$$*
u$$$$$$$$$u$$$$$$$$$u
u$*$*$*$*$*$*$u
uuu         $$u$ $ $ $ $u$$         uuu
u$$$$      $$u$u$u$u$u$u$$      u$$$$
$$$$$$uu   *$$$$$$$$$$$*       uu$$$$$$$
u$$$$$$$$$$$$$$$   *****   uuuu$$$$$$$$$$$$
$$$$$***$$$$$$$$$$$$$uuu   uu$$$$$$$$$$$$$***$$$*
***          **$$$$$$$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$$$$$$$$uuu
u$$$$uuu$$$$$$$$$$$$$uu **$$$$$$$$$$$$$$$$$uuu$$$
$$$$$$$$$$$$$***          **$$$$$$$$$$$$$$$$$*
*$$$$$*                   **$$$$$**
$$$*           PRESS ANY KEY!           $$$*
```



# Current Threats and Trends

---





# Barracuda Security Insights

Last Updated: Sep 05, 2023, 09:00 (PST)

Current Threat Level: **High**

Current Cybersecurity Index: **148.3** ▲ 9.9

24 Hours

Previous 7 Days

Previous 30 Days



Zero-hour advanced threats in previous 30 days

Total: **144,368**

Email: **137,284**

Web: **3,226**

Network: **3,858**



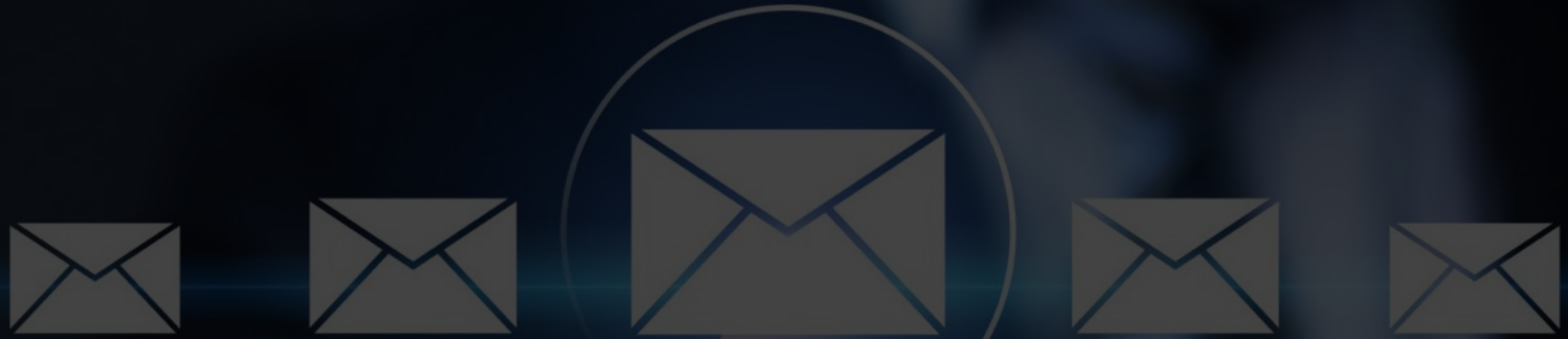


# End users are frequent targets

of data breaches involved a **human** element.

**82%**

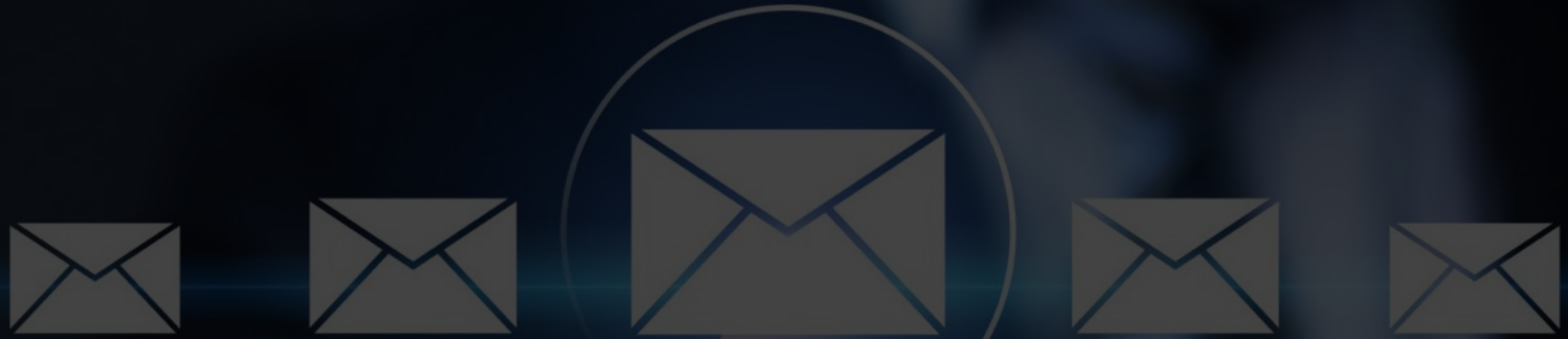




# Phishing

is an email scam designed to steal personal information from victims. Cybercriminals use phishing, the fraudulent attempt to obtain sensitive information such as credit card details and login credentials, by disguising as a trustworthy organization or reputable person in an email communication.





## **Spear phishing**

is a personalized phishing attack that targets a specific organization or individual. These attacks are carefully designed to elicit a specific response from a specific target. Attackers invest time in researching their targets and their organizations to craft a personalized message, often impersonating a trusted entity.





The worldwide information security market is forecast to grow **11.3%** to reach more than **\$188.3 billion in 2023.**



# Different Types of Attacks



**Brand  
impersonation**



**Business email  
compromise  
(BEC)**



**Blackmail**





# Brand impersonation

**83%** of spear phishing attacks involve brand impersonation.

## Effective because:

- Often includes **zero-day** links
- Uses **compromised accounts**
- Appears to come from a **trusted business application**

The Google logo is displayed in its characteristic multi-colored font (blue, red, yellow, green, red).

# Business email compromise (BEC)

## Effective because:

BEC scams accounted for **\$1.7 billion** of losses to online scams, according to the FBI's annual Internet Crime Report

## Effective because:

- Very **personalized**
- **Does not** contain malicious links or attachments
- Launched from **compromised accounts**
- Uses **urgency**, personalization and pressure





# Blackmail

**1 in 10** spear phishing emails are sextortion attacks.

## Effective because:

- **Does not contain** malicious links or attachments
- Under reported due to intentionally **embarrassing nature** of the threats.



Caution



SYSTEM HACKED...

## What **Damage** Can a Successful Attack Do?

- Risk to the business
  - Loss of data
  - Downtime
  - Lost productivity
  - Post-attack disruption
  - Restoration
  - Reputational harm





Caution



SYSTEM HACKED...

## What **Damage** Can a Successful Attack Do?

- Aftermath

- Computers wiped
- Reverted to pen and paper
- Six weeks to recover
- Lost revenue
- New hardware
- Overtime



# How can you protect yourself?

---





# Many Tools Are Not Solving The Problem

of malware is delivered via **email**.

94  
%



# Use multi-factor authentication (MFA)



Over **1.2 million** Microsoft enterprise accounts will be compromised each month, with **99.9 percent** of those accounts **not enabling MFA**.





# Learn how to recognize and report an attack



There is a cyberattack  
every 39 seconds.

Source: Finntech News



# Use DMARC authentication



Only **3%** of email domains  
utilize **DMARC policies**

Source: Agari Cyber Intelligence Division





# Basic cybersecurity hygiene for business

1



Establish what you  
want to protect

2



Build concentric  
rings of security

3



Monitor your  
environment

4



Reduce response  
time

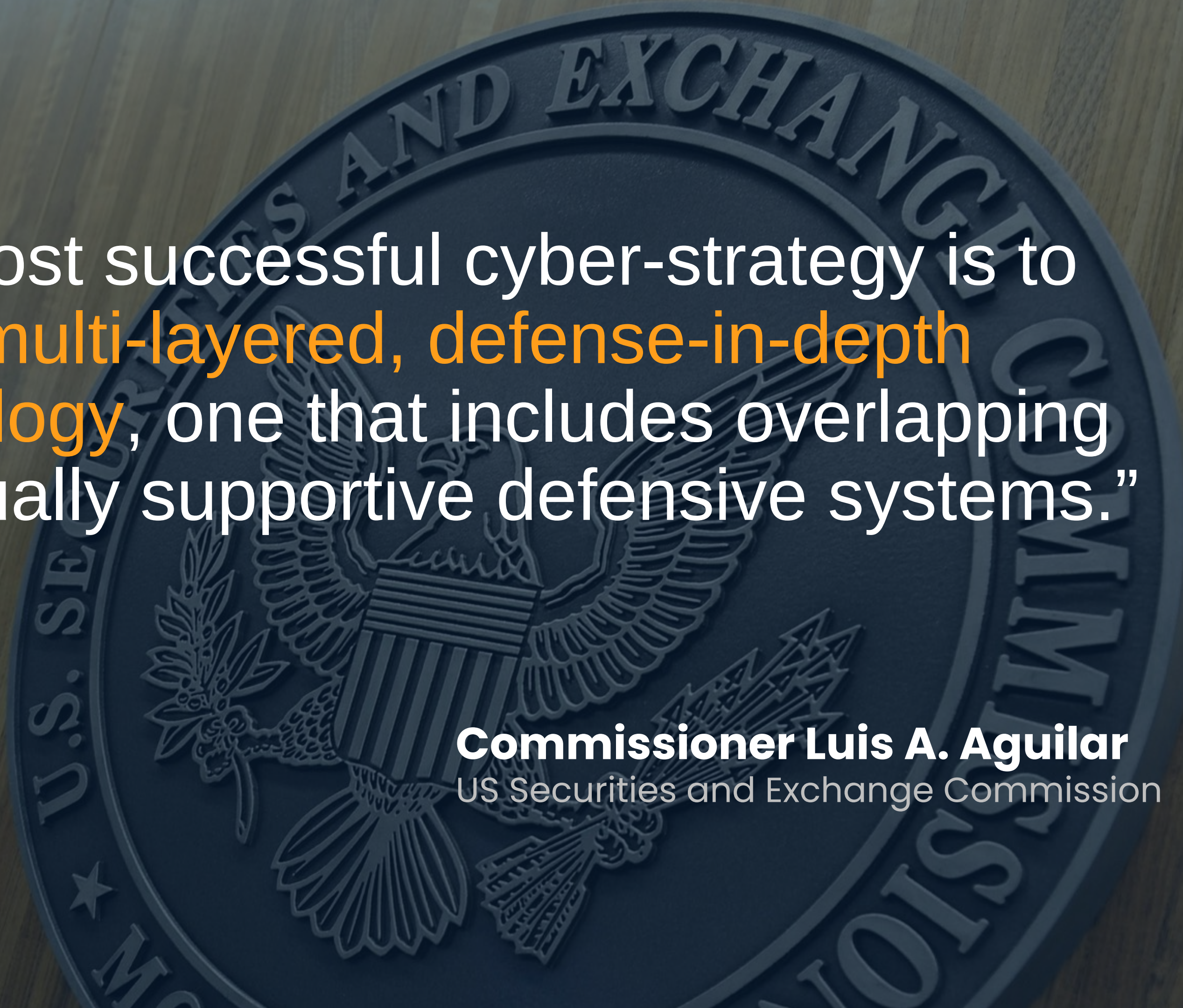
5



Secure your  
people, process,  
and technology





The background of the slide features a large, semi-transparent seal of the U.S. Securities and Exchange Commission. The seal is circular and contains an eagle with wings spread, holding an olive branch and arrows. The text "U.S. SECURITIES AND EXCHANGE COMMISSION" is visible around the perimeter of the seal.

“...the most successful cyber-strategy is to adopt a multi-layered, defense-in-depth methodology, one that includes overlapping and mutually supportive defensive systems.”

**Commissioner Luis A. Aguilar**  
US Securities and Exchange Commission

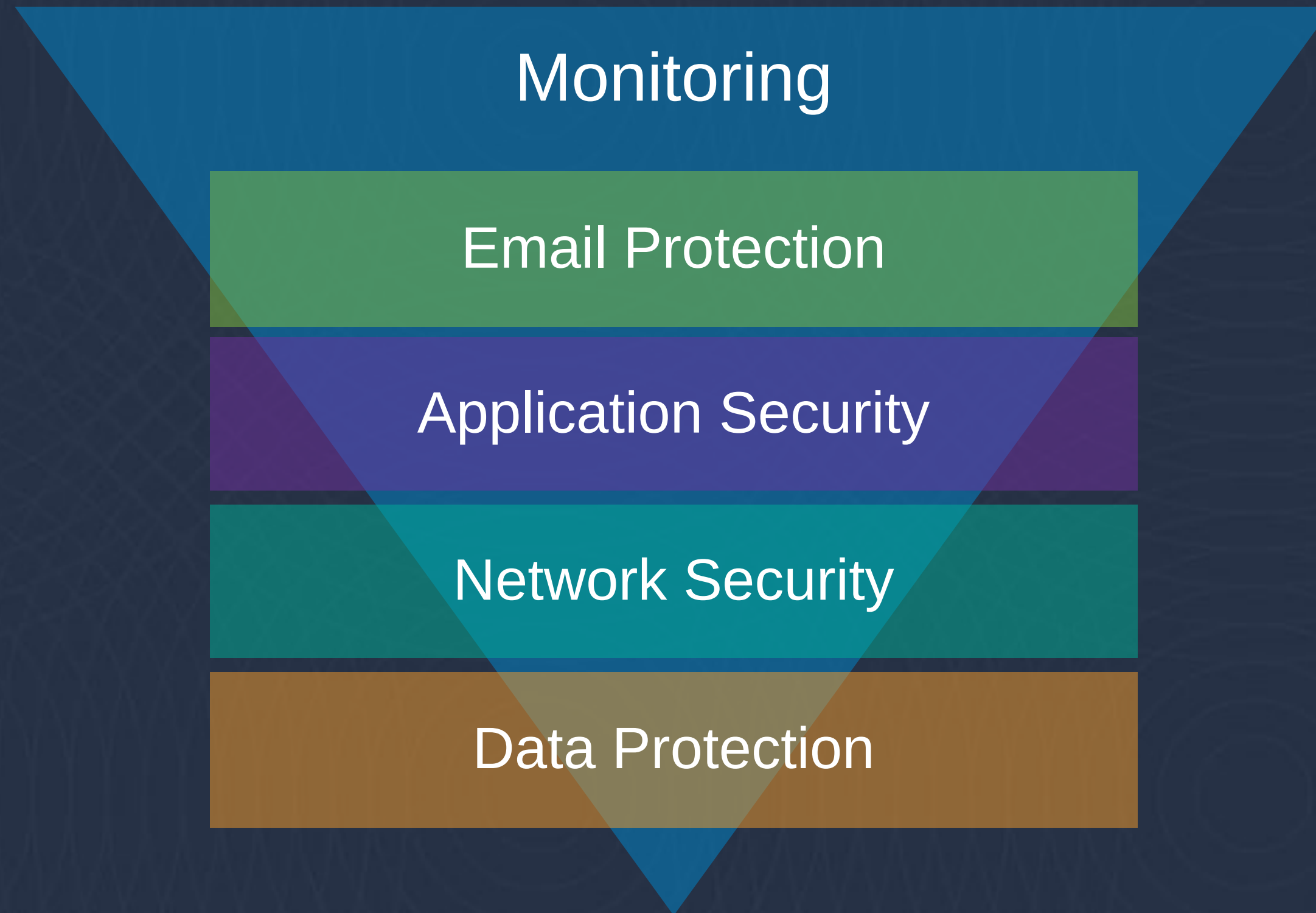


What does a multi-layered  
defense look like?

---



# Layered Cybersecurity - Defense in Depth

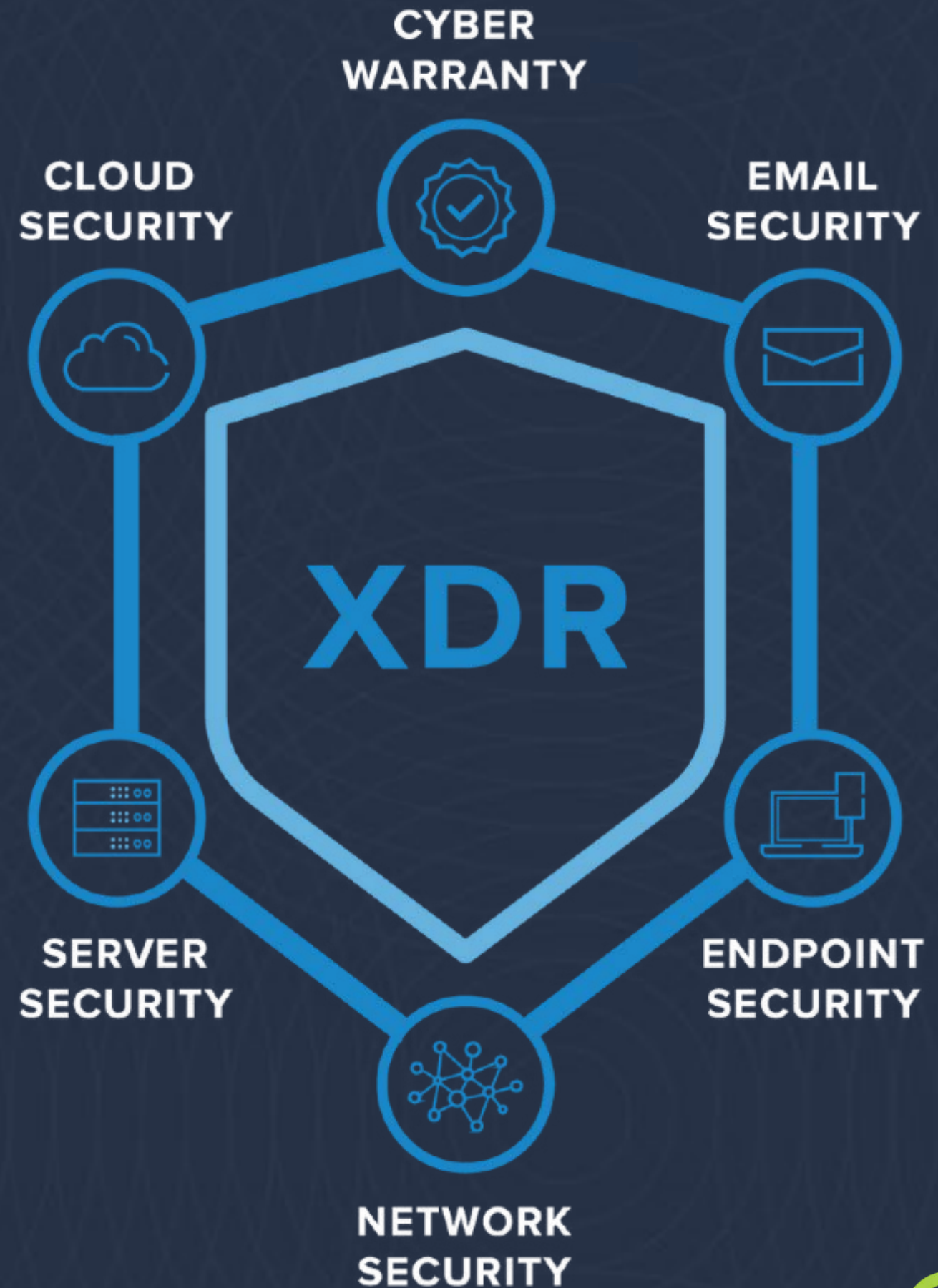




# Monitor Your Environment

Protect all major attack vectors.

- Enforces essential cybersecurity hygiene
- Protects against sophisticated cyberattacks, including **zero-day**, **supply chain attacks**, **ransomware**, and much more
- 24x7x365 Security Operations Centre
- 40+ integrated data sources



# Next steps

1

Talk to your Managed Service Provider about how you can ensure cyber hygiene across your digital environment

2

Request a free email threat scan of your Microsoft365 inboxes to understand what email-born threats are sitting in your organization's inboxes right now!





# Free to our Audience:



Currently, we are offering a completely Free Security Audit and Penetration Test. Take advantage of it here: <https://www.truadvantage.com/cyberaudit/>



Please send your questions to [Kayvan@truadvantage.com](mailto:Kayvan@truadvantage.com)



Join our future Power-Hour Webinars and Workshops:  
[TruAdvantage.com/power-hour](https://TruAdvantage.com/power-hour)



To have a quick chat regarding this webinar, our IT services, or our free IT Audit please schedule a quick chat here: [www.truadvantage.com/QuickChat](http://www.truadvantage.com/QuickChat)



# Thank You

---