NET-measure

Industrial CyberSec Forum 2023

Reveal the Invisible! : You can’t protect what you can’t see

09/02/2023

Agenda

- Introduction NET-measure
- Reveal the invisible
- DDoS attacks
- NDR
- Conclusion
- Q&A

Introduction NET-measure

NET-measure

- Successful Belgian private company since 2006 in IT Monitoring
- Average growth of more than 20%/year
- IP Monitoring on all levels is our core business
- NET-measure delivers the Software, Hardware, Services & Rental
- Small team of experts, each in their own domain
- Focus as supplier for industries, large organizations, government agencies, ministries and multinationals
- Offices in Hoeilaart, Focus on BeNeLux with world-wide activity and support

Improving Quality of Life by improving Customer Experience in IT

NET-measure

What we do:

Always-on Connectivity -Business Continuity

Risk Anticipation

Full Network Visibility – Cloud Networking

Capturing, Storing and Analyzing Data at large capacities and at line speed for :

- IT Performance monitoring
    - Network performance Monitoring : IP, OTDR, Handheld WiFi, Copper, Fiber
    - Application Assurance / Transaction performance Monitoring / VoIP / UC&C
    - Active inventory Monitoring : infrastructure, VM
    - Protocol analysis : Profinet and Bacnet

- Security
    - DDoS protection
    - Cybersecurity asset management (IoT – BYOD)
    - Forensic Investigation

FLUKE

netAlly

Allegro Packets
Network Multimeter

NETSCOUT
Platinum Partner

Rebasoft

Reveal the invisible – Self protection

68% **of business say they lack high visibility into internal traffic !**

source: Positive Technologies

– Inventory discovery : ALL devices on the network

- User: Servers, pc's, printers, PLCs, Scanners, Camera's, IoT devices ...
- Network: routers, switches, access points, firewalls, taps ...

– Policy compliancy

- Requirements of the organisation (eg Facebook on printer port)

– Vulnerability Management

- Automated Vulnerability Detection without scans
- Hardware, drivers and software vulnerabilities

NIST Database from National Information Technology Laboratory

DDoS Attacks: Types

- Volume Based Attacks
  (Volumetric)
- Protocol Attacks
  (Vector/state exhaustion attack)
- Application Layer Attacks
  (ex HTTP Flooding)

NET-measure

DDoS: Horizon intelligence is info from:

20,000+

Customers

100+

Countries

Customers Include…

90%

of the World’s Tier 1 Service Providers

9 in 10

of the Largest Cloud Hosting Providers

3 in 5

of the Largest Social and Online Brands

90%

of the US Fortune 100 Companies

9 in 10

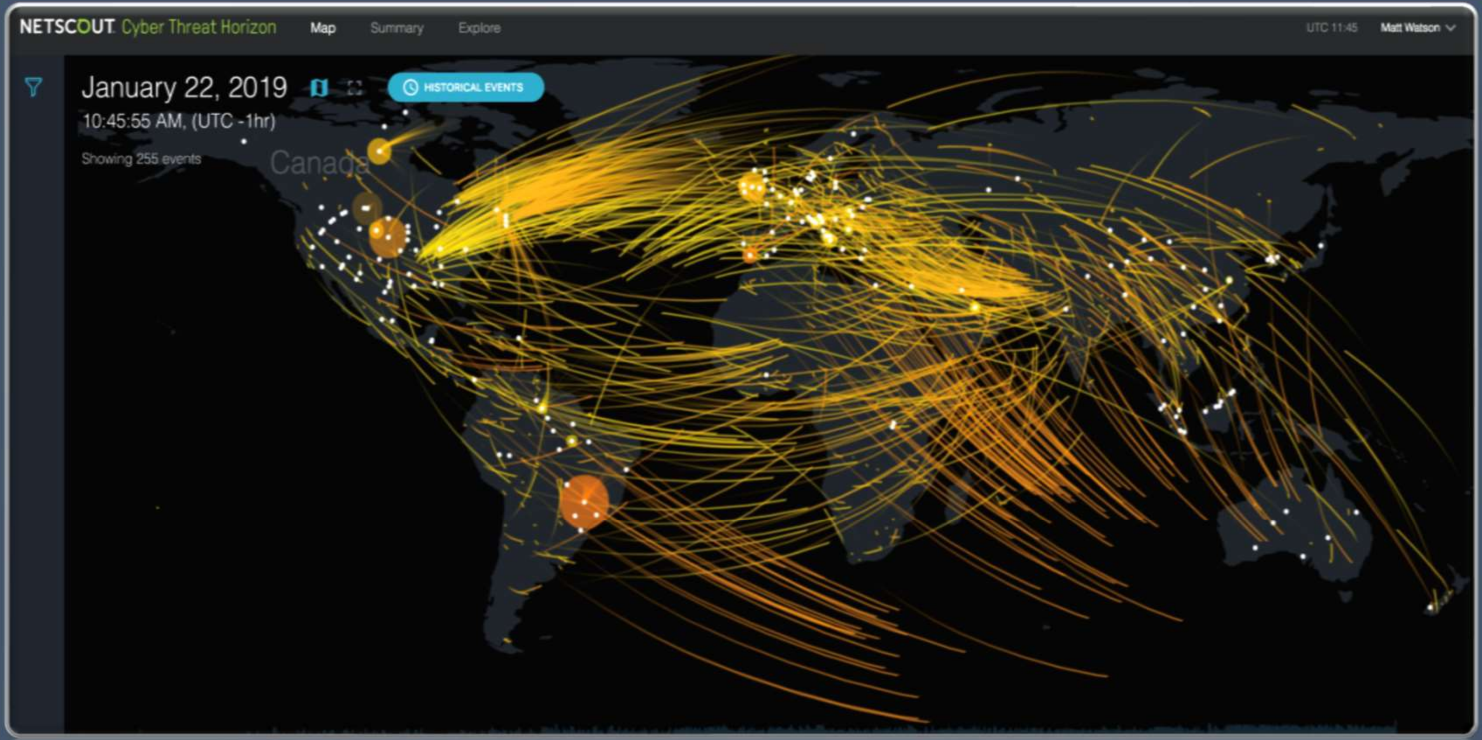
of the Largest Global Financial Institutions

Cyber Threat Horizon is an information service that enhances cybersecurity situational awareness for Enterprise and Service providers. It delivers highly contextualized visibility into ‘over the horizon’ threat activities. Netscout’s Horizon is powered by Atlas, Netscout’s globally distributed threat analysis platform

LIVE MAP

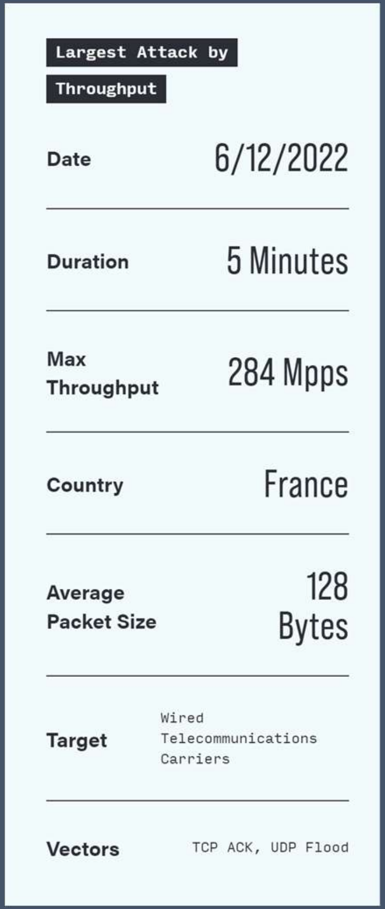
DDoS Attack Trends

- > 7.5 million DDoS attacks in 2022 (up to Oct)
- Complex multi-protocol layer attacks on the rise



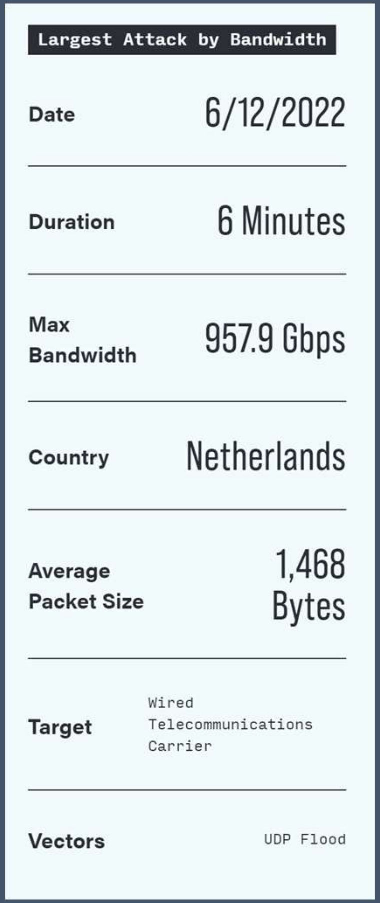
DDoS attacks have never been more innovative, dynamic, or consequential

EMEA figures – Volume based



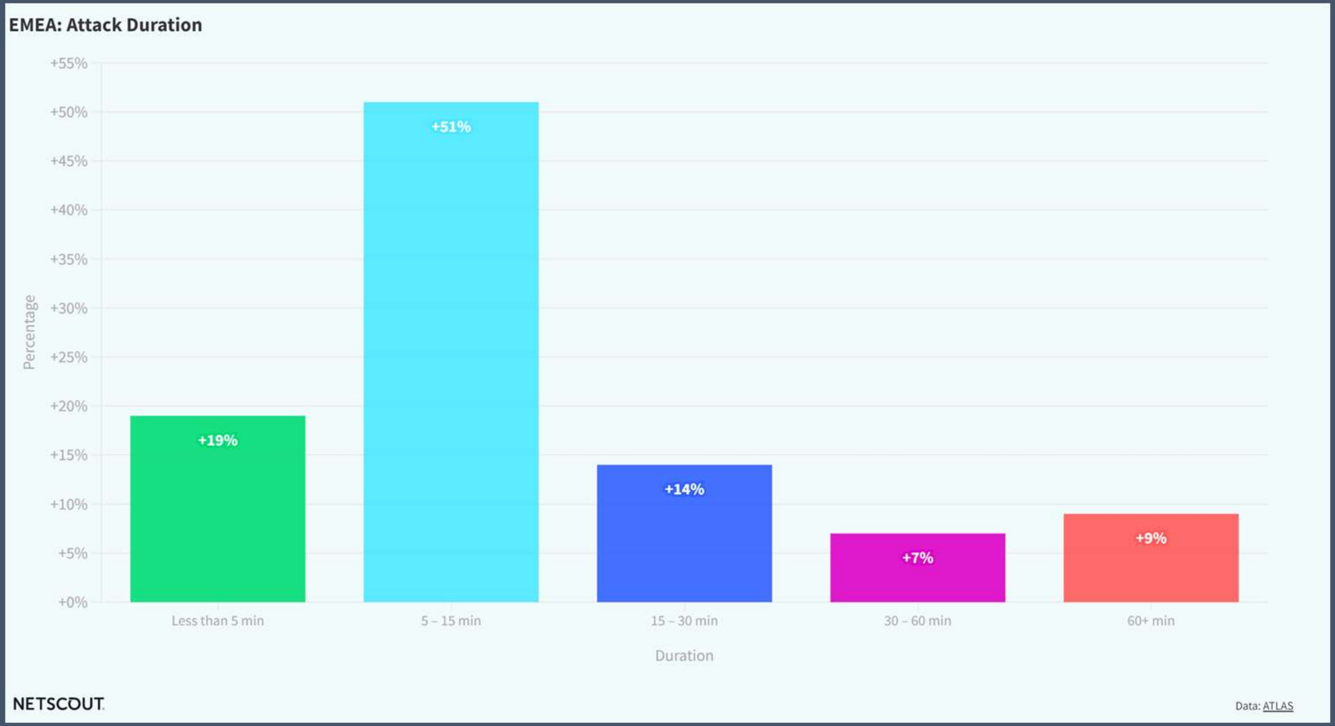
Largest Attack by Throughput

Date	6/12/2022
Duration	5 Minutes
Max Throughput	284 Mpps
Country	France
Average Packet Size	128 Bytes
Target	Wired Telecommunications Carriers
Vectors	TCP ACK, UDP Flood



Largest Attack by Bandwidth

Date	6/12/2022
Duration	6 Minutes
Max Bandwidth	957.9 Gbps
Country	Netherlands
Average Packet Size	1,468 Bytes
Target	Wired Telecommunications Carrier
Vectors	UDP Flood

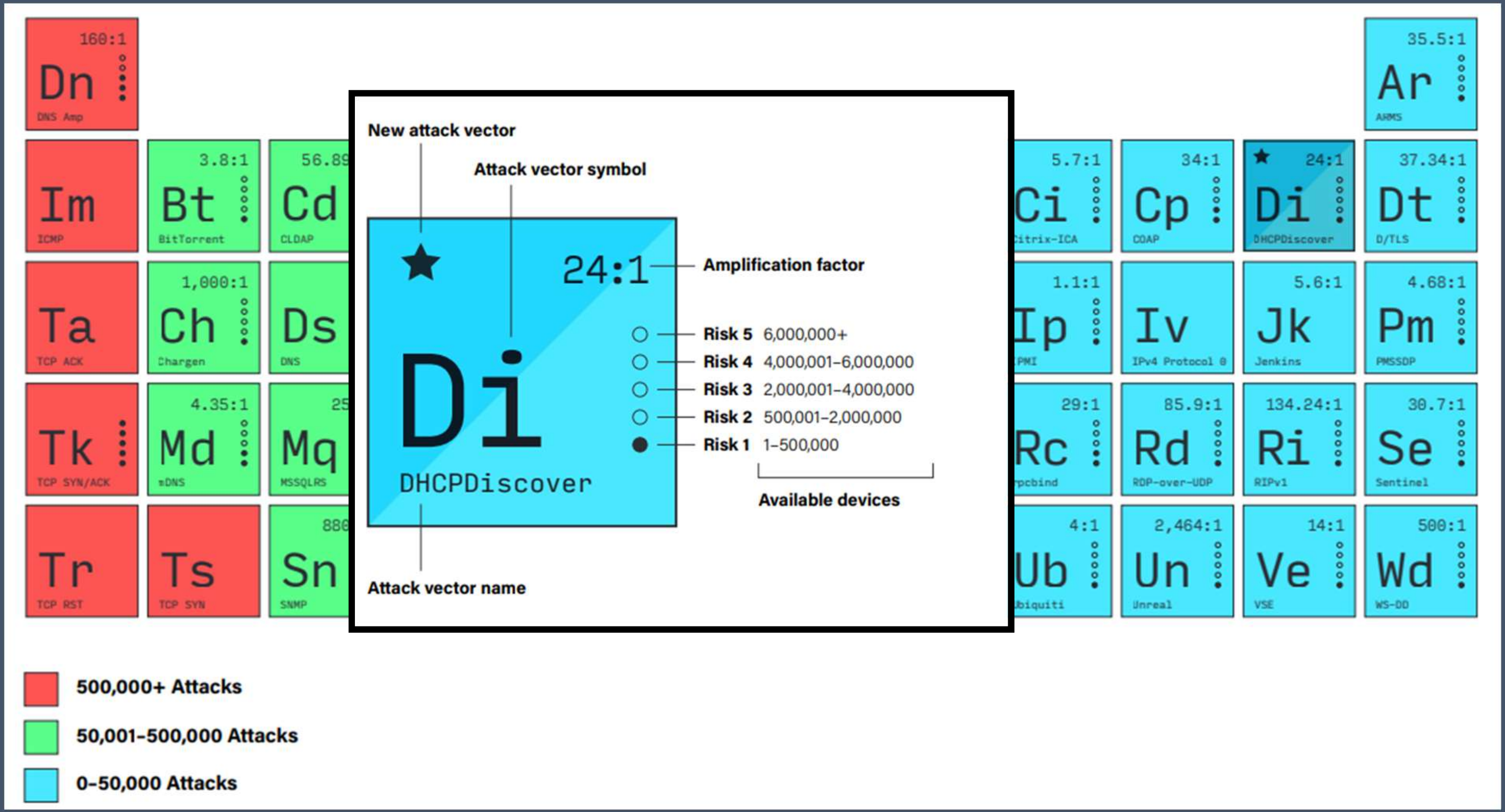


EMEA: Attack Duration

Data: ATLAS

ICSF 2023 : www.NET-measure.com - sales@NET-measure.com

Periodic table of protocol attacks



160:1 Dn DNS Amp						35.5:1 Ar ARMS
Im ICMP	3.8:1 Bt BitTorrent	56.89 Cd CLDAP	5.7:1 Ci Citrix-ICA	34:1 Cp COAP	★ 24:1 Di DHCPDiscover	37.34:1 Dt D/TLS
Ta TCP ACK	1,000:1 Ch Chargen	Ds DNS	1.1:1 Ip PMI	Iv IPv4 Protocol 0	5.6:1 Jk Jenkins	4.68:1 Pm PMSSDP
Tk TCP SYN/ACK	4.35:1 Md mDNS	25 Mq MSSQLRS	29:1 Rc rpcbind	85.9:1 Rd RDP-over-UDP	134.24:1 Ri RIPv1	30.7:1 Se Sentinel
Tr TCP RST	Ts TCP SYN	880 Sn SNMP	4:1 Ub biquiti	2,464:1 Un Unreal	14:1 Ve VSE	500:1 Wd WS-DD

New attack vector

Attack vector symbol

★ 24:1

Di

DHCPDiscover

Amplification factor

○ **Risk 5** 6,000,000+

○ **Risk 4** 4,000,001–6,000,000

○ **Risk 3** 2,000,001–4,000,000

○ **Risk 2** 500,001–2,000,000

● **Risk 1** 1–500,000

Available devices

Attack vector name

🟥 **500,000+ Attacks**

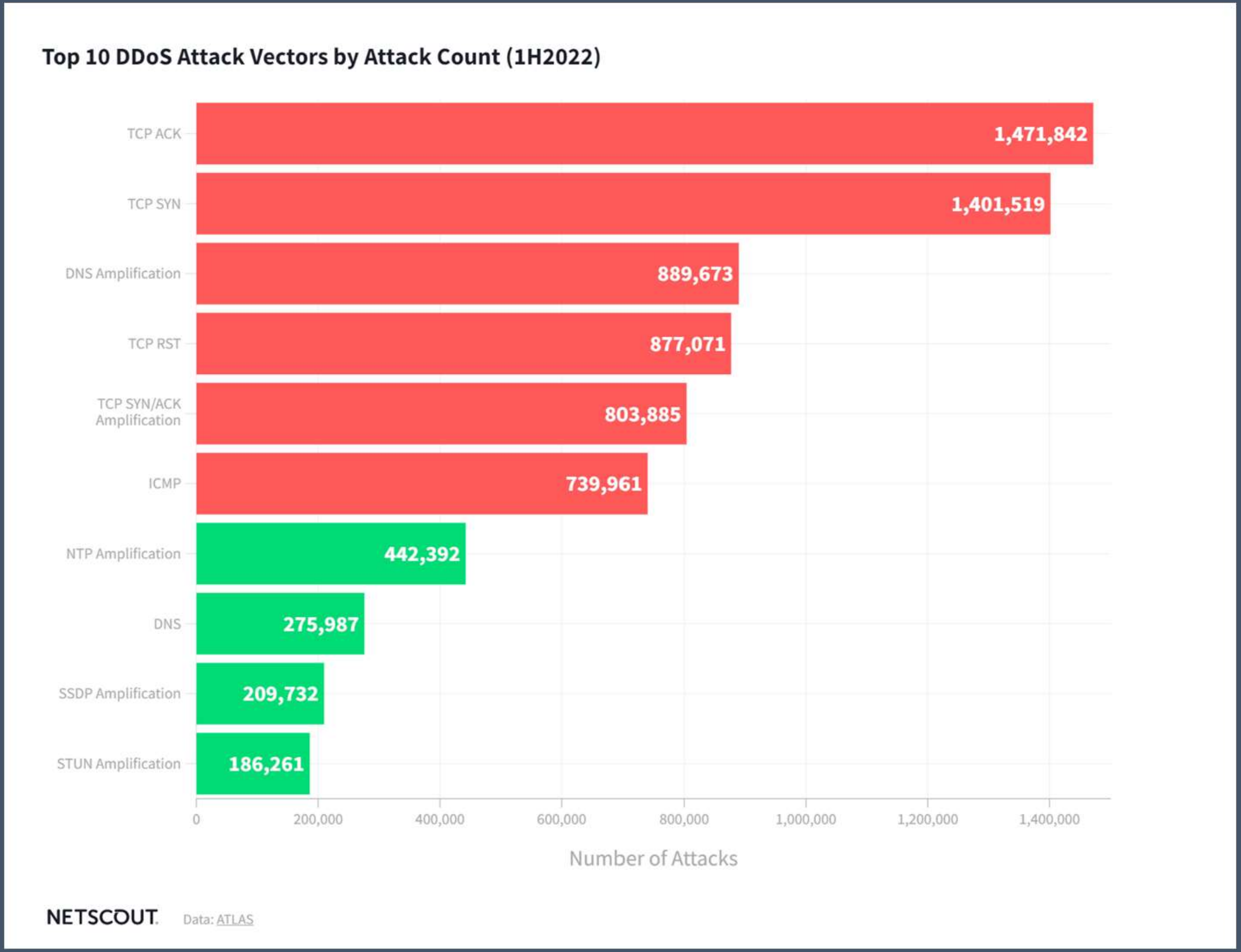
🟩 **50,001–500,000 Attacks**

🟦 **0–50,000 Attacks**

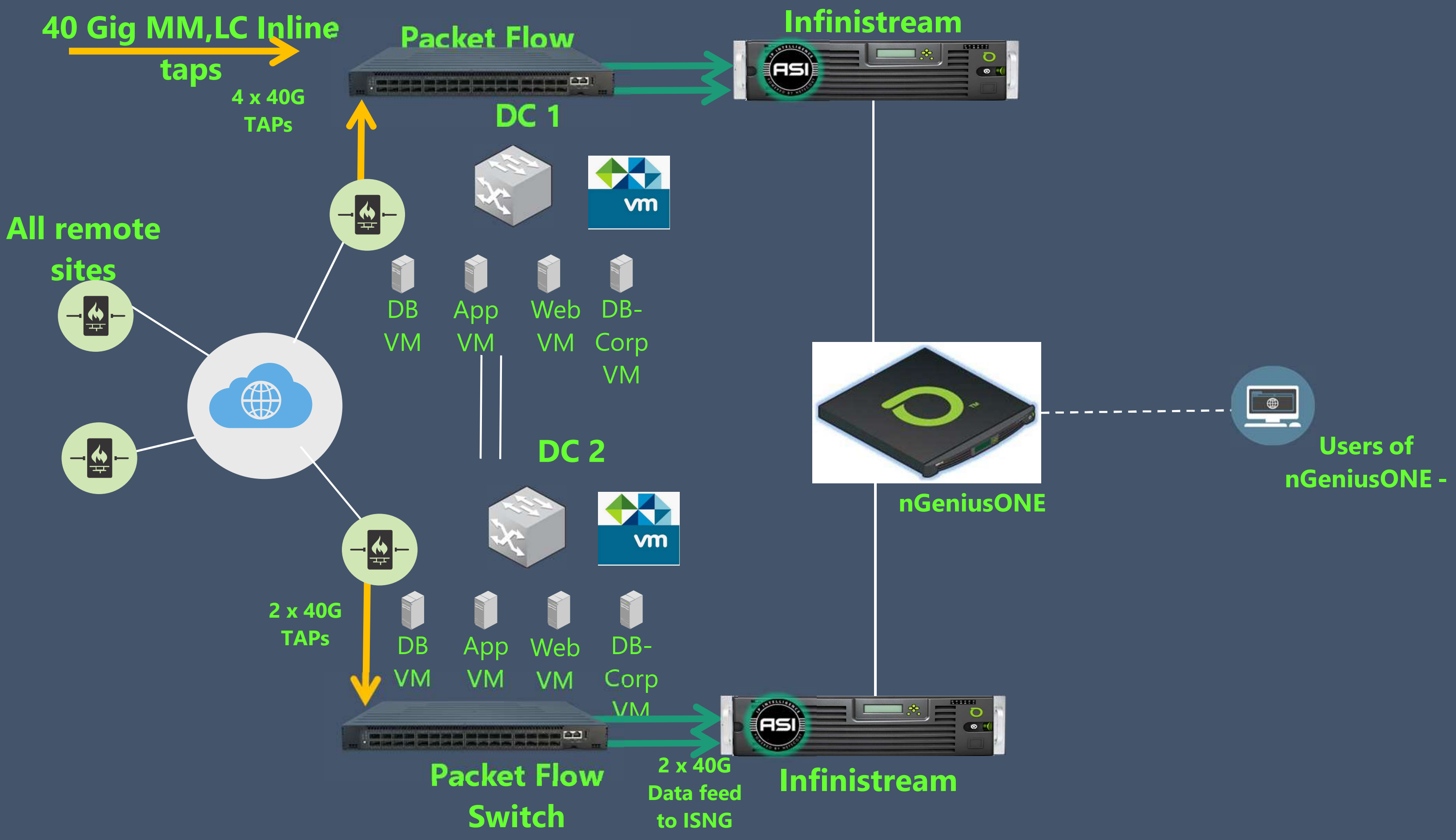
https://www.netscout.com/threatreport/ddos-global-attack-trends/#ddos-attack-vectors

Source: NETSCOUTs 19th bi-annual
DDoS Threat Intelligence Report

Protocol Attacks – most used



NDR – starts with Monitoring

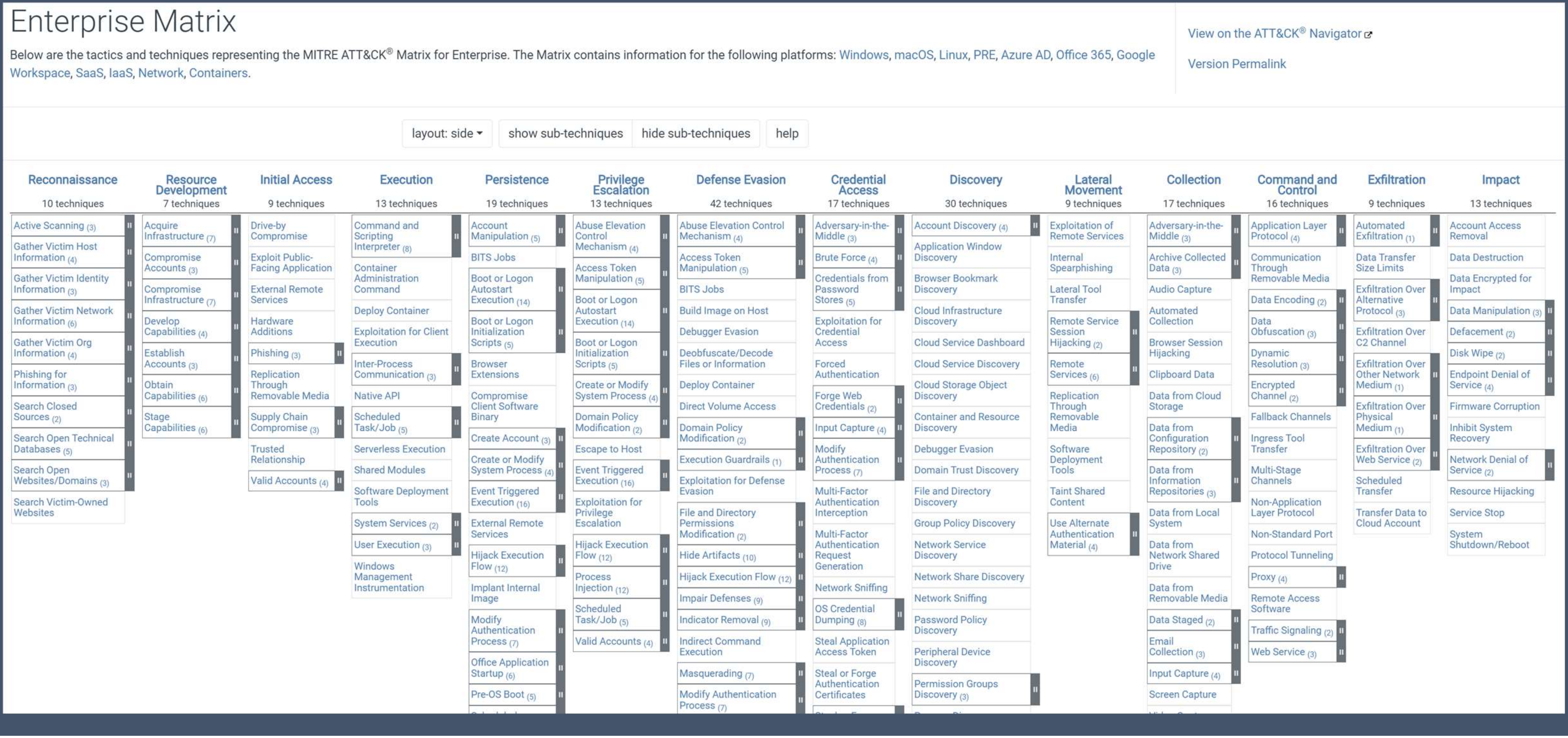


2 x 40G Data feed to ISNG

NET-measure

Cyber Intelligence NDR Platform

The Mitre ATT&CK Matrix for Enterprise & AI



Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

View on the ATT&CK® Navigator

Version Permalink

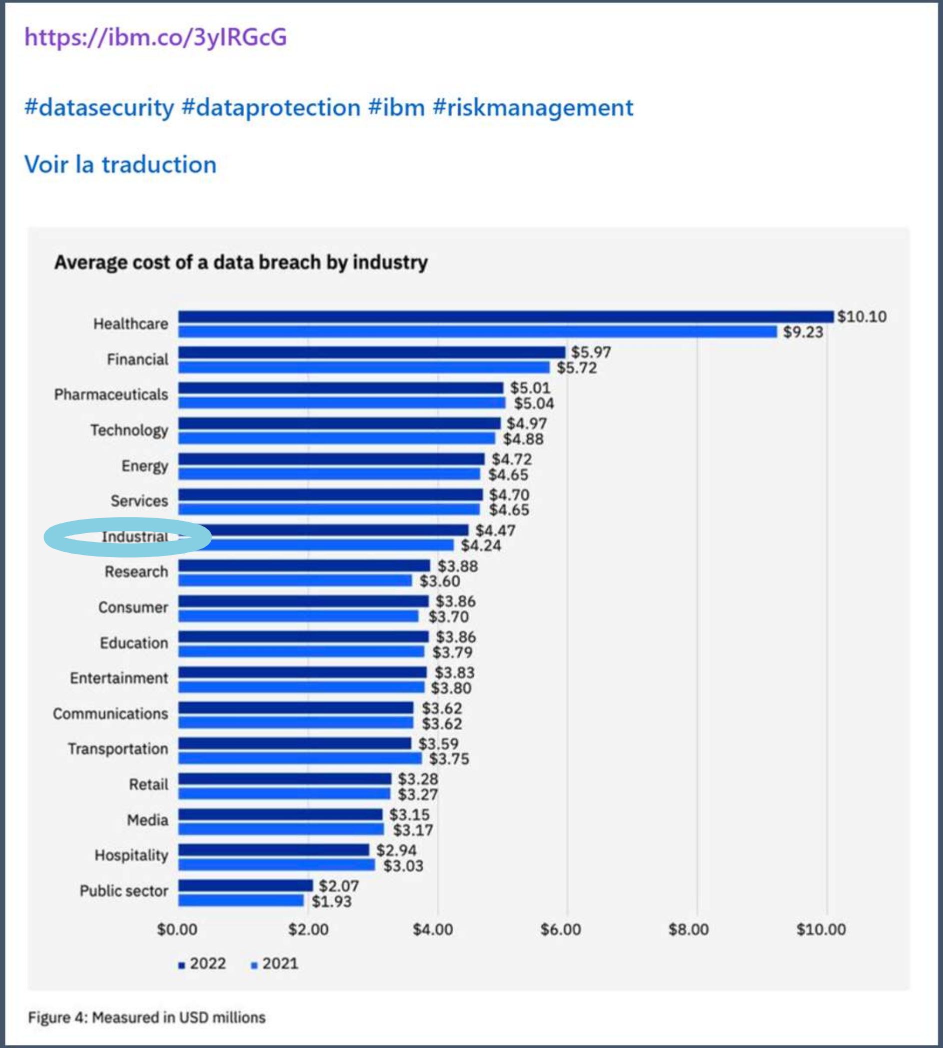
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (12)	Process Injection (12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (3)	Implant Internal Image	Scheduled Task/Job (5)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (7)	Valid Accounts (4)	Hide Artifacts (10)	Steal Application Access Token	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Hijack Execution Flow (12)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Impair Defenses (9)		Network Sniffing		Input Capture (4)	Traffic Signaling (2)		
						Indicator Removal (9)		Password Policy Discovery		Screen Capture	Web Service (3)		
						Indirect Command Execution		Peripheral Device Discovery					
						Masquerading (7)		Permission Groups Discovery (3)					
						Modify Authentication Process (7)							

How does NDR works ?

Network Detection and response (NDR)

- is a security tool that monitors an enterprise's network traffic to gain visibility into potential cyberthreats.
- NDR relies on advanced capabilities, such as behavioral analytics, machine learning, and artificial intelligence to uncover threats and suspect activities.
- Once detected, the solution takes action against threats using its own capabilities, or through coordinated actions in conjunction with other cybersecurity tools.
- NDR solutions work by modeling the tactics, techniques and methodologies found in the MITRE ATT&CK framework.
- The findings can also be shared with security information event management (SIEM) solutions to create broader security assessments.

Average cost:



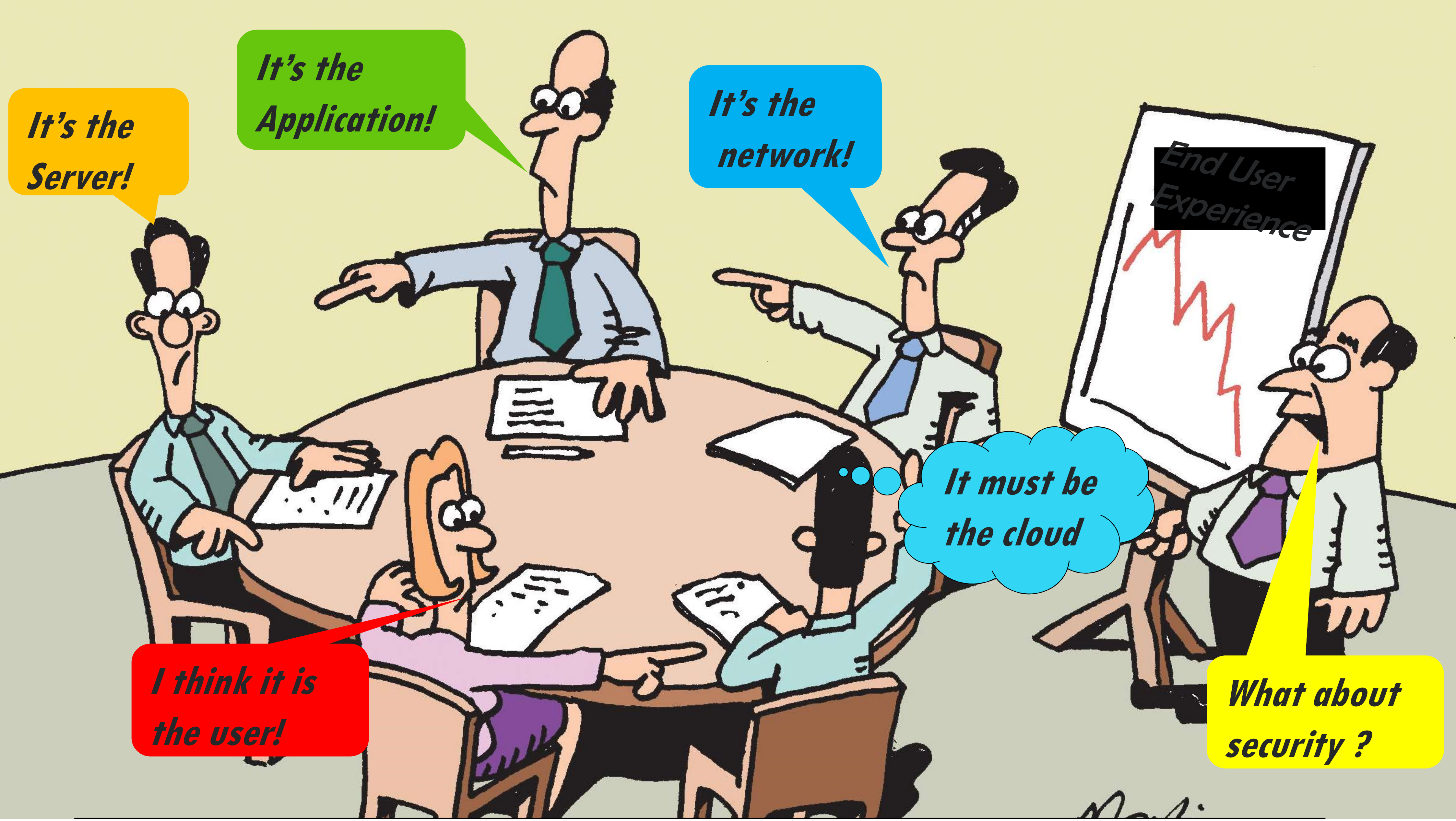
https://ibm.co/3yIRGcG

#datasecurity #dataprotection #ibm #riskmanagement

Voir la traduction

Average cost of a data breach by industry

Figure 4: Measured in USD millions


It's the Server!
It's the Application!
It's the network!
[redacted]
It must be the cloud
I think it is the user!
What about security ?

NET-*measure*

Raymond Lauwersstraat
B-1560 Hoeilaart

Thank you for your interest