BLACKFOG Webinar

Introducing ADX:
The New Standard in Cybersecurity Protection

Thursday,
November 18th
10am PT / 6pm GMT



Dr. Darren Williams
Founder & CEO,
BlackFog, Inc.



Michael Sampson
Senior Analyst,
Osterman Research

www.blackfog.com

Introductions



Dr. Williams is a serial entrepreneur and founder of 3 technology startups over the last 20 years, two of which have been sold to public companies. He is currently the founder and CEO of BlackFog, Inc. a global cyber security company focusing on ransomware prevention and cyber warfare.

Dr. Williams holds a Ph.D. and Bachelor of Science with Honors from the University of Melbourne, authoring several scientific papers and software applications for auto-radiographic densitometry and analysis.



© 2021 BlackFog & Osterman Research

Introductions



Michael is the Senior Research Analyst at Osterman Research, with broad interests in cybersecurity, data protection and information governance.

Michael is the author of seven books on collaboration and user adoption, including Re-Imagining Productive Work with Office 365, User Adoption Strategies (2nd Edition), and Collaboration Roadmap.

Michael holds a Master of Commerce with first-class honors in telecommunications-based IT from the University of Canterbury in New Zealand.



© 2021 BlackFog & Osterman Research

Survey Design

Respondents	Firm Size	Industry
CIO/IT manager, CISO/security manager, Cybersecurity professional	Requirement >250 employees (actual average 5,620)	Cross-industry
Familiar with how organization protects against data exfiltration	250-1000 n=132 >1000 n=123	

© 2021 BlackFog & Osterman Research

Research Finding

Data exfiltration is a key element in many cybersecurity incidents

© 2021 BlackFog & Osterman Research

Cybersecurity incidents with data exfiltration



© 2021 BlackFog & Osterman Research

Research Finding

Organizations want to prevent data exfiltration

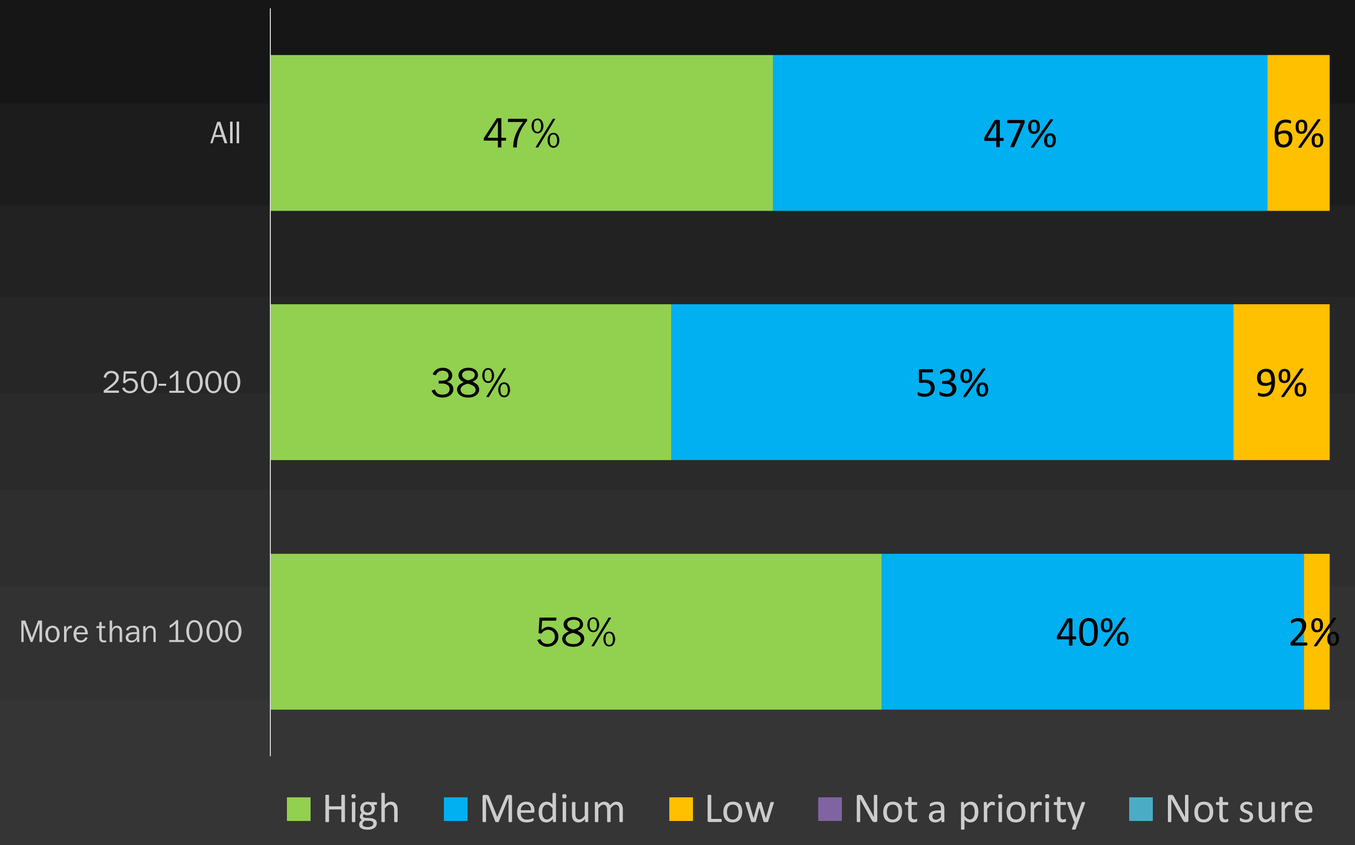
© 2021 BlackFog & Osterman Research

Data Exfiltration a Top Priority

94%

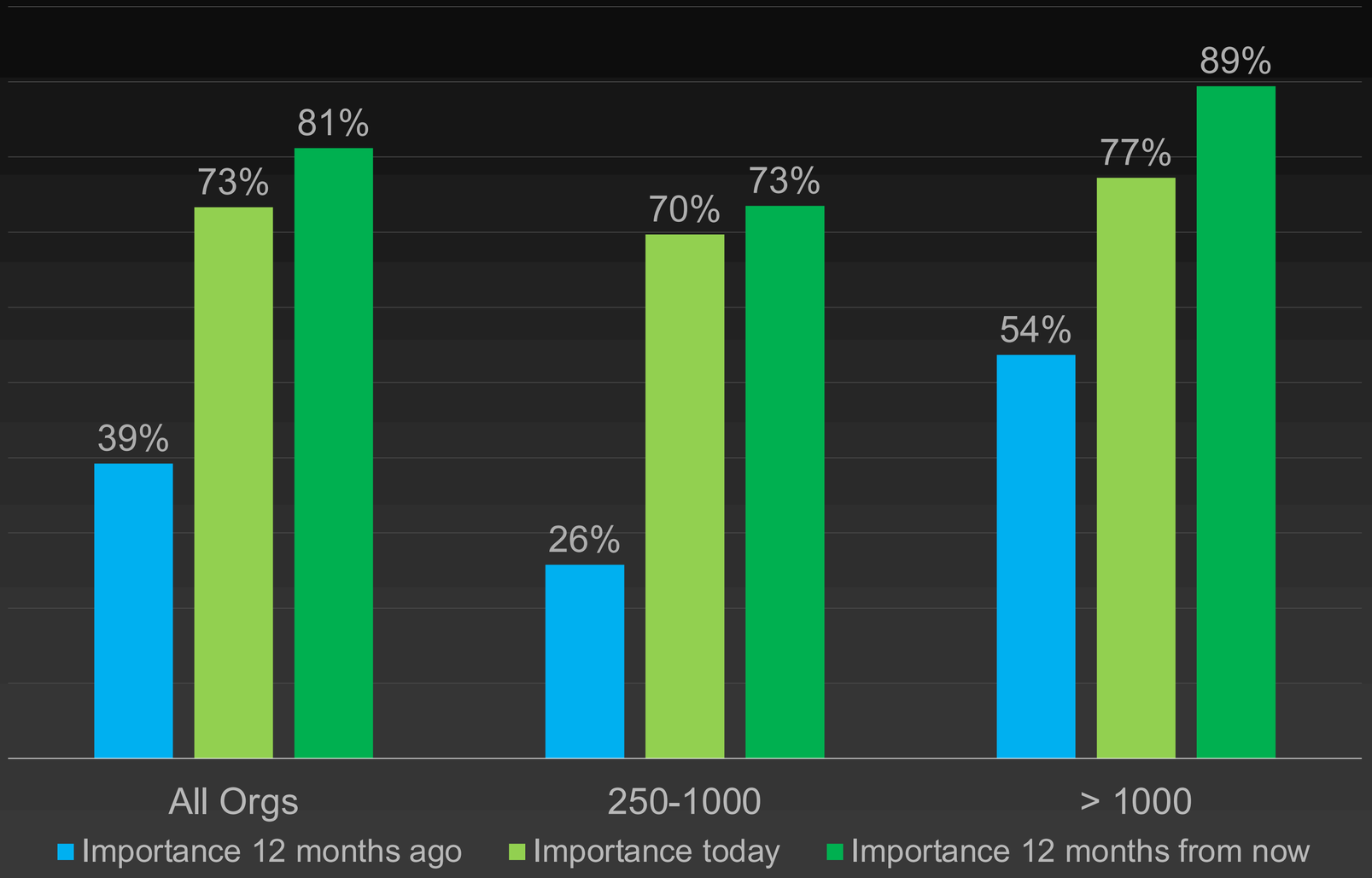


Of organizations consider
Anti Data Exfiltration a top priority



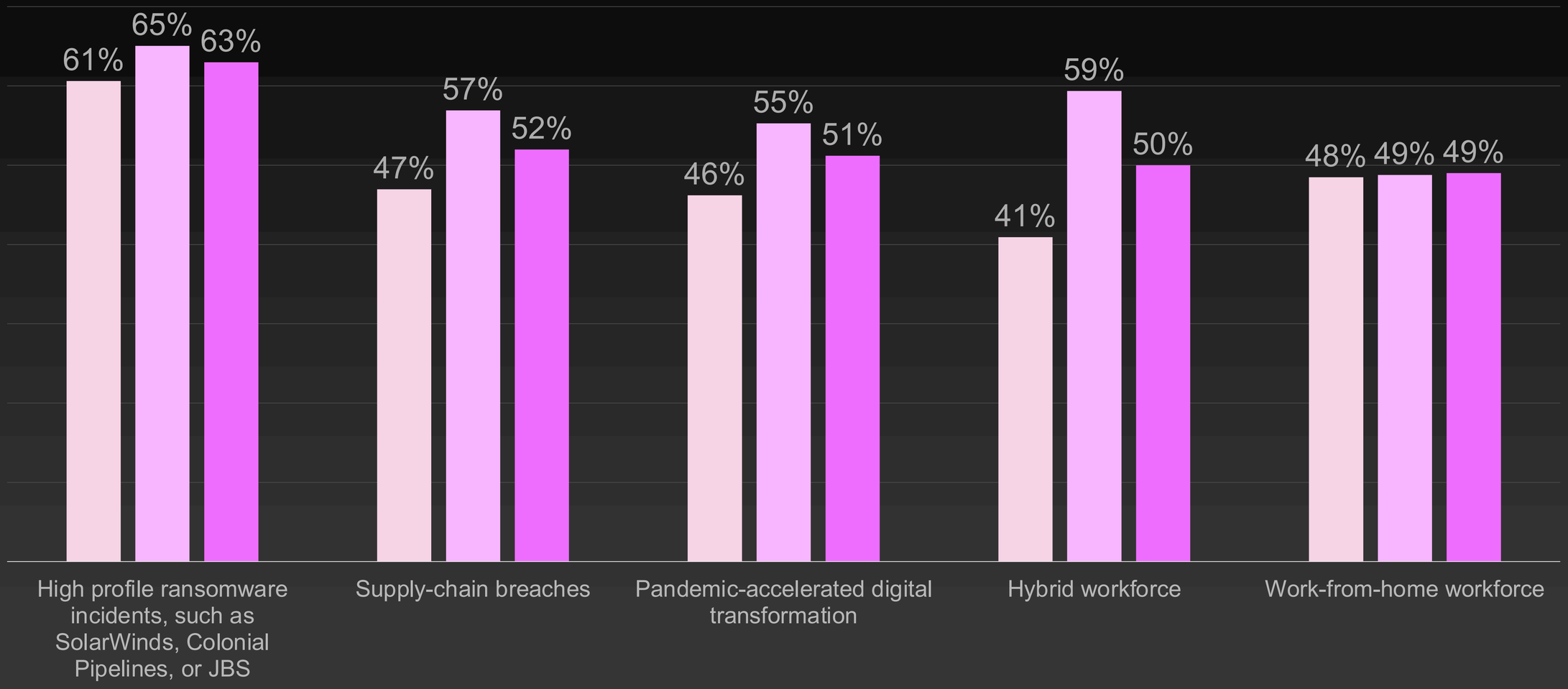
© 2021 BlackFog & Osterman Research

Priority is increasing YoY



© 2021 BlackFog & Osterman Research

Wider trends compound the threat



© 2021 BlackFog & Osterman Research

Research Finding

Current cybersecurity protections are not stopping data exfiltration

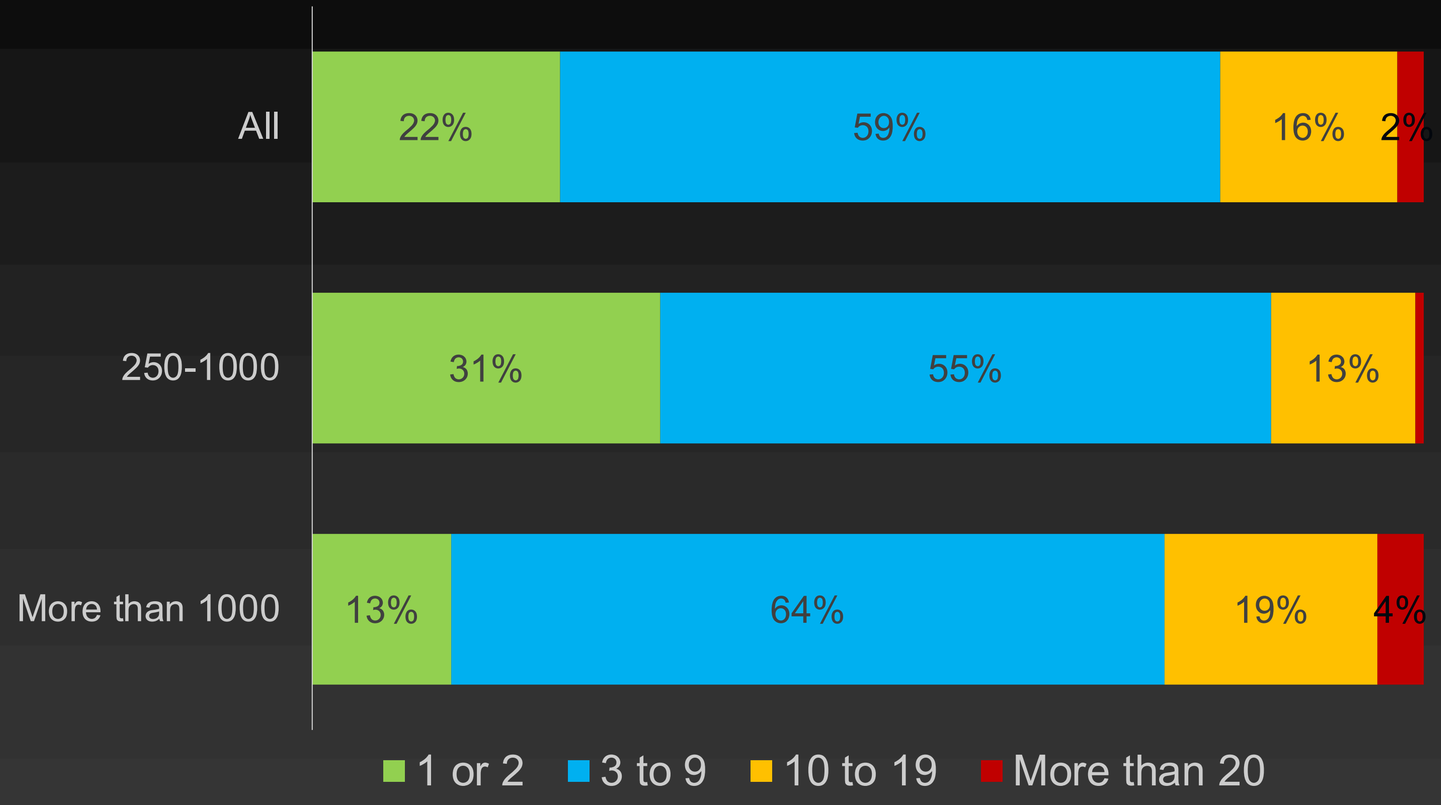
© 2021 BlackFog & Osterman Research

Number of Tools



80%

Currently use up to 10 cybersecurity solutions



© 2021 BlackFog & Osterman Research

Types of Tools

1 or 2 Tools

- Anti-Virus
- Backup

3 to 9 Tools

- Anti-phishing
- Anti-ransomware
- Secure email
- Secure web
- Firewall
- MFA
- Security training

10-19 Tools

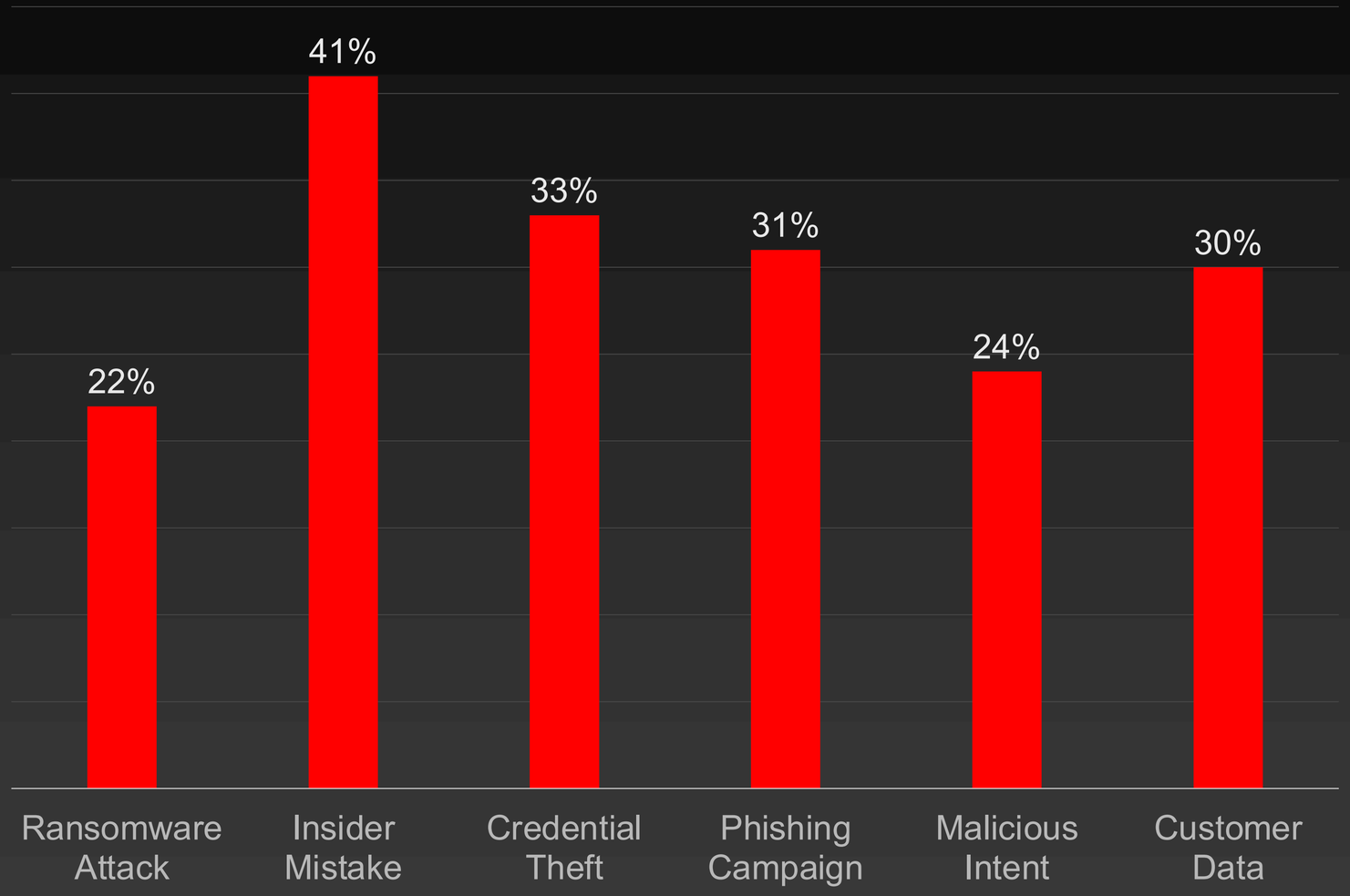
- Endpoint
- Threat Intel
- Vulnerability
- Managed services
- DLP
- Cloud backup
- MDM
- EDR/XDR
- SIEM
- SOAR

© 2021 BlackFog & Osterman Research

Data is Still Being Exfiltrated



Almost 3/5 organizations are not confident in their ability to stop data exfiltration in a ransomware attack



© 2021 BlackFog & Osterman Research

Low Confidence in DLP

68%

Say existing data loss prevention (DLP) tools are difficult to configure



51%

Say DLP cannot prevent data exfiltration

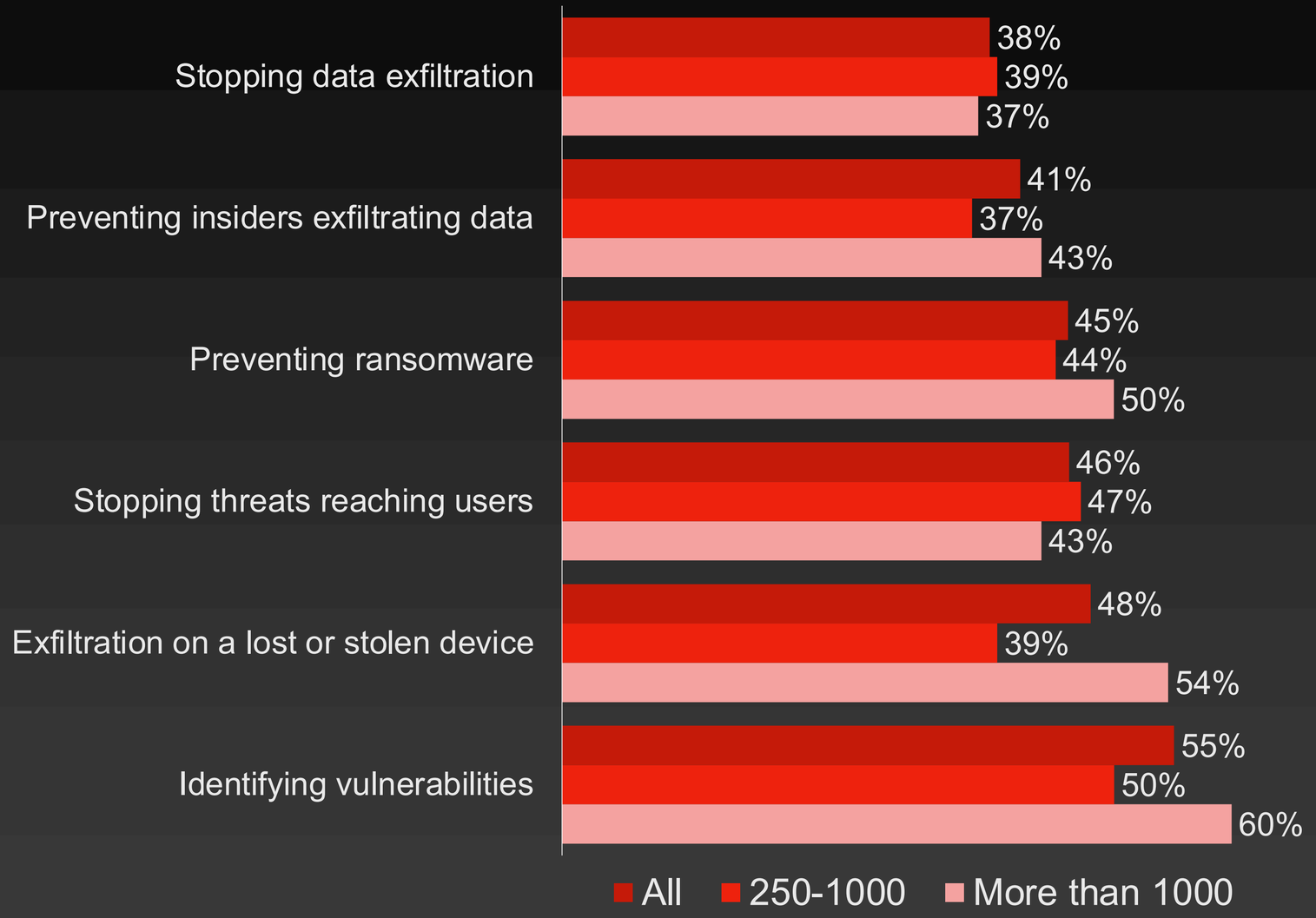
© 2021 BlackFog & Osterman Research

No Confidence



62%

Have no confidence that their current cybersecurity tools prevent data exfiltration



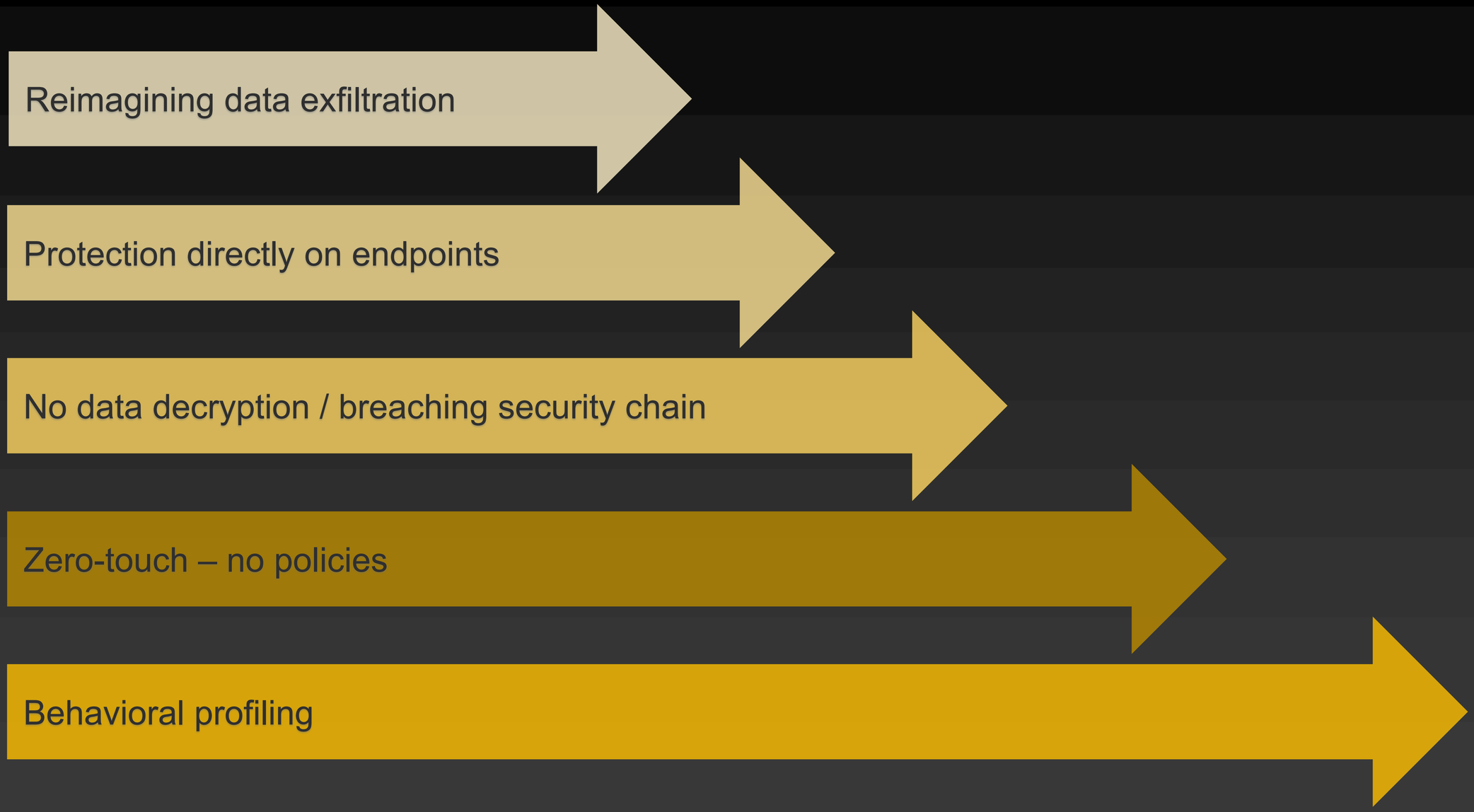
© 2021 BlackFog & Osterman Research

Research Finding

Something new is needed: Introducing Anti Data Exfiltration (ADX)

© 2021 BlackFog & Osterman Research

Key Attributes of ADX



© 2021 BlackFog & Osterman Research

ADX versus DLP

Attribute	ADX	DLP
Policy Creation	None to low	High
Policy Management	None to low	High
Detection Method	Behavioral Packet monitoring	Signature and pattern matching
Deployment Location	Endpoint	Edge of Network/ Cloud
Encryption Handling	Honors Security Chain	Requires Decryption
IT Management Effort	Low	High
Ability to Bypass	Low	High
Cost	Low	High
Expertise Required	Minimal	Significant

© 2021 BlackFog & Osterman Research

Conclusion

Despite threats, urgency, and tools, data exfiltration is still happening

© 2021 BlackFog & Osterman Research

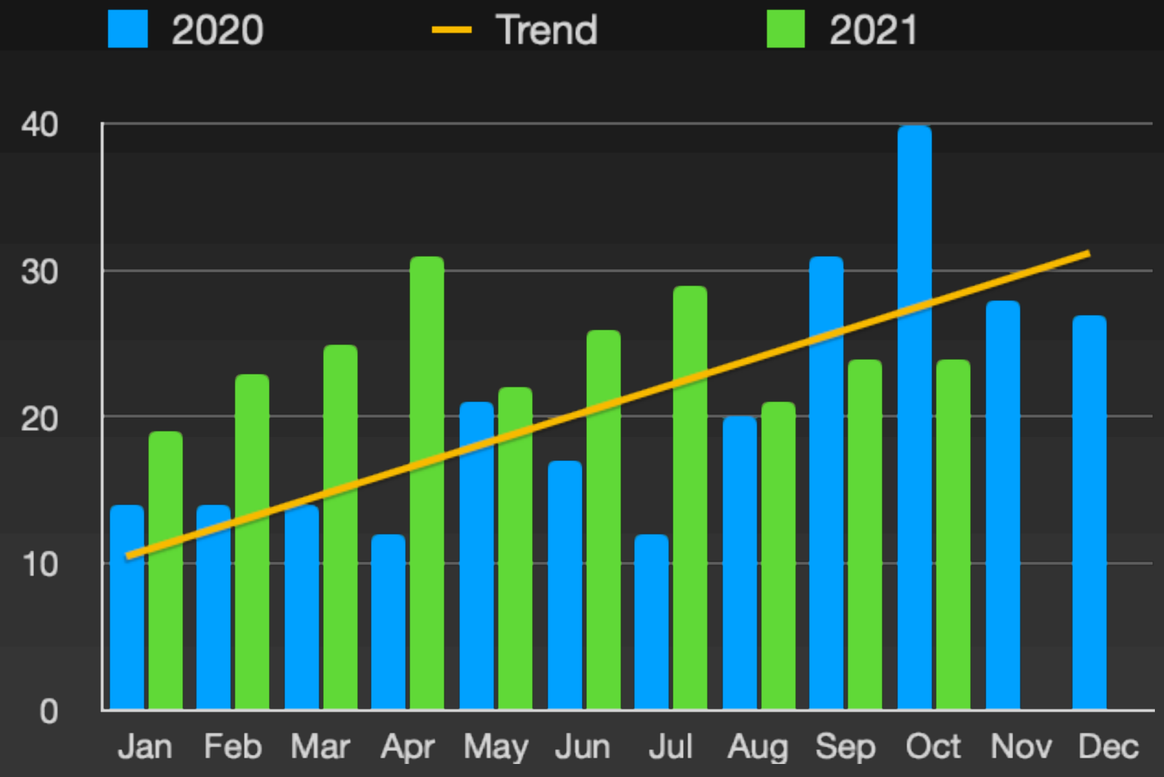
Conclusions

1. Best of breed solutions are failing
   - Even @ large orgs with over 10 tools
2. Cyberattacks focus on extortion
   - Defensive approaches don’t solve the problem
3. Anti Data Exfiltration Critical
   - Without exfiltration cyberattacks are neutralized

© 2021 BlackFog & Osterman Research

2021 The Year Ransomware Broke Through

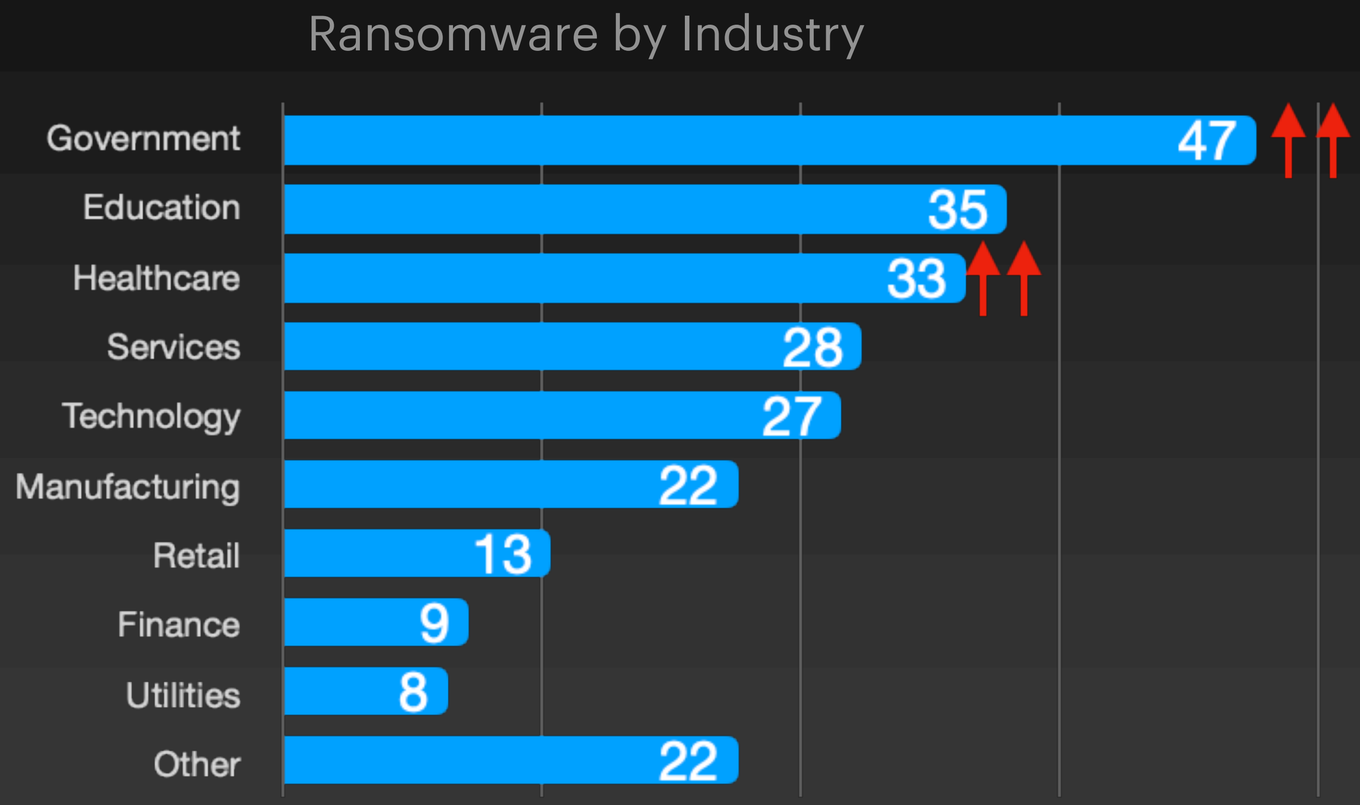
- New records in 2021
- Ransomware eclipsed all of 2020 in first 10 months of the year
- Will cost over 6 trillion this year
- Average ransom payout is now $570k up 82%
- Average demand 5.3m up 518%
- Globally
  - USA 50%
  - UK 11%



Statistics Copyright © 2021 BlackFog, Inc.

How did we get Here?

- No Industry is immune
- Cyber gangs target low hanging fruit
- Easy high value targets
  - Government
  - Education
  - Healthcare
- Typically lack investment, talent and resources
- Why now?
  - Gangs are coordinated
  - Access to AI
  - 80% Effective at bypassing AV



Statistics Copyright © 2021 BlackFog, Inc.

The Cost of Doing Nothing

- Many reasons for attacks
  - Extortion
    - Double and triple
  - Espionage
  - Insider threats
  - Warfare / disruption
- Cost of an attack
  - Direct cost (ransom)
  - Business disruption
  - Remediation
  - Lawsuits
  - Government fines



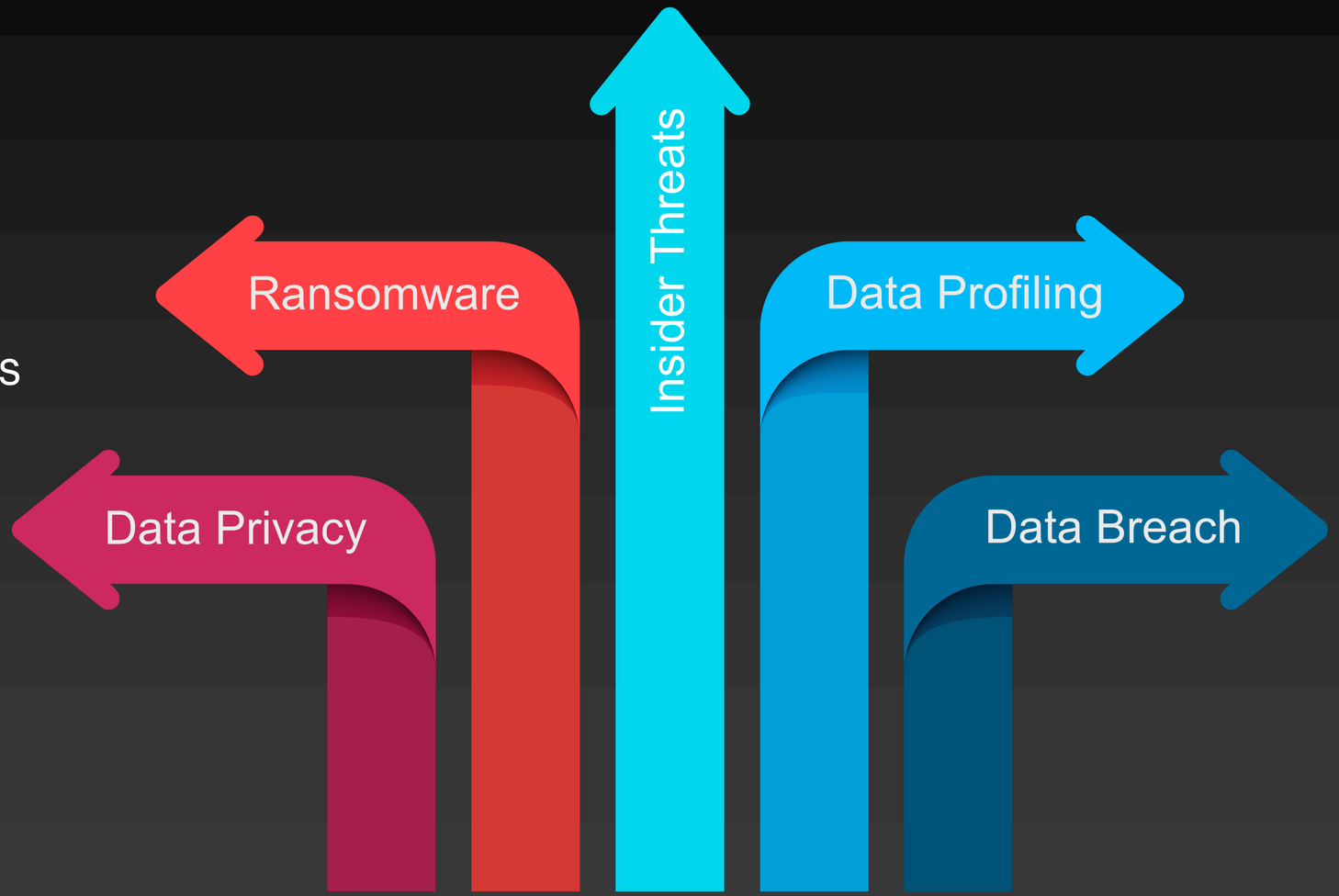
Fighting Back

- Security typically focuses on traditional approaches
  - Defensive
  - Firewalls
  - AV solutions
- Solutions clearly ineffective
  - Record attacks
  - Record breaches / data loss
  - Cybercriminals bypass solutions
    - Polymorphism
    - AI Training
    - Phishing
    - Dwell time



Anti Data Exfiltration (ADX)

- Assumes the attackers will get in
  - Focuses on prevention
  - Stops data leaving the device
  - Stops communication to C2 Servers
  - Stops lateral movement
  - Stops insider threats
  - Stops exfiltration to restricted countries
  - Stops data breaches



7 Day Ransomware Assessment

7
Days

25
Devices

4
Platforms

Consultant with VP of Threat Intelligence
Law enforcement professional and forensics expert

Detailed report produced highlighting what was discovered

Examples Case Studies & Stories from the trenches...

Case Study: Auto Parts Manufacturer

Thursday

- Assessment set for Monday morning
- License sent in advance of meeting

Friday

- IT Manager decides to install on 4 devices before weekend
- Unaware to Manager this was in full production mode

Saturday

- From Friday 11:30pm to Saturday 2:30am massive attack underway
- BlackFog preventing all C2 communication and exfiltration

Monday

- We explained findings to VP / Gen Manager
- Suspicious we had set this up, until IT explained that he validated the finding

Now a happy BlackFog customer

Case Study: Building Materials Manufacturer

Tuesday

- Assessment begun on 10 devices
- Training mode enabled

Tuesday

- 10:43pm 1,314 Ransomware attacks on owners device
- Moved to production mode and attacks stopped

Wednesday

- No Activity on any device

Thursday

- Attacks begin on Owners Wife’s device
- 49,000 Ransomware attempts. All Blocked.

Attacks stopped after 4 days and they moved onto other victims. Now a happy BlackFog customer

Contact us







@blackfogprivacy



/company/blackfog

Dr. Darren Williams
Founder & CEO
dwilliams@blackfog.com



@OstermanRsch



/company/osterman-research-inc.

Michael Sampson
Senior Analyst
michael.sampson@ostermanresearch.com

© 2021 BlackFog & Osterman Research