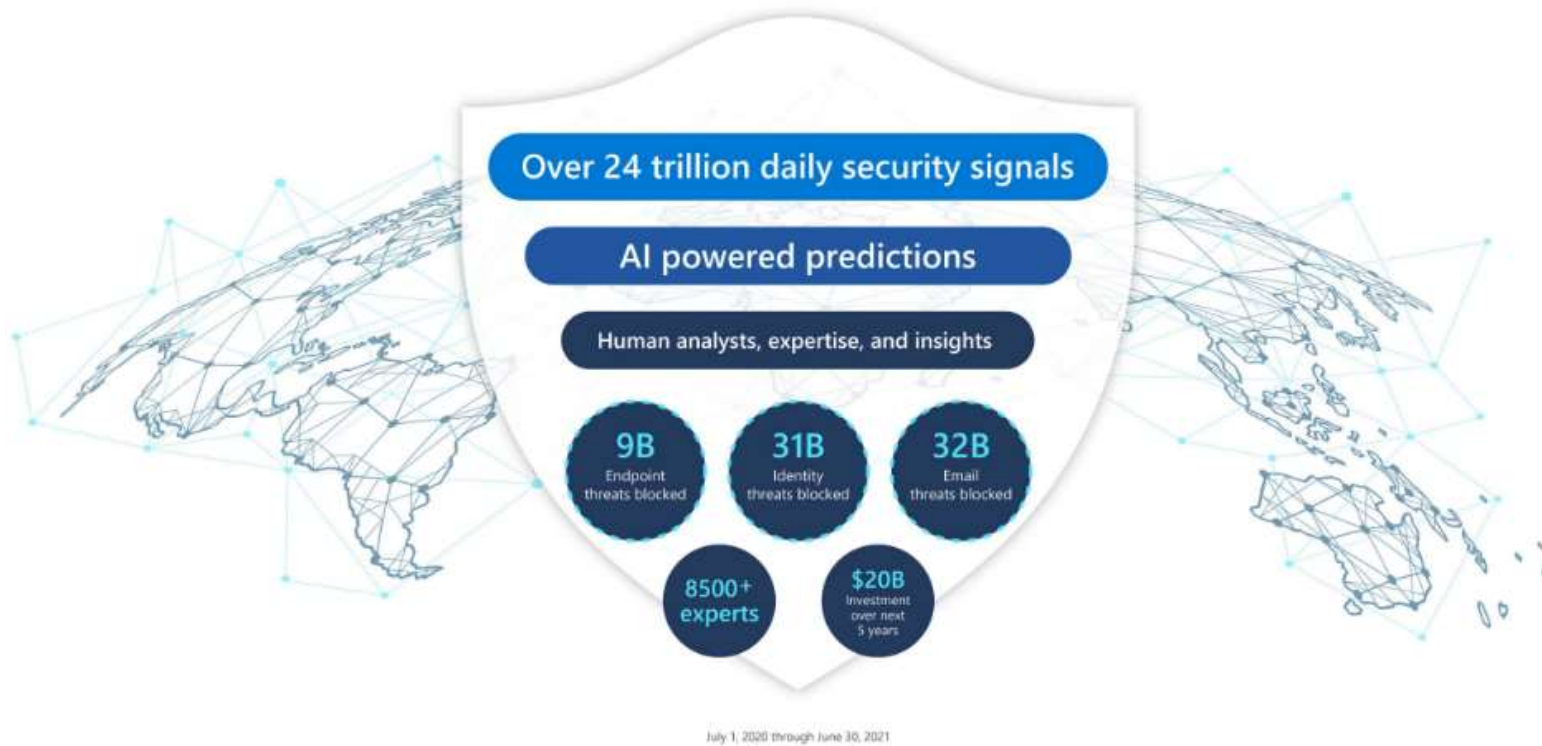**Microsoft**

Advancing Oregon's Cybersecurity

Michael Mattmiller
February 15, 2023

Microsoft security signals

Volume and diversity of signals processed by Microsoft

Over 24 trillion daily security signals

AI powered predictions

Human analysts, expertise, and insights

| 9B | 31B | 32B |
| Endpoint threats blocked | Identity threats blocked | Email threats blocked |

8500+ experts

$20B Investment over next 5 years

July 1, 2020 through June 30, 2021

THE MICROSOFT DIGITAL DEFENSE REPORT DRAWS ON INSIGHTS, DATA, AND SIGNALS FROM ACROSS MICROSOFT, INCLUDING THE CLOUD, ENDPOINTS, AND THE INTELLIGENT EDGE.
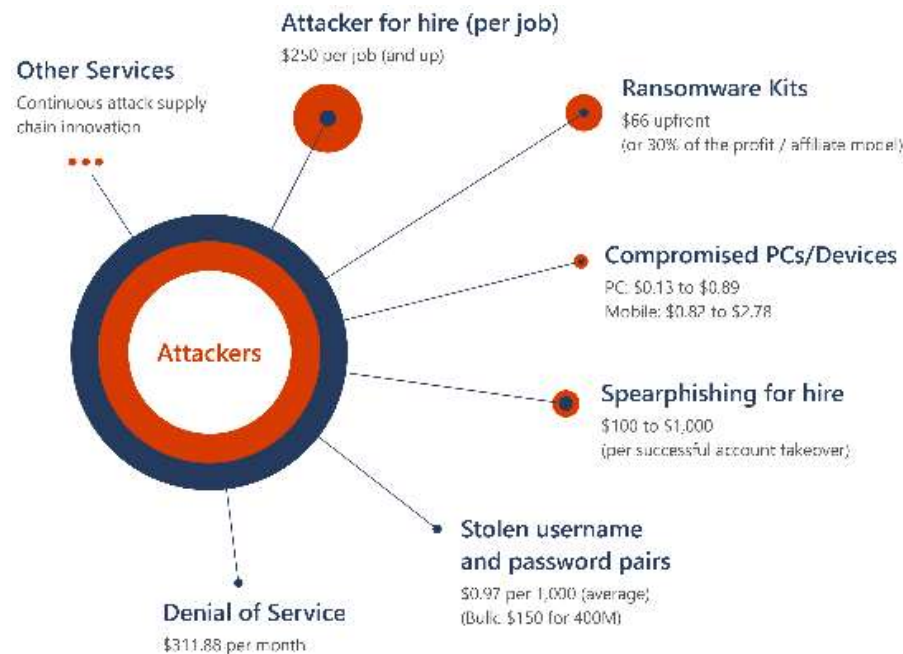
The state of cybercrime

- A threat to national security
- Cybercriminals attacking all sectors
- Ransomware attacks increasingly successful
- Cybercrime supply chain continues to mature

POSITIVE TRENDS
- Transparency: governments and companies coming forward
- Priority: new laws, task forces, resources, partnerships

The cybercrime economy and services

Other Services
Continuous attack supply chain innovation

Attacker for hire (per job)
$250 per job (and up)

Ransomware Kits
$66 upfront
(or 30% of the profit / affiliate model)

Compromised PCs/Devices
PC: $0.13 to $0.89
Mobile: $0.82 to $2.78

Attackers

Spearphishing for hire
$100 to $1,000
(per successful account takeover)

Stolen username and password pairs
$0.97 per 1,000 (average)
(Bulk: $150 for 400M)

Denial of Service
$311.88 per month

WITH NO TECHNICAL KNOWLEDGE OF HOW TO CONDUCT A CYBERCRIME ATTACK, AN AMATEUR THREAT ACTOR CAN PURCHASE A RANGE OF SERVICES TO CONDUCT THEIR ATTACKS WITH ONE CLICK.

What we're seeing in ransomware data and signals

Ransomware encounter rate (machine count): Enterprise customers (Defender data)
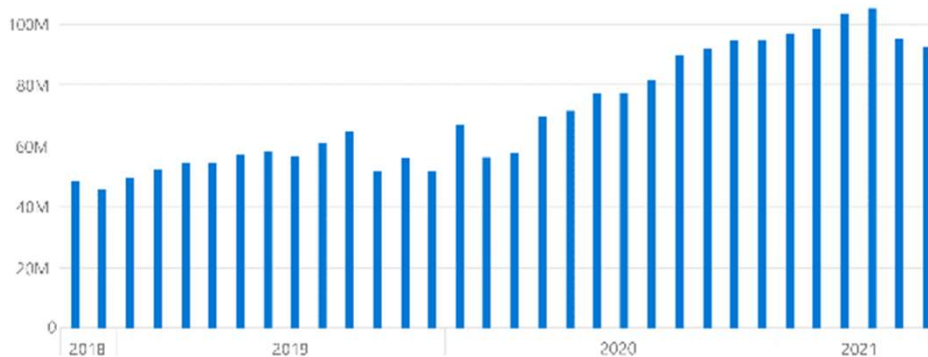
Overall increase in ransomware encounters, with notable surge to consumer and commercial encounters in late 2019,6 when RaaS started to grow, and in early 2020 at the onset of the COVID-19 pandemic.

DART ransomware engagements by industry (July 2020-June 2021)
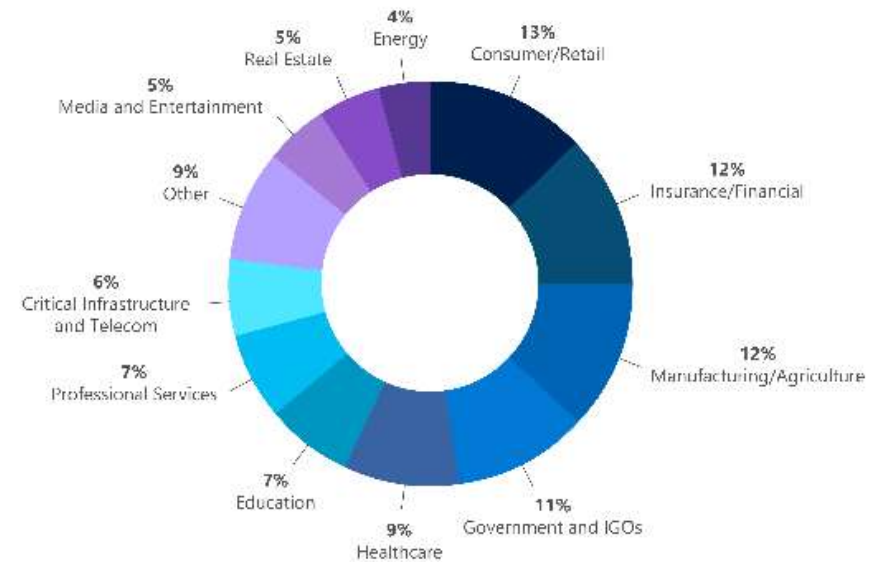
Deploy ransomware protection

1. **Prepare a recovery plan**
Recover without paying

2. **Limit the scope of damage**
Protect privileged roles

3. **Make it harder to get in**
Incrementally remove risks

The stakes have changed. There is a massive growth trajectory for ransomware and extortion.

The cybersecurity bell curve:

Basic security hygiene still protects

Zero Trust across the digital estate

VISIBILITY

AUTOMATION

ORCHESTRATION

SOME KEY THEMES IN THE REPORT:

- INTEGRATE CYBERSECURITY INTO BUSINESS DECISION MAKING

- TREAT CYBER AS A BUSINESS RISK

- RESILIENCE INCLUDES CYBERSECURITY

Microsoft's commitment to accelerate cybersecurity

MODERNIZE

SECURE

DEFEND

Benefits available to US State and select Local Governments

Modernize legacy software: productivity products including Windows, Exchange and SharePoint

One-year advanced protection package

Zero Trust guidance for configuration

Custom deployment services

Training for government IT and Security teams

Urgent action is needed to address the cybersecurity skills crisis

Cyberattacks threaten our privacy, national security, and our daily lives.


Only 3% of US students are attaining a credential in computer and information sciences, far fewer specialize in cybersecurity.

With nearly 500,000 open cybersecurity roles in the US, skills in cybersecurity can help launch students into high-growth, high-paying jobs.

Our commitment

Help **skill 250,000 people in cybersecurity by 2025**— starting with new community college and nonprofit partnerships—to **cut the US talent gap by 50%**
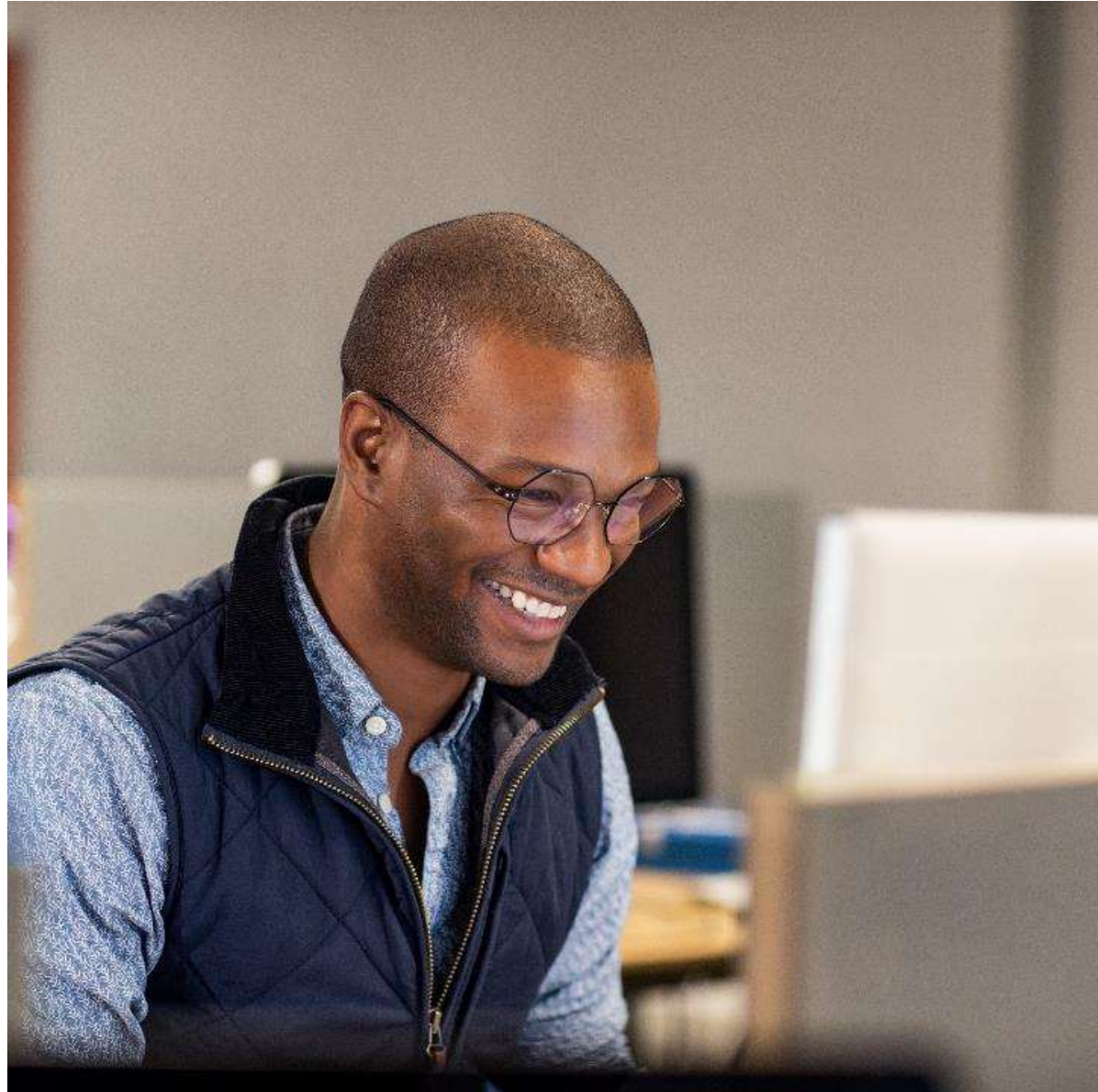
Supporting Oregon with cybersecurity resources

Faculty professional development support

Community of practice to support expanding cybersecurity programs

Scholarships for low-income students including Veterans

Ready-to-teach curriculum and teaching materials

Microsoft

View the Digital Defense Report report
https://aka.ms/MDDR

Learn more about Microsoft's Cybersecurity Community College commitment:
Microsoft on the Issues

Learn more about Microsoft in Government
https://www.microsoft.com/government

Thank you