



Minding Security Gaps

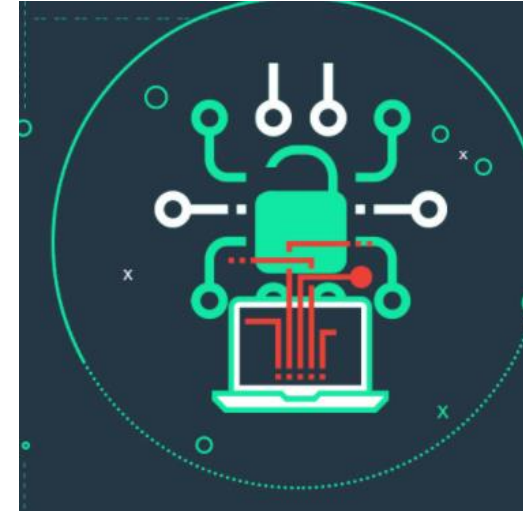
How Virtual Patching can protect businesses

Krista Laplante-Gaul – krista_laplangaul@trendmicro.com
Technical Sales Engineer

Why are zero-day vulnerabilities & exploits significant



Vulnerabilities



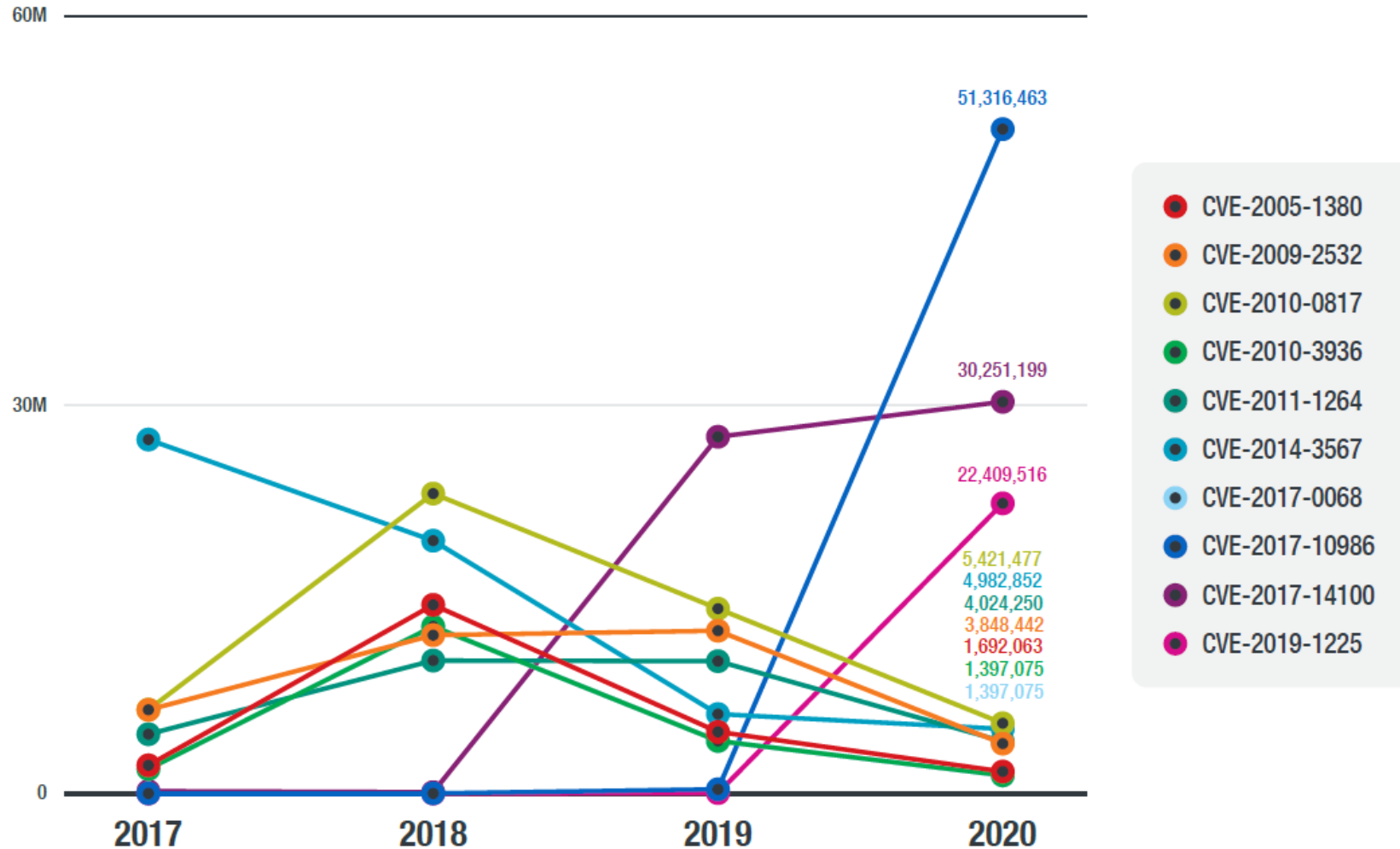
Exploits

<https://www.trendmicro.com/vinfo/fr/security/news/vulnerabilities-and-exploits/security-101-zero-day-vulnerabilities-and-exploits>



State of Vulnerabilities

The 10 most exploited vulnerabilities

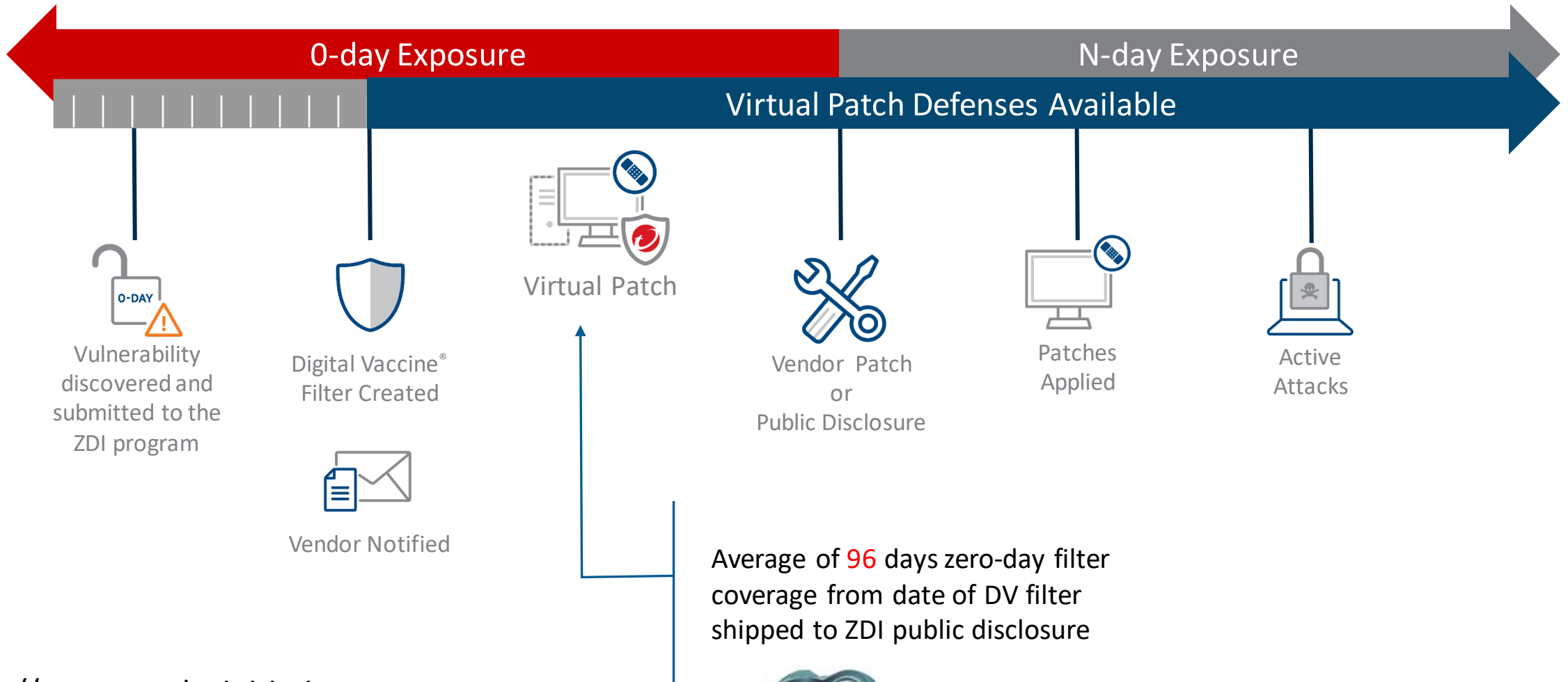


A comparison of the detection counts of the 10 most exploited vulnerabilities from 2017 to 2020



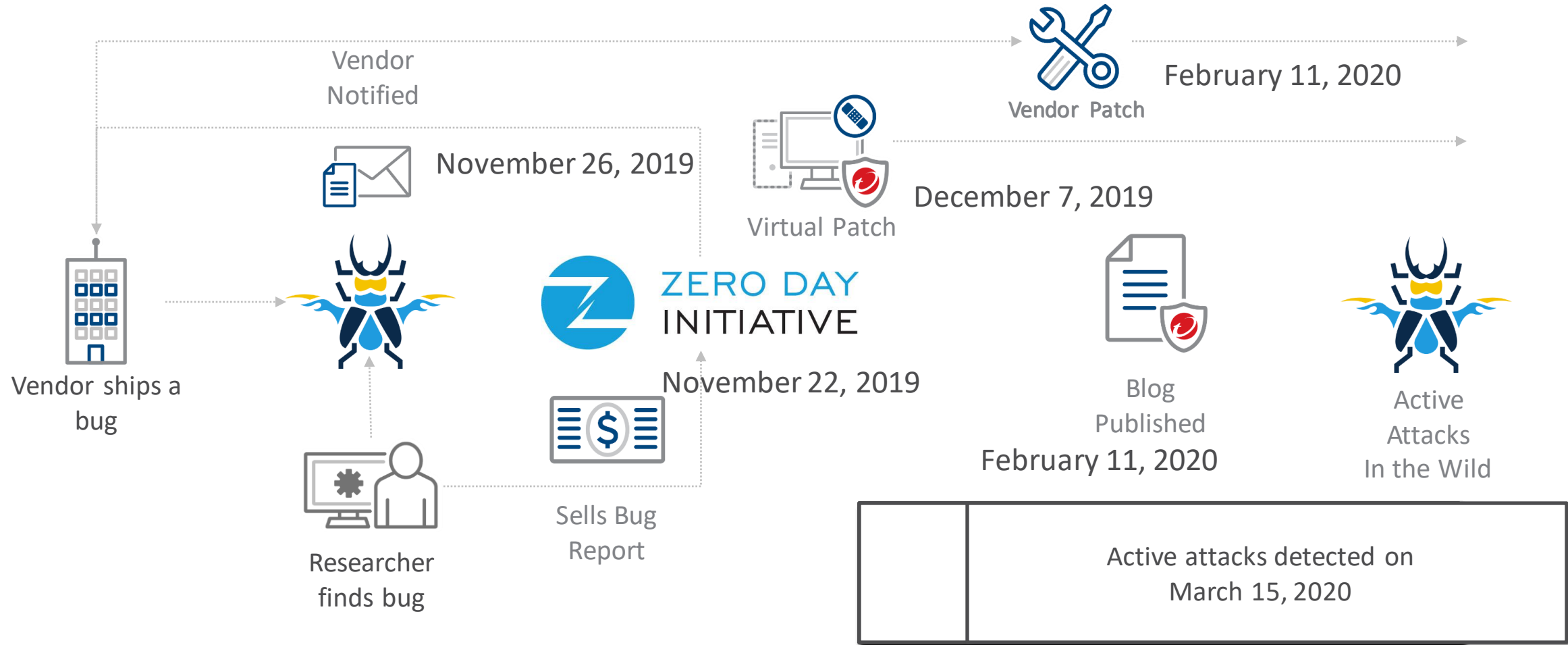
The Lifecycle of a Vulnerability

How it works



<https://www.zerodayinitiative.com>

Case Study – CVE-2020-0688





What happens to unpatched IT infrastructures?

Window to Patch Very Small

Attack overview

1. Command and Control
September 7, 09:07 – 09:13 UTC
Cobalt Strike DNS Beacon

3. Exploit
September 15, 13:36 UTC
Unusual volume of RPC calls to 'Netlogon'



2. Exploit Code Announced
September 14
CISA reports that the CVE-2020-1472
exploit code is widely available

Figure 1: A timeline of the attack



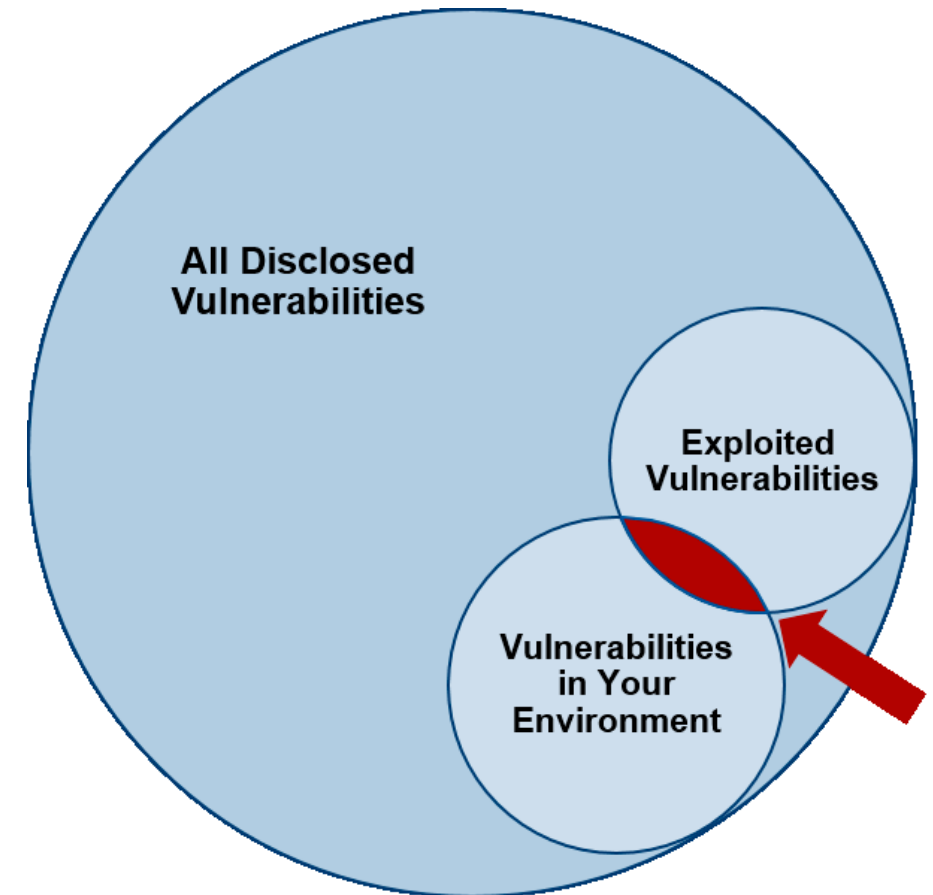
Prioritize and defend against the latest threats

Prioritizing vulnerabilities



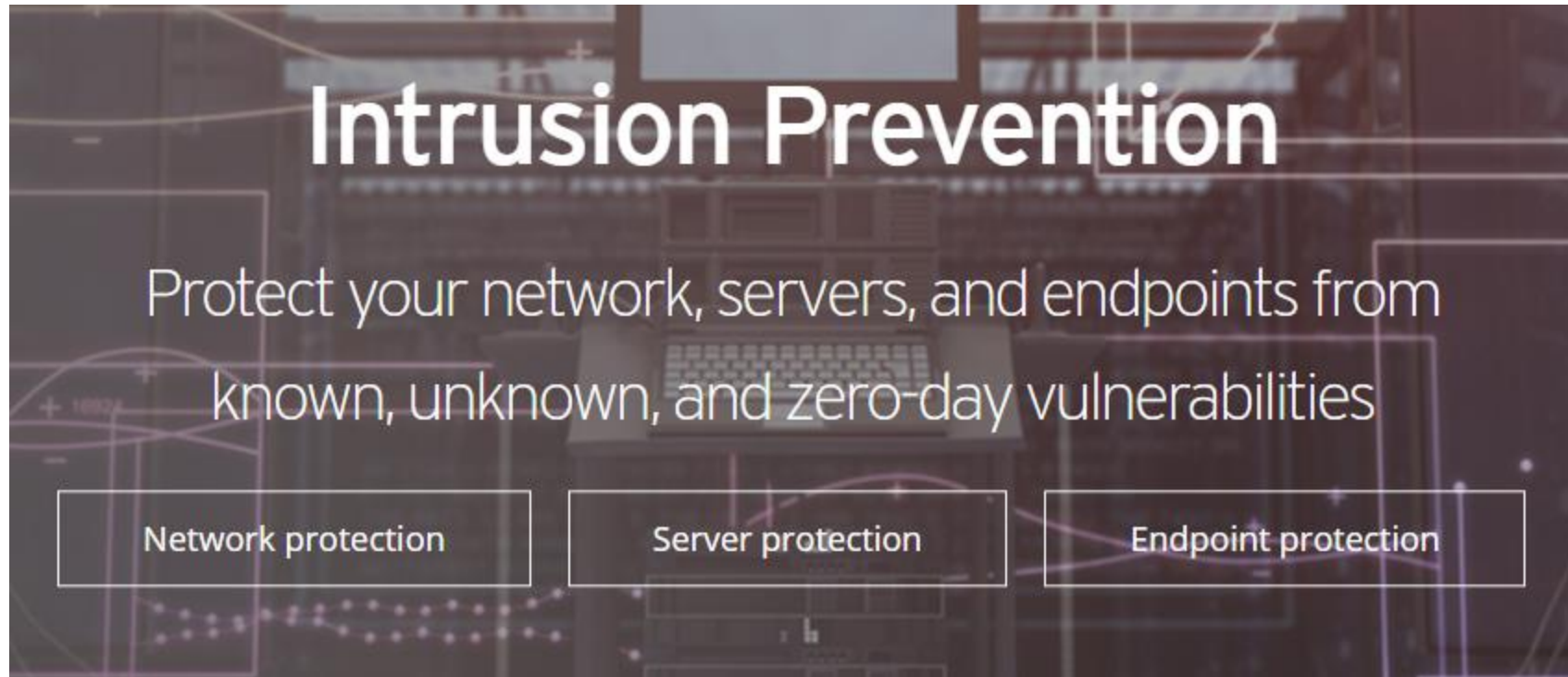
Addressing your highest security risks

- “Vulnerabilities and their exploitation are still the root cause of most breaches.”
- The vast majority of malware are leveraging known vulnerabilities to propagate
- How do you tune to maximize defenses with the resources you have?
- How do you prioritize the most important threats?



<https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021/>

Protect against the full range of threats

A graphic with a dark background featuring a grid and glowing lines. The text is centered and reads: "Intrusion Prevention" in large white font, followed by "Protect your network, servers, and endpoints from known, unknown, and zero-day vulnerabilities" in a smaller white font. Below this, three white-bordered boxes are arranged horizontally, containing the text "Network protection", "Server protection", and "Endpoint protection" respectively.

Intrusion Prevention

Protect your network, servers, and endpoints from known, unknown, and zero-day vulnerabilities

Network protection Server protection Endpoint protection

https://www.trendmicro.com/en_ca/business/capabilities/intrusion-prevention.html



Thank You!

Krista Laplante-Gaul – krista_laplantegaul@trendmicro.com
Technical Sales Engineer