THOMSON REUTERS® | Microsoft

Ransomware: What Firms Need to Know!

HOUSEKEEPING

RECORDING

You will be provided with a recording of today's presentation

YOUR QUESTIONS

Use the "Ask a Question" function to submit

LEARN MORE

Visit legal.tr.com for insights and tips

JOIN US ON SOCIAL

@EliteLink @Azure on Twitter

TODAY'S SPEAKERS

JESSE MRASEK

Senior Cloud Solutions Architect,
Microsoft
Mrajess@microsoft.com

MARK GENDEIN

Principal Architect, Legal Technology,
Thomson Reuters
Mark.Gendein@thomsonreuters.com

COLLEEN SCIMECA

Sr. Product Strategist, Legal Technology,
Thomson Reuters
Colleen.Scimeca@thomsonreuters.com

TODAY'S AGENDA

- Ransomware in Legal
- How it Happens
- Hybrid Work Environment
- Prevention / Mitigation
- Security Benefits with the Microsoft & Thomson Reuters Partnership
- Key Takeaways
- Q&A

POLL #1
QUESTION

What is

Ransomware?

A type of **malicious software** designed to **block access** to a computer system until a **sum of money is paid**

Who are these

Ransomware People?

Ransomware as a Service (RaaS)

Well organized group

Complex payments

What if we just

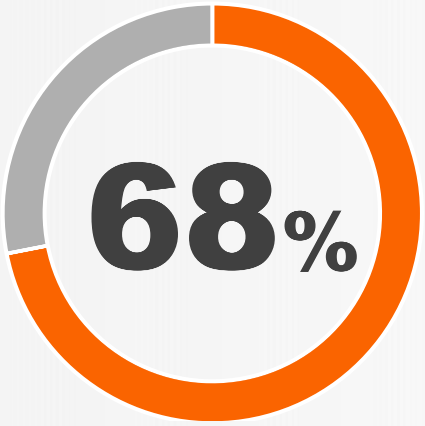
Pay the Ransom?

Mined your data

Sold your data

Released your data to the public

Re-extort you

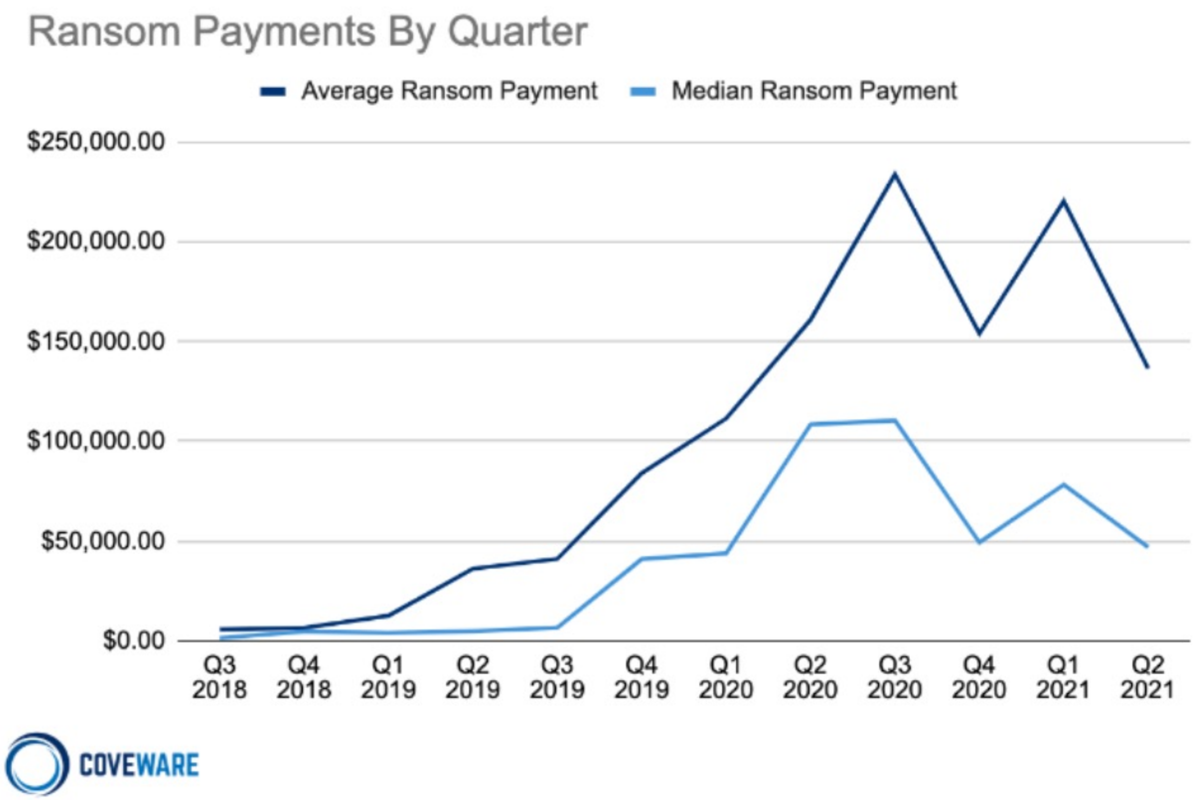


face a 2nd attack
within a year

*https://www.darkreading.com/application-security/ransomware-makes-up-half-of-all-major-incidents/d/d-id/1339667

Ransomware Stats

Q2 2021 Coveware Stats:



Average Ransom Payment

$136,576

Average Days of Downtime

23 Days

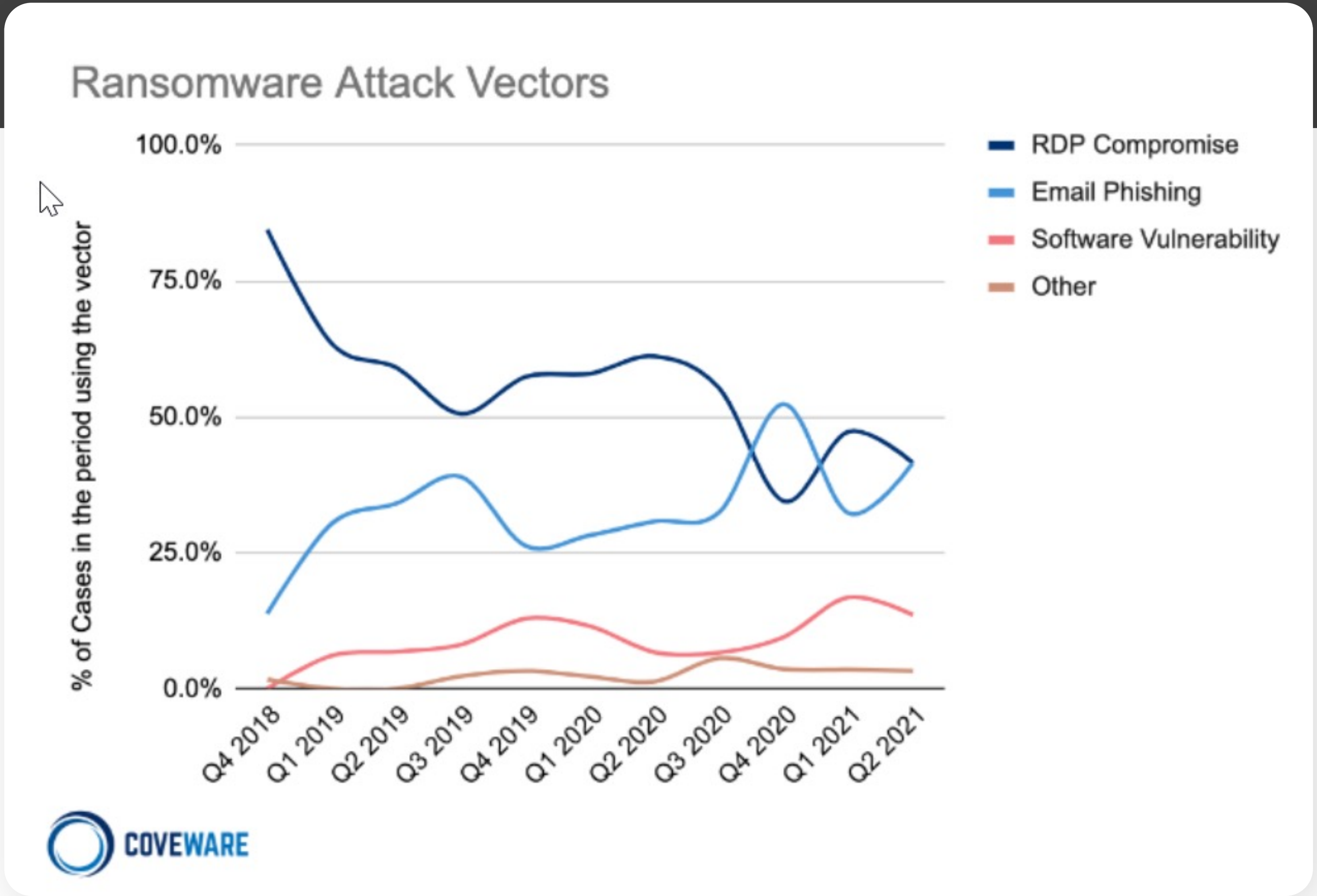
https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority

How cyber criminals get in

- **RDP (Remote Desktop Protocol)**
  weak/reused password

- **Email phishing**
  a scam by which an Internet user is duped

- **Social Engineering**
  when fraudsters pretend to be someone or something else to win a person's trust.



Ransomware attacks are a risk for firms large and small

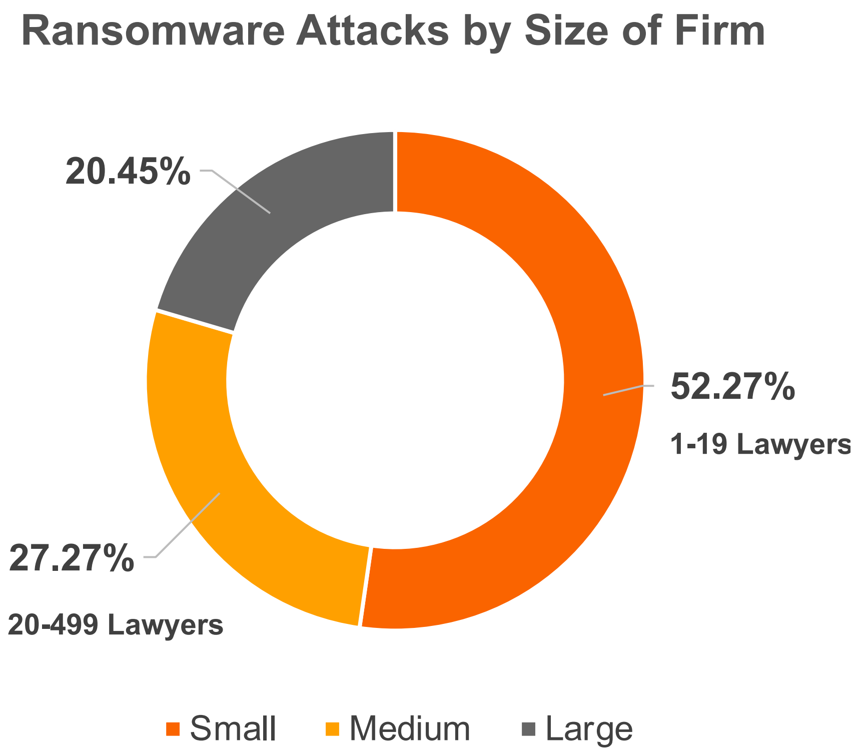


Figure 1: Ransomware Attacks by Law Firm Size
Source Tari Schreider Ransomware Attack Database

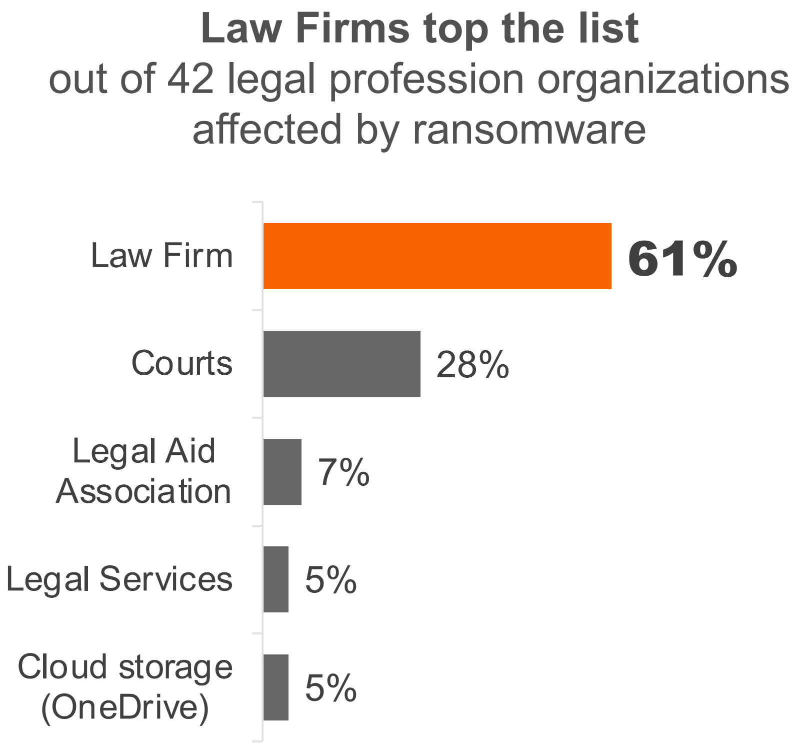
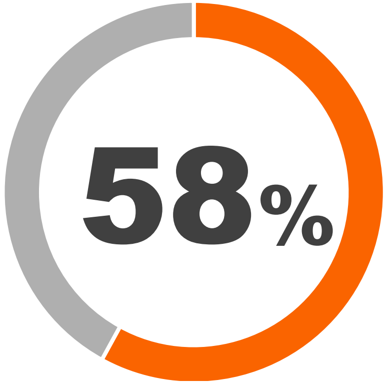


Figure 2: Ransomware Attacks by Legal Organization
Source Tari Schreider Ransomware Attack Database

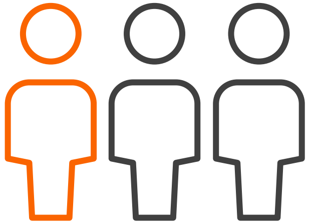
https://www.law.com/corpcounsel/2020/05/26/ransomware-attacks-in-the-legal-profession/

THOMSON REUTERS®

Ransomware in Law Firms



Small and midsize law firms have experienced a ransomware incident



1 in 3

Have been attacked in the last 12 months

69%

Law firms pay the ransom

But only

65%

(2 in 3) firms regain access to their data

So

35%

of firms pay a ransom only to get nothing in return

https://blog.capterra.com/law-firm-ransomware/

THOMSON REUTERS®

How it happens

a demonstration

Why Are Law Firms Being Targeted?

Law firms – one-stop shop for holding voluminous sensitive client data!

- Financial Records
- Medical Records
- Passport #s
- Biometric Data
- Social Security #s
- Company Trade Secrets
- Client Tax Documents
- Health Insurance Info
- Credit Card Info
- M&A Activities
- Online Account Credentials

POLL #2
QUESTION

Impacts of a Hybrid Work Environment

Additional risks:

- Public spaces/networks
- Unsecured personal devices
- Distracted workforce susceptible to phishing

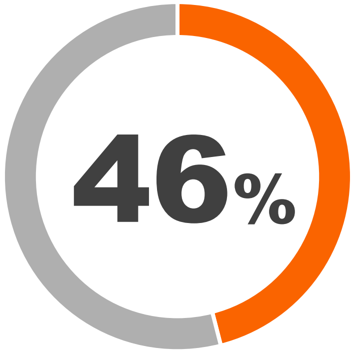
But enhanced security benefits:

- Pushed firms into the cloud for enhanced security
- Less outdated software
- Two-factor authentication
- Machine learning/anomaly detection

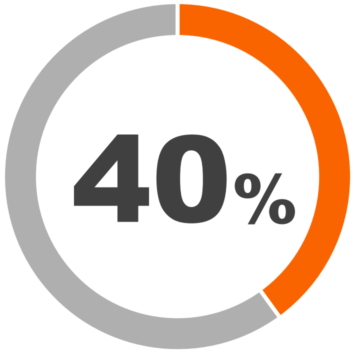
Prevent and mitigate an attack

Firms have a long way to go to prevent cyber security threats

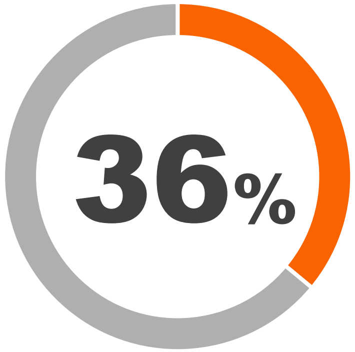
Employees are their greatest risk



of law firms surveyed conduct cyber security training programs to prevent phishing attacks*



of firms indicated they have a disaster recovery/business continuity plan *



of U.S. law firms obtained cyber insurance policies in 2020 **

* The 2020 ABA Legal Technology Survey Report https://www.law.com/legalnewswire/news.php?id=2832120

** https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/

THOMSON REUTERS®

Create a Cybersecurity Culture

- Hold short topical monthly training sessions
- Deliver comprehensive cybersecurity training twice a year
- Run quarterly mock phishing cybersecurity attacks
- Conduct mock calls

  e.g., saying from bank, fiduciary for fake emergency
- Word plug-in for security
- Educate on Phishing, Smishing (SMS Phishing), Spoofing

Very few firms **(5%)** hold trainings at the recommended monthly cadence

*https://www.logicforce.com/2021/01/13/lawfirm-it-scorecard-2021/#top

THOMSON REUTERS®

Prevent an Attack

Audit/Assess

- Cybersecurity Risk Assessment – professional audit
- Audit your 3rd party vendors for privacy/security
- Personal devices vs. firm provided devices

Systems

- Update systems, software, applications, auto-updates
- Block unknown applications
- Back up network

Log-Ins

- Strong passwords
- Multifactor authentication
- Biometric log-in
- Password manager
- Apply security patches
- Use anti-malware programs

Policies

- Have IRP- Incident Response Plan
- Purchase cyber insurance

Mitigation Steps

Demand proof that they have the data and aren’t spoofing!

- Hire data breach expert, digital forensics professional
- Hire ransomware negotiator
- Notify law enforcement
- Notify cyber insurance company but…
- Understand laws/regulations (GDPR, PIPEDA, CCPA, ABA 493)
- Notify affected clients
- To pay or not to pay
- Public statement / PR / Protect Brand
- Work on stopping second attack

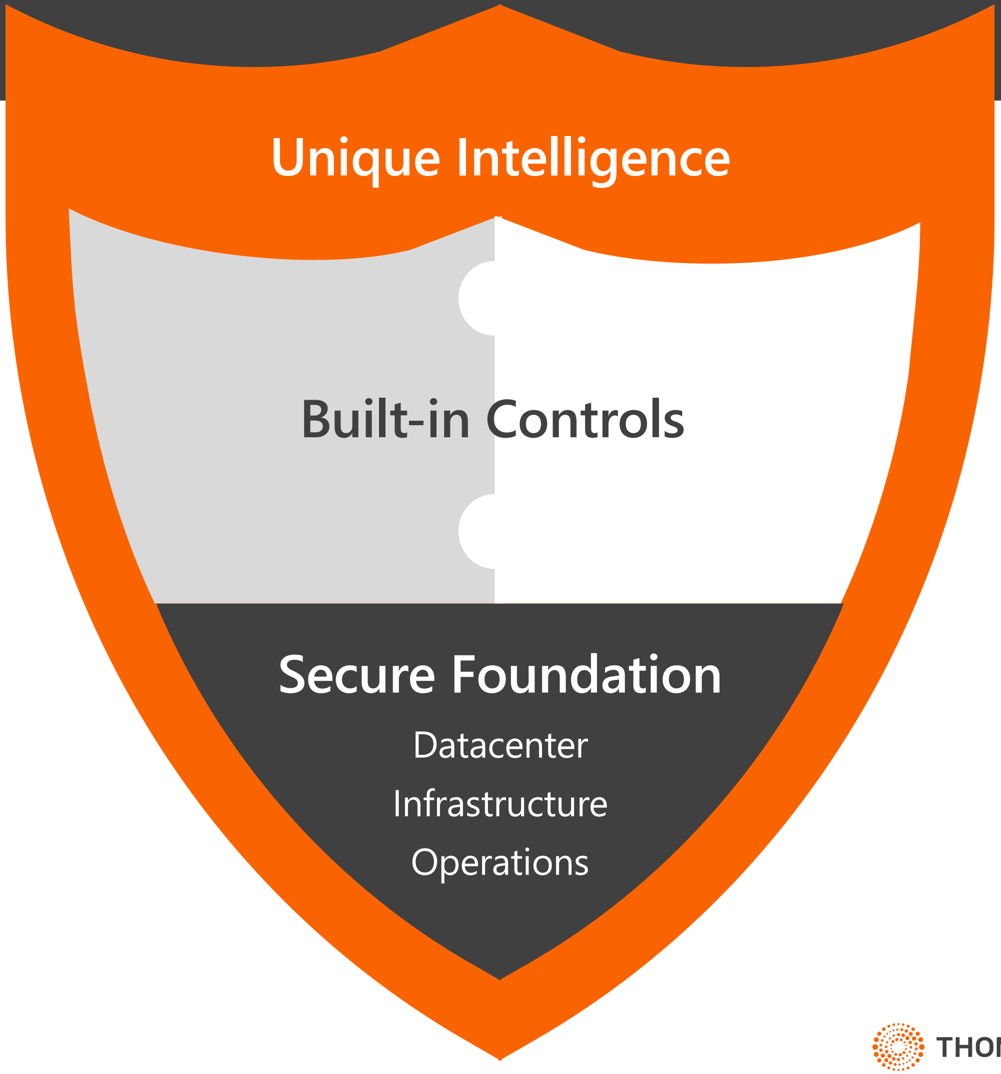
Gain unmatched security

Microsoft Azure

$1B+ annual investments

Over 3500 security experts

Trillions of diverse signals



Unique Intelligence

Built-in Controls

Secure Foundation

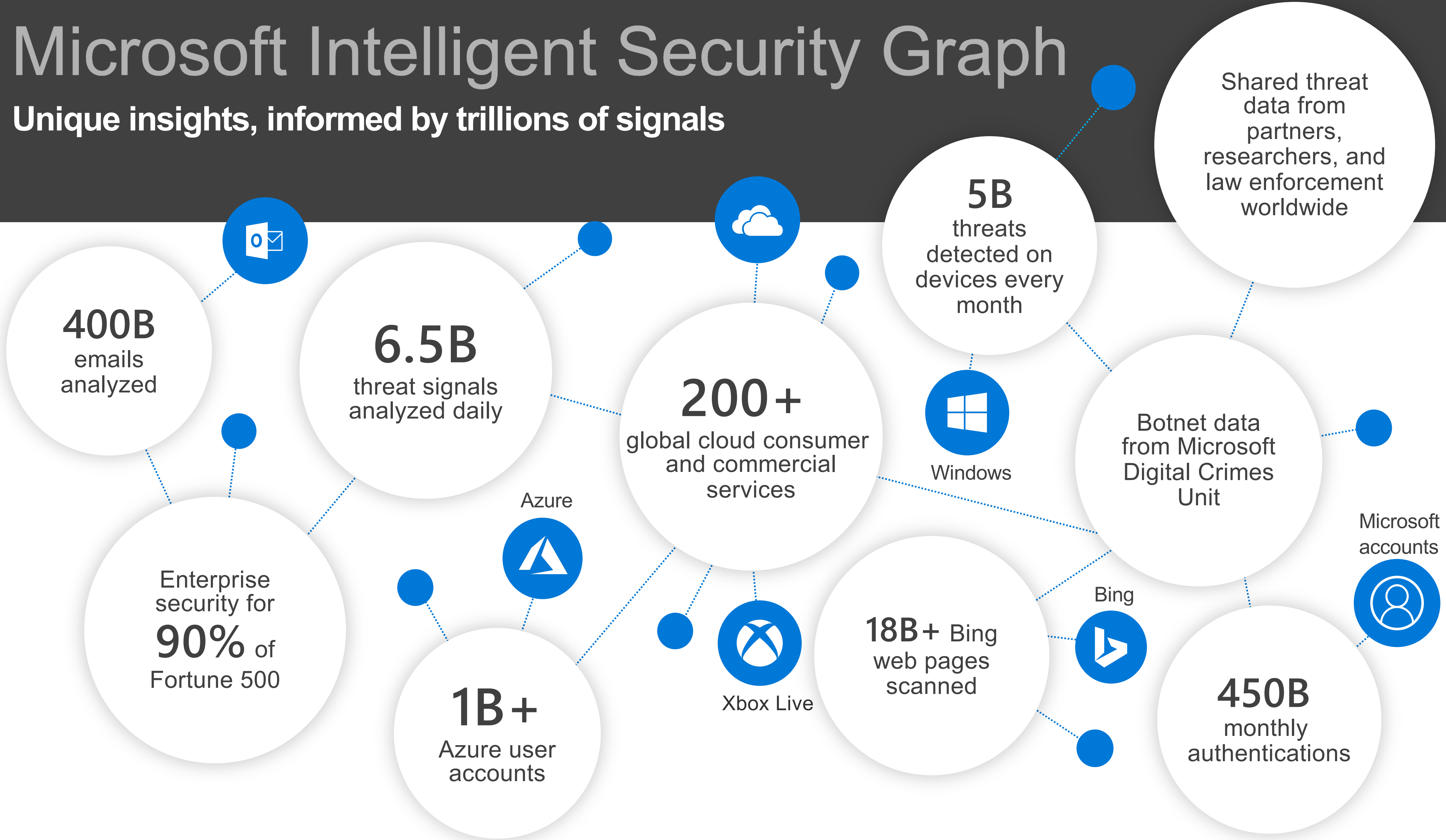
Datacenter

Infrastructure

Operations

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



400B emails analyzed

6.5B threat signals analyzed daily

Enterprise security for **90%** of Fortune 500

1B+ Azure user accounts

200+ global cloud consumer and commercial services

5B threats detected on devices every month

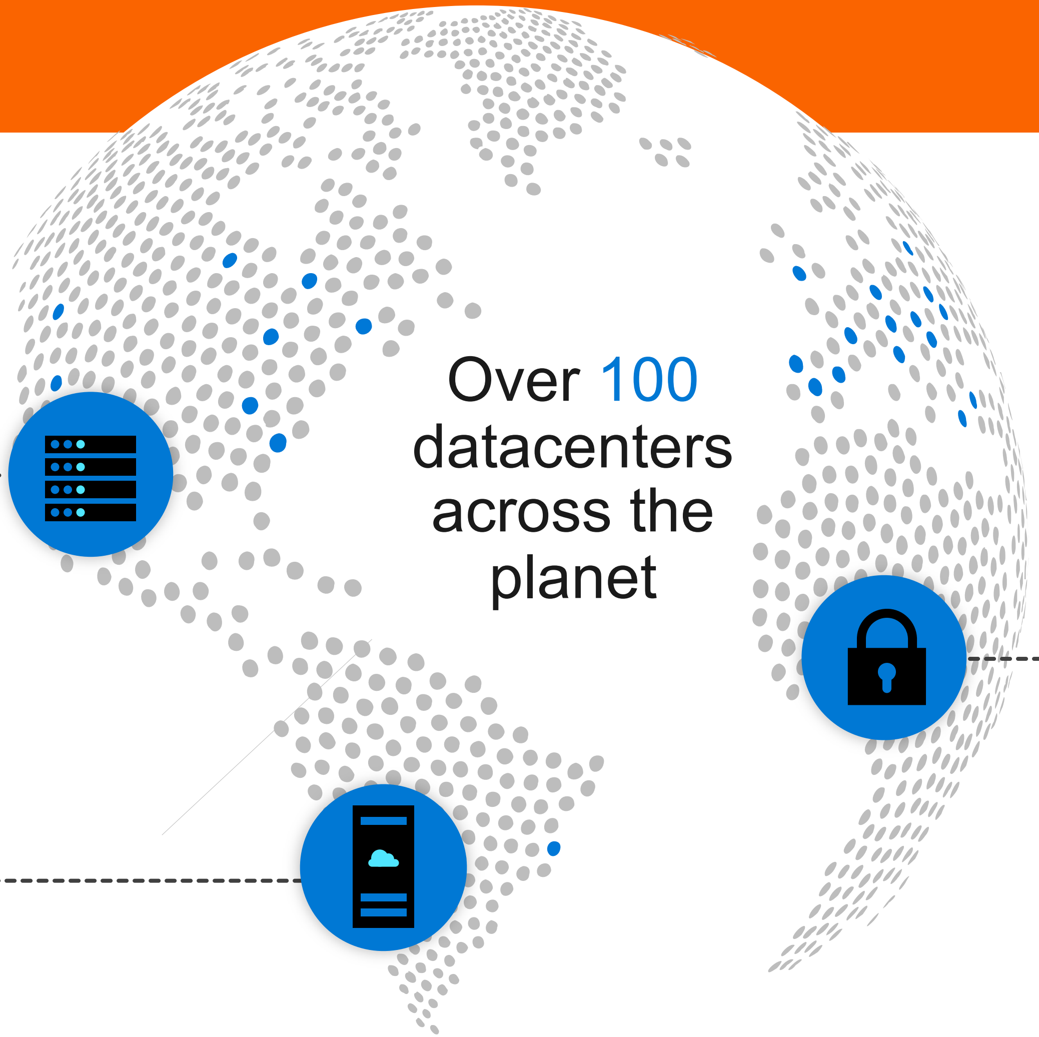
Shared threat data from partners, researchers, and law enforcement worldwide

Botnet data from Microsoft Digital Crimes Unit

18B+ Bing web pages scanned

450B monthly authentications

A secure foundation at global scale



Over 100 datacenters across the planet

Each physical datacenter protected with world-class, multi-layered protection

Global cloud infrastructure with custom hardware and network protection

Secured with cutting-edge operational security

- Restricted access
- 24x7 monitoring
- Global security experts

Thomson Reuters & Microsoft Partnership

Thomson Reuters builds on what Azure provides

- Security Center recommendations
- Vulnerability assessments
- Alerts and notifications

Layer additional tools and practices

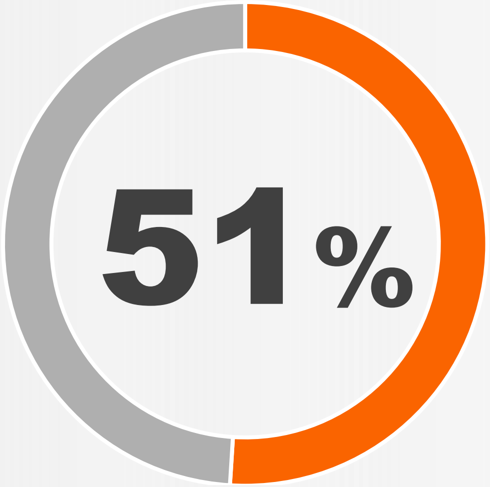
- SOC and Incident Response
- Best practices and policy enforcement
- 3rd-party tools and scans

POLL #3 QUESTION

Third-party vendors pose a risk

What questions should you ask?

Are you **evaluating the privacy and security practices** of your vendor or just relying upon purported reputation?



of organizations have experienced a data breach **caused by a third-party***

*https://www.securitymagazine.com/articles/95143-of-organizations-have-experienced-a-data-breach-caused-by-a-third-party#:~:text=51%25%20of%20organizations%20have%20experienced,%2D05%2D06%20%7C%20Security%20Magazine

THOMSON REUTERS®

Key Take-aways

- Understand what ransomware is, how it happens
- Be prepared for a ransomware attack BEFORE it happens; have a plan
- Build a cybersecurity culture at your firm
- Know your 3rd party vendors' cybersecurity certifications/audits
- Get help! Hire cybersecurity experts
- Leverage Security Benefits through the Thomson Reuters & Microsoft Partnership

Q&A

THOMSON REUTERS®

What’s next

RESOURCES

Explore the solution

Learn more about the advantages of 3E

Get a Consultation

Schedule a free demo of 3E Cloud

Learn More

Access on-demand webinars from Thomson Reuters and Microsoft