paloalto NETWORKS

Cybersecurity in K-12 Education

May 12th, 2021

Barry Rosenberg
Systems Engineer

brosenberg@paloaltonetworks.com

Agenda

- K-12 landscape and challenges
- Threat Focus: Ransomware
- Palo Alto Networks approach
- Reference architectures and how we can help
- Further Reading & Appendix

Cybersecurity Challenges In K-12 Education

paloalto NETWORKS

K-12 education: A popular but under-the-radar target for cyberattacks

School districts, especially small ones, a favorite target for hackers

Teen hacker discovers bugs in education software exposing millions of student records

"When it comes to cybersecurity, school districts don't present the content-rich targets that major corporations or government agencies might, but they also don't have the same resources to protect themselves."

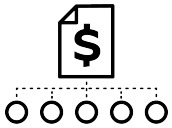
Jim Flanagan, chief learning service officer at the International Society for Technology in Education

Education sector clicks on more phishing links than any other industry--2019 Verizon Data Breach Investigations Report

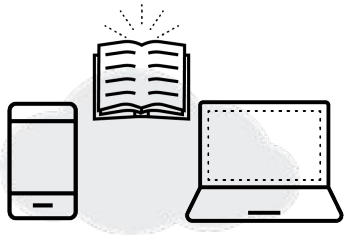
83% of UK schools have experienced at least 1 cyber-incident; only ⅓ train staff on cybersecurity

What's behind the rise in security incidents in education?

Large, diverse user groups



Limited funding
Small IT Staffs



Rapid change in learning models

Sophistication of attackers

Ransomware accounts for 80% of malware infections in educational services sector.

- 2020 Verizon Data Breach Investigations Report

What Is Ransomware?

The Challenge: Ransomware is cyber threat public enemy #1.

In 2020, ransom demands averaged $847,000.* *Don't be next!*

PRO CYBER NEWS

Ransomware Poses a Threat to National Security, Report Warns

Tech companies urge U.S. to make sweeping policy and legal changes to combat cybercriminals

Business - Insider

Ransomware Is Getting Worse, and Cybersecurity Has No Easy Answers

Hacked companies are paying off ransomware gangs, the criminals are reinvesting the profits in making bigger and bolder attacks, and there's ...

5 hours ago

Fox News

Large Florida school district hit by ransomware attack, hackers demanded $40M

The computer system of one of the nation's largest school districts was hacked by a criminal gang that encrypted district data and demanded ...

1 day ago

The Hill

University of California victim of ransomware attack | TheHill

The University of California (UC) said Wednesday that it was the victim of a ransomware attack.

20 hours ago

ON TECH

Don't Ignore Ransomware. It's Bad.

Ransomware attacks can bring down schools and hospitals. It's time we took them more seriously.

KTLA

University of California victim of nationwide ransomware attack

The University of California is warning its students and staff that a ransomware group might have stolen and published their personal data and ...

1 day ago

Chicago Tribune

CNA website still down as a result of ransomware attack

CNA's website was still down Friday nearly two weeks after what the Chicago-based insurance giant is now calling a ransomware attack.

1 day ago

Fox Business

Ransomware, Microsoft attacks are surging at the same time: Report

Ransomware is spiking as cyberattacks on Microsoft jump, according to a report.

1 day ago

Defending against today's sophisticated ransomware attacks starts with an assessment of your ability to prevent and respond!

* Source: Unit 42 2021 Ransomware Threat Report

Ransomware Overview

What is Ransomware?

- Ransomware is form of malware that encrypts a victim's files.
- Attackers then demand ransom payment from the victim in order to restore access to their data.
- Ransomware has become increasingly easy to get hold of and is available in many formats targeting multiple platforms
- Most ransomware infections are opportunistic, some attacks are specifically targeted to organizations and individuals

Unit 42 2021 Ransomware Report Highlights

Key Highlights

- The average ransom paid by organizations in the US, Canada, and Europe **increased from US$115,123 in 2019 to $312,493 in 2020**—a 171% year-over-year increase.
- In 2020, the highest ransomware demand **grew to $30 million.**
- Attackers used COVID-19 to prey on specific organizations—**particularly the healthcare sector**, which was the most targeted vertical for ransomware in 2020.
- Attackers have began to adopt **double extortion methods** by threatening to leak sensitive data or information if the ransom is not paid

Table 1: Costs Associated with Ransomware Incidents in 2020 in the US, Canada, and Europe (US$)

	2020 Data	Earlier Data (Where Available)
Avg. ransom demand	$847,344	–
Avg. ransom paid	$312,493	$115,123 (2019)
Highest ransom demand	$30,000,000	$15,000,000 (2015–2019)
Highest ransom paid	$10,000,000	$5,000,000 (2015–2019)
Lowest ransom demand	$1,000	–
Avg. cost of forensic engagement	$73,851	$62,981 (2019)
Avg. cost of forensic engagement, small and midsize business	$40,719	–
Avg. ransom demand, small and midsize business	$718,414	–
Avg. cost of forensic engagement, large enterprise	$207,875	–
Avg. ransom demand, large enterprise	$2,923,122	–

* Source: Unit 42 2021 Ransomware Threat Report

Ransomware Overview - How an Attack Works

Joe the user

Opens email

Browses web

Credentials are compromised

Clicks phishing link/downloads malicious file

Lands on compromised website

Remote desktop protocol (RDP)

Loader drops additional tools to support attack

- Recon
- Looking at Data
- Exfiltration
- Lateral Movement

Ransomware deployed and encrypts files/data

Demand ransom usually paid in the form of cryptocurrency

Prevention:
The Palo Alto Networks Approach

Advanced, Automated Security Across the Entire IT Infrastructure

Prevent everything that you can

Rapidly detect & investigate everything you can't prevent

Automate response and remediation

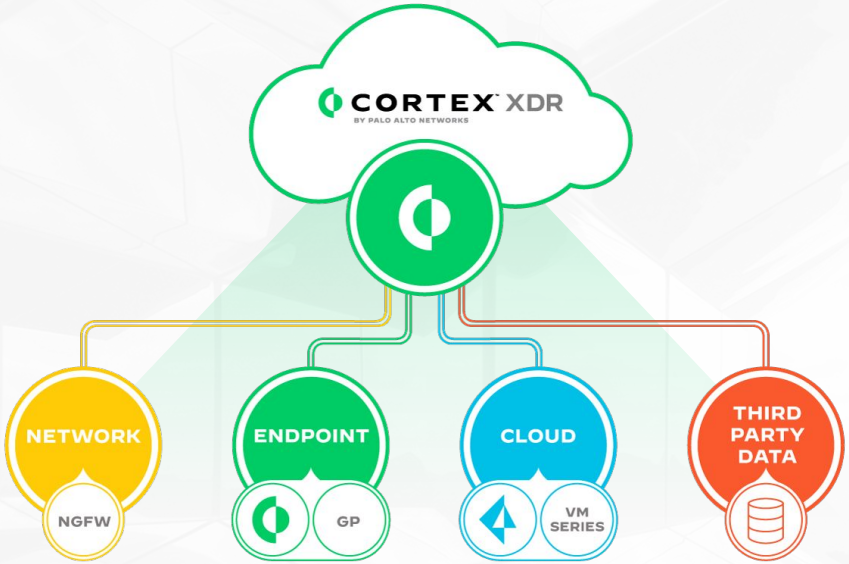
Manage & secure the entire attack surface

Threat Intelligence

Managed Threat Hunting

Incident Response

Prevent, Detect, Investigate, & Respond with Cortex XDR

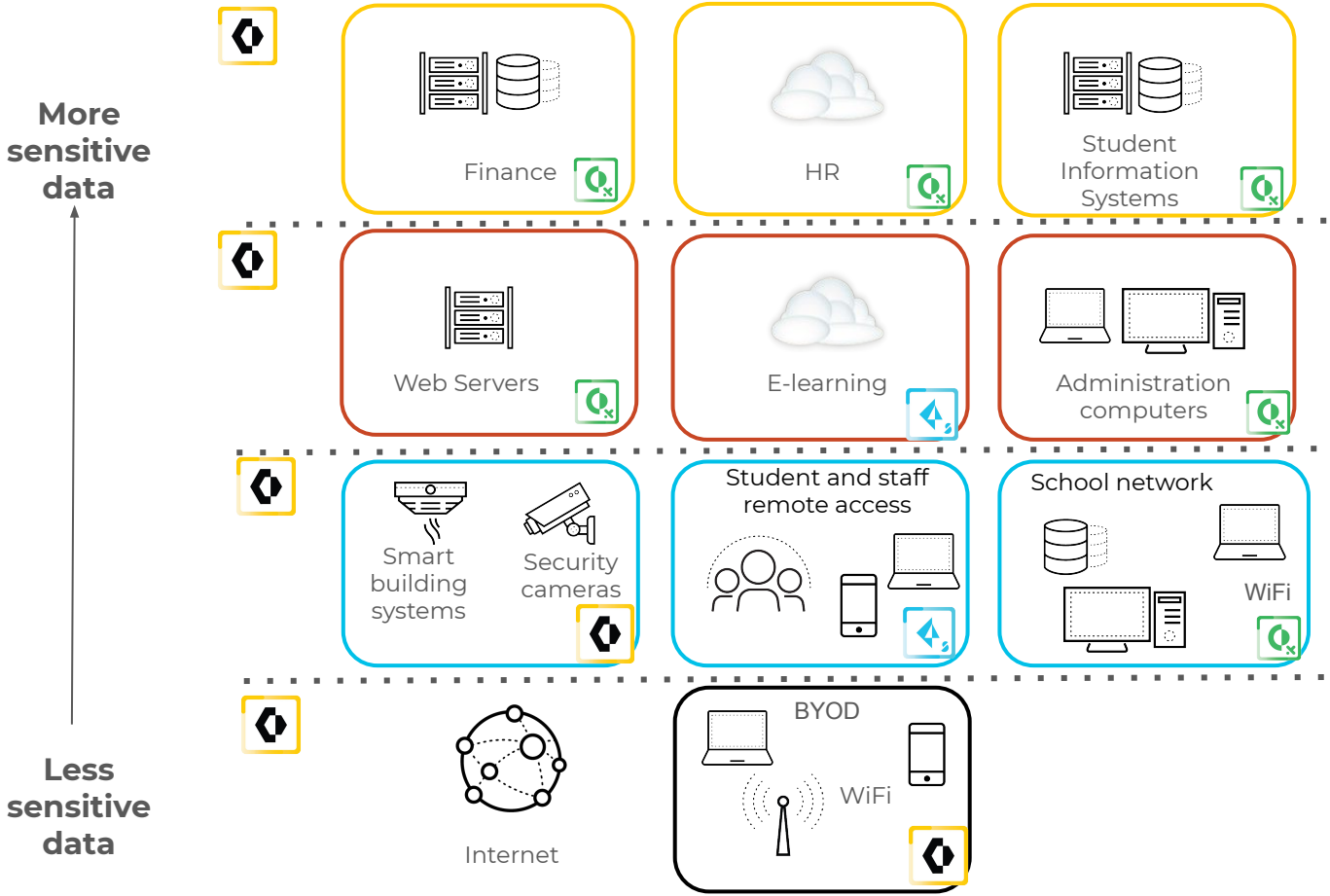


Automatically coordinate across the network, cloud, and endpoints

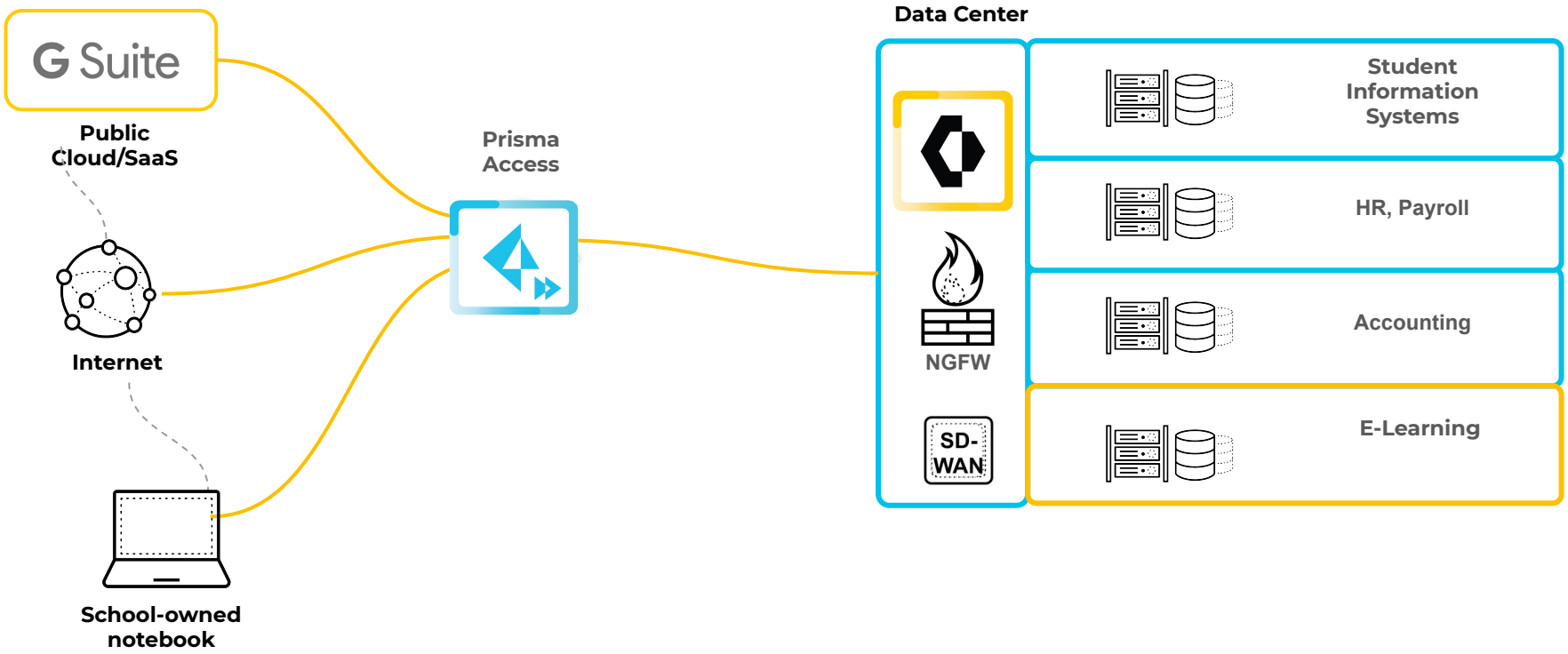
Take an organization-wide view of user, network, and device behavior

Machine-learning and curated rule-based analytics

Implementing Zero Trust in K-12: An example



Example: Protect students no matter where they travel



Your Cybersecurity Partner of Choice

paloalto NETWORKS

The Unit 42 Ransomware Readiness Assessment

Cybersecurity risk assessment focused on controls and the people, processes, and technologies necessary to mitigate the ransomware threat. We offer control enhancements, remediation recommendations, and a strategic roadmap to achieve a **Target State of Ransomware Readiness**

Option 1

- **Ransomware Readiness Assessment**
- **Ransomware Threat Landscape Briefing**
- **Ransomware Tabletop Exercise**
- **50 hours reserved for Incident Response**

Option 2

Everything in Option 1, plus....

Ransomware Compromise Assessment using XDR[1]

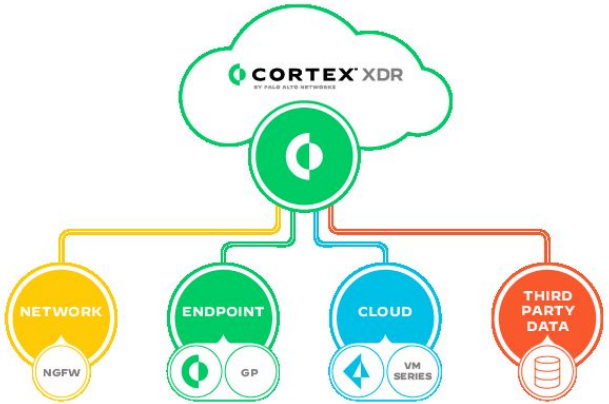
[1] Covers up to 10,000 endpoints. Additional tiers available for larger environments.

 |

Summary

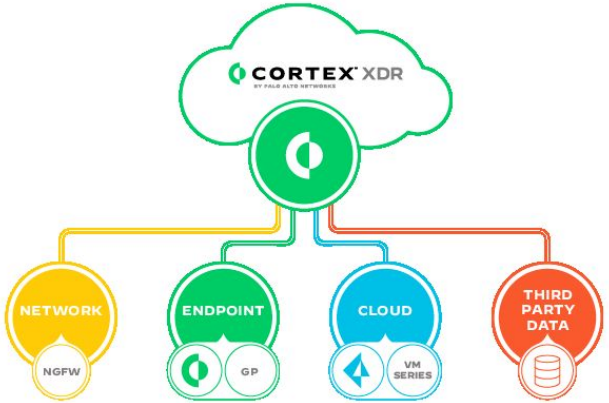
Multilayered approach

- Next-generation antivirus on all devices, laptops, servers
- Strong, zero-trust based network security. Protect the users wherever they are in the world.
- Detect & stop stealthy attacks fast with machine learning across all of your user & network data
- Leverage outside expertise as needed to check readiness



Further Reading

- Landing Page: Thwart Ransomware in Government & Education
- 6 Steps to Stop Ransomware in Schools and Governments
- Top Five threats to K-12 Online Student Safety, Data and Compliance
- Unit 42 2021 Ransomware Threat Report
- Ransomware's New Trend: Exfiltration and Extortion



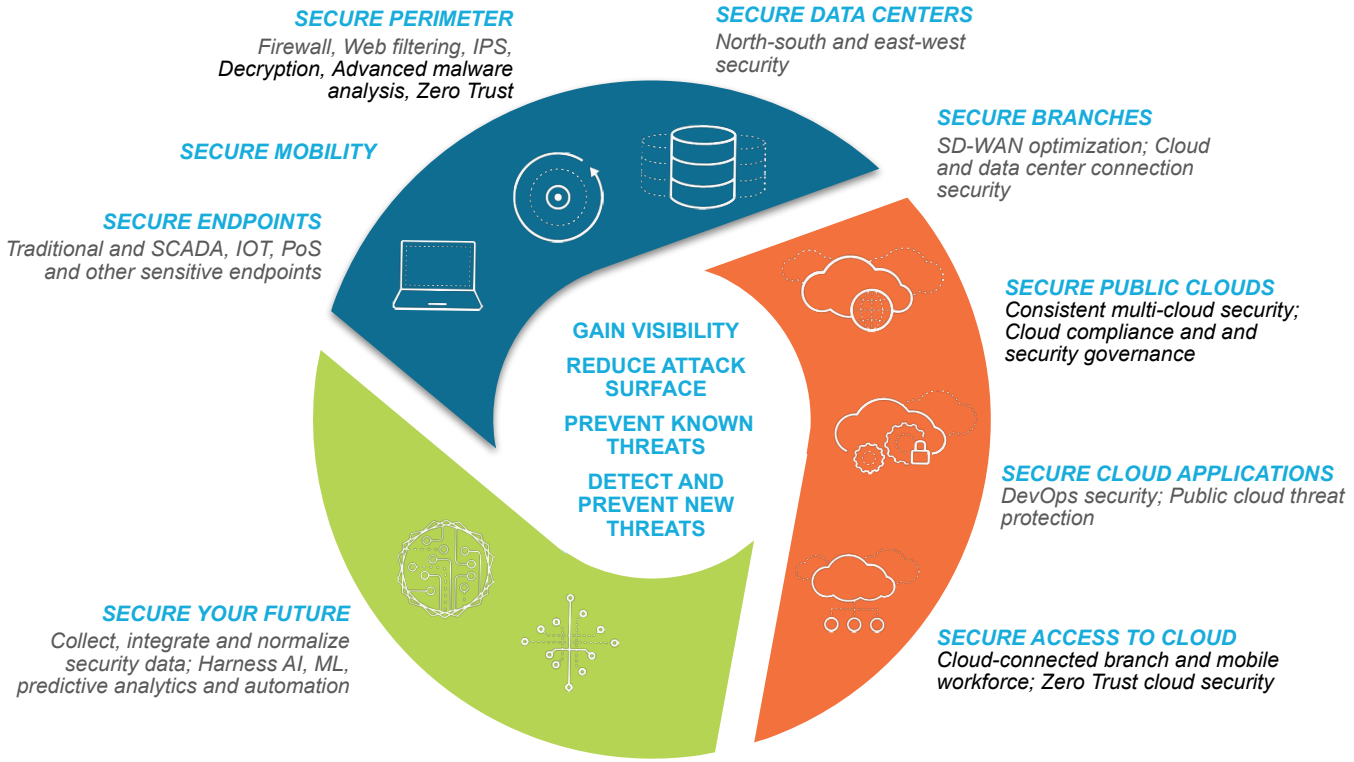
Thank you!

www.paloaltonetworks.com

Barry Rosenberg
brosenberg@paloaltonetworks.com

Appendix

Meeting K-12 Priorities and Needs
Start Anywhere: Consistently secure your Enterprise, Cloud or Future



Cortex XDR Capabilities

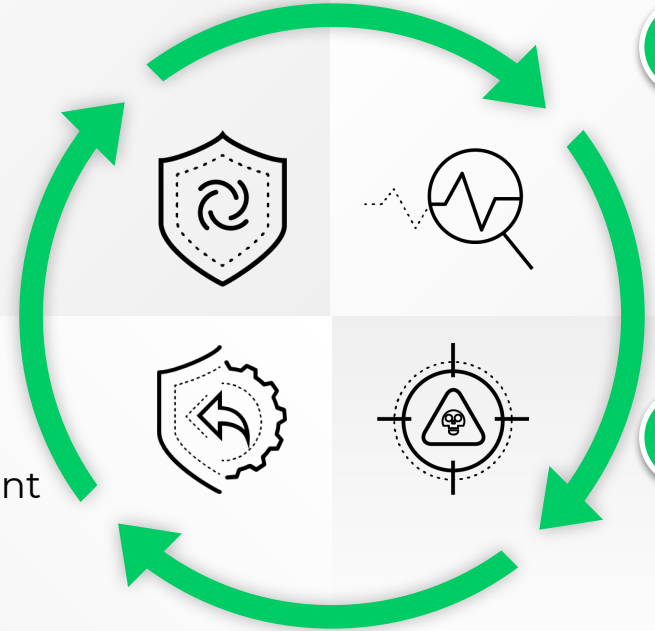
1 Prevent

Market-leading endpoint security

- Next-generation antivirus
- Device control, disk encryption, host firewall

2 Automatically Detect

- Behavioral analytics with machine learning
- Customizable detection
- Vulnerability management



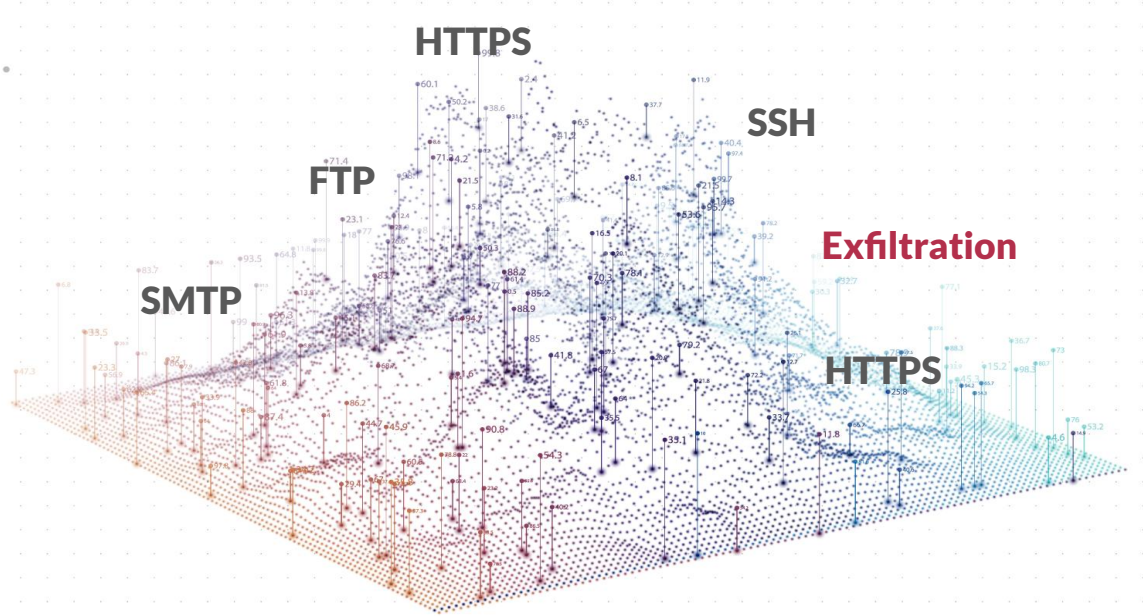
3 Rapidly Investigate

- Root cause & timeline analysis
- Threat hunting
- Integrated threat intel

4 Respond & Adapt

- Integrated enforcement
- Live Terminal
- Search and Destroy

The Most Complete Analytics Compared to NTA, UBA, or EDR Vendors



Behavioral analytics per customer for NTA, UBA

AI-based analysis with WildFire & Cortex XDR agent

Crowdsourced analytics to improve accuracy