SECURITY SUMMIT

Verona, 10 ottobre 2023

Security Summit

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

CON UNA POSTURA CORRETTA, SI EVITANO ANCHE I CYBER DOLORI

Nicolas Agrianidis, Sales Manager, Symbolic
Andrea Muzzi, Technical Manager, WithSecure™

Luca Bechelli, Comitato Scientifico Clusit

10 ottobre Verona 2023 orario 14.50-15.30

Nicolas Agrianidis

SALES MANAGER, SYMBOLIC

Andrea Muzzi

TECHNICAL MANAGER, WITHSECURE™

Luca Bechelli

COMITATO SCIENTIFICO CLUSIT

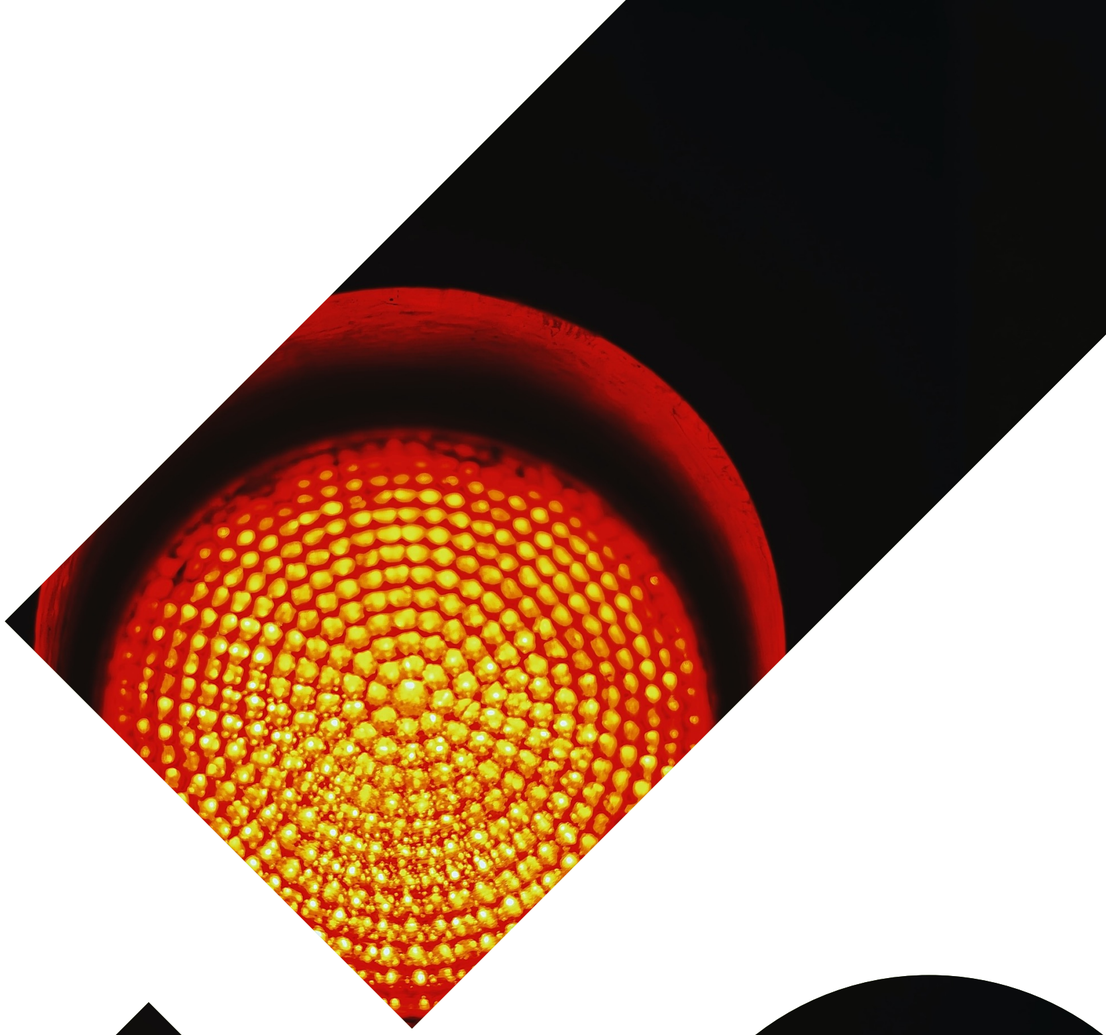
PARTNER @P4I - DIGITAL360

Un cambio di paradigma

Dalla "protect" posture alla "threat prevention"

You can protect your environment……

You *can't* prevent all threats.



No environment is unbreachable – prevention alone is not enough

New cyber threats and attack vectors emerge rapidly

Human element in cyber security is a rare occurrence

Heavyweight xDR solutions require considerable skills

Lightweight EDR solutions lack means to effectively stop advanced attacks

IL COSTO MEDIO È DI 4 MILIONI DI DOLLARI PER OGNI VIOLAZIONE RILEVATA

…come il costo medio globale delle violazioni informatiche abbia raggiunto i 4,45 milioni di dollari nel 2023 – massimo storico per il report – in aumento del 15% negli ultimi 3 anni.

A livello globale, i **costi di rilevamento** sono aumentati del 42% rispetto allo stesso periodo dell'anno precedente, mentre in Italia, il costo complessivo delle violazioni di dati è pari a 3,55 milioni di euro, in crescita rispetto ai 3,03 milioni di euro nel 2021.

Fonte IBM Report Cost of a Data Breach 2023

Verona

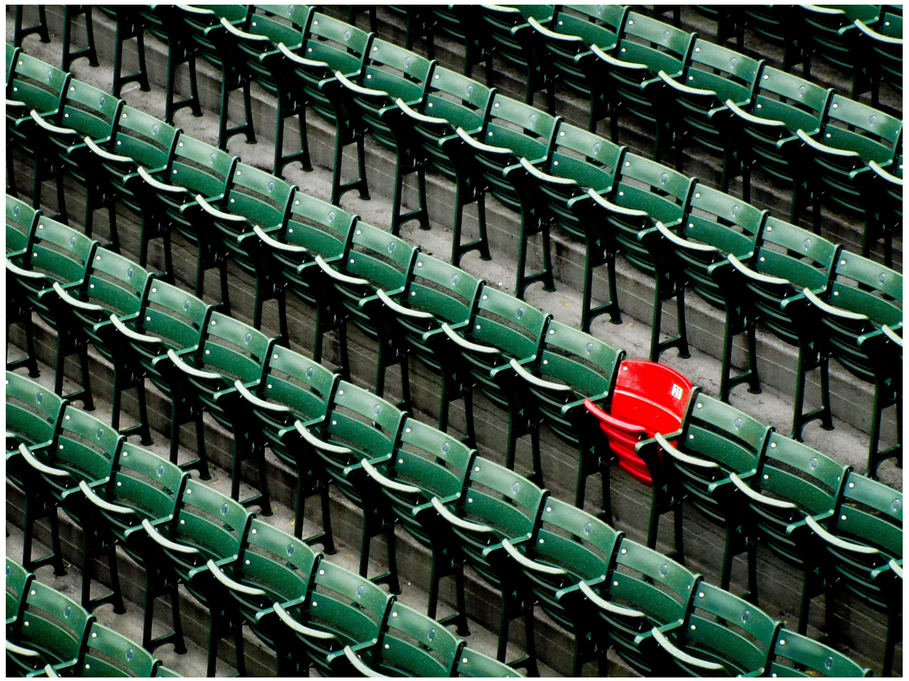
	Denunce/100.000 abitanti	Posiz.
Omicidi volontari consumati	0,4	51
Tentati omicidi	0,9	71
Violenze sessuali	11,4	24
Furti	1.402,0	24
Furti con strappo	10,7	33
Furti con destrezza	133,9	19
Furti di autovetture	37,8	45
Furti in esercizi commerciali	128,7	17
Furti in abitazione	284,1	23
Rapine	32,8	24
Estorsioni	16,1	54
Usura	0,4	26
Associazione per delinquere	0,9	42
Associazione di tipo mafioso	0,0	104
Riciclaggio e impiego di denaro	1,6	58
Truffe e frodi informatiche	511,5	40
Incendi	6,5	71
Stupefacenti	39,8	75

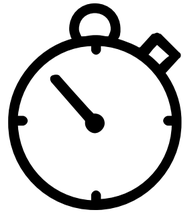
One vulnerability is enough for the attacker

The attacker is looking for how to execute code on a target machine
LURE A USER OR USE A VULNERABILITY

Over 3 months

The average time until a known security vulnerability is remediated





~ 1 week

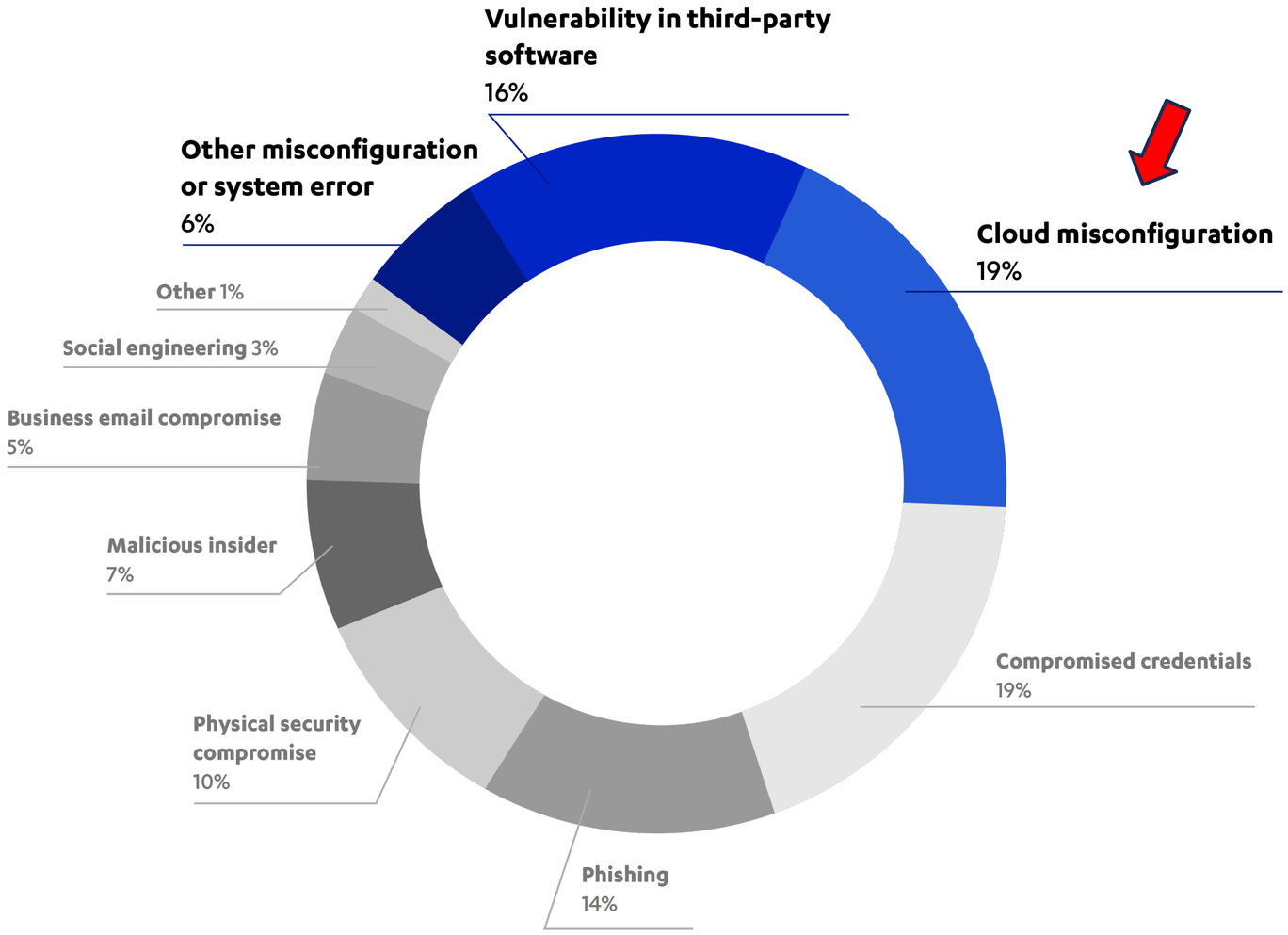
The average time for attackers to weaponize and exploit a vulnerability

Patch Management VS. Vulnerability Management

- Updates software, operating systems, and applications
- Doesn’t always fix security issues
- IT Operations-led

- Discovers vulnerabilities on connected devices and systems and reports them
- Corrects security issues
- Security Operations-led

Popular attack vector: vulnerability exploits



Main attack vectors
are users and vulnerabilities in security architecture

More than a third
of breaches are caused by vulnerable systems and misconfigurations

Where’s the risk?

- Out-dated software
- Misconfigured systems
- Insecure web applications

How to tackle it?

- Continuous vulnerability scanning
- Strict vulnerability management processes
- Cover all your assets: servers, desktops, printers, routers, etc.

Vulnerability Management Lifecycle

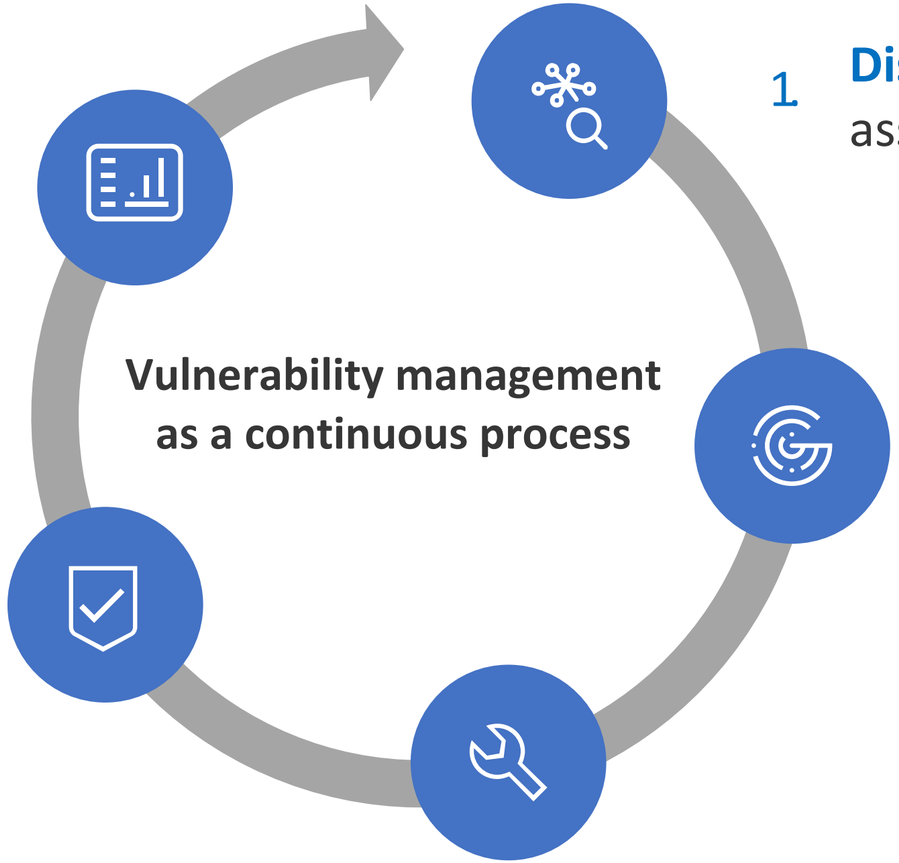
1. **Discover** all network assets

2. **Scan** assets and applications for vulnerabilities

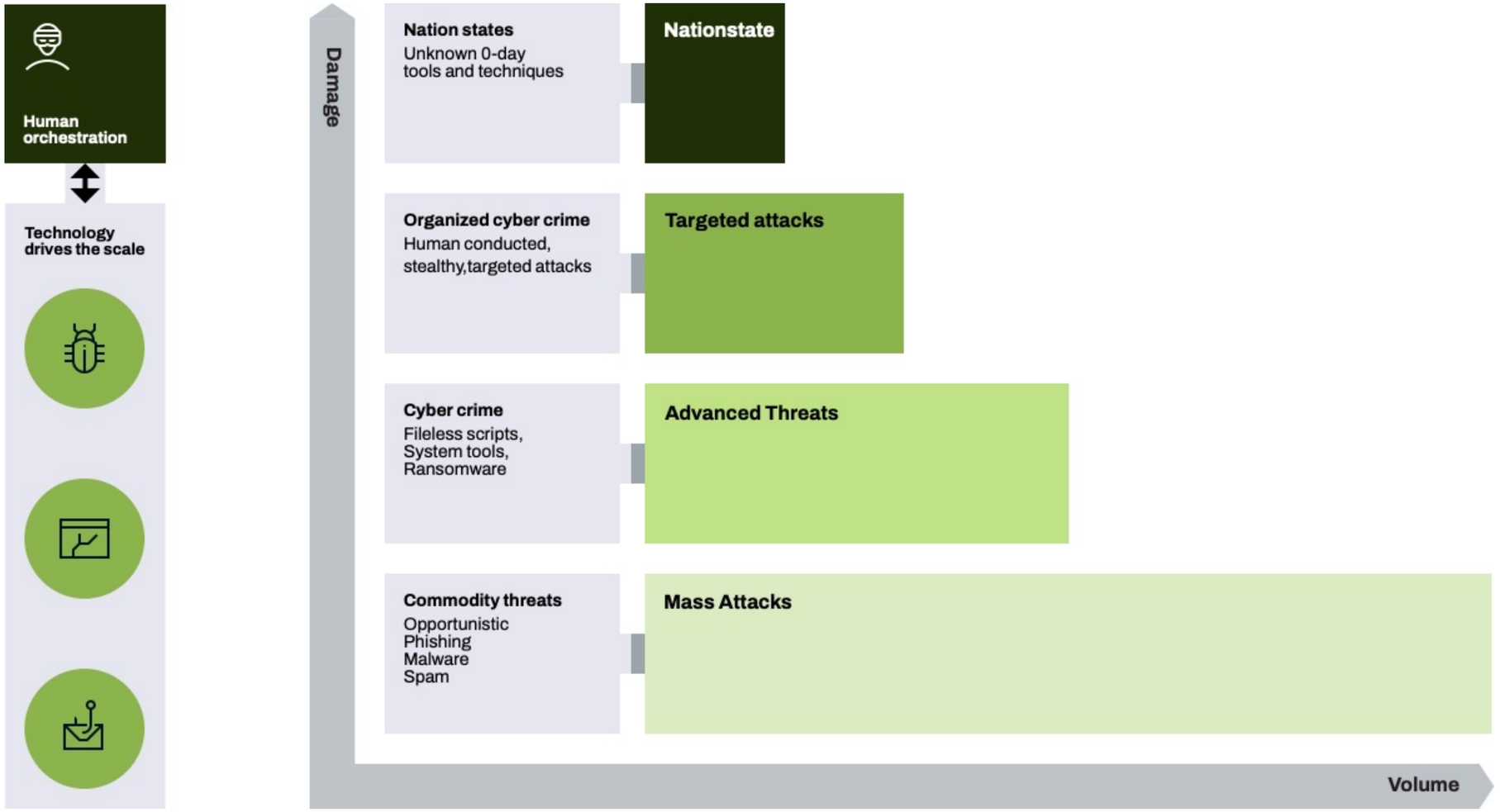
3. **Remediate** effectively via a managed process

4. **Validate** that corrective actions were completed

5. **Document** all corrective actions taken for auditing



Understanding the threat landscape



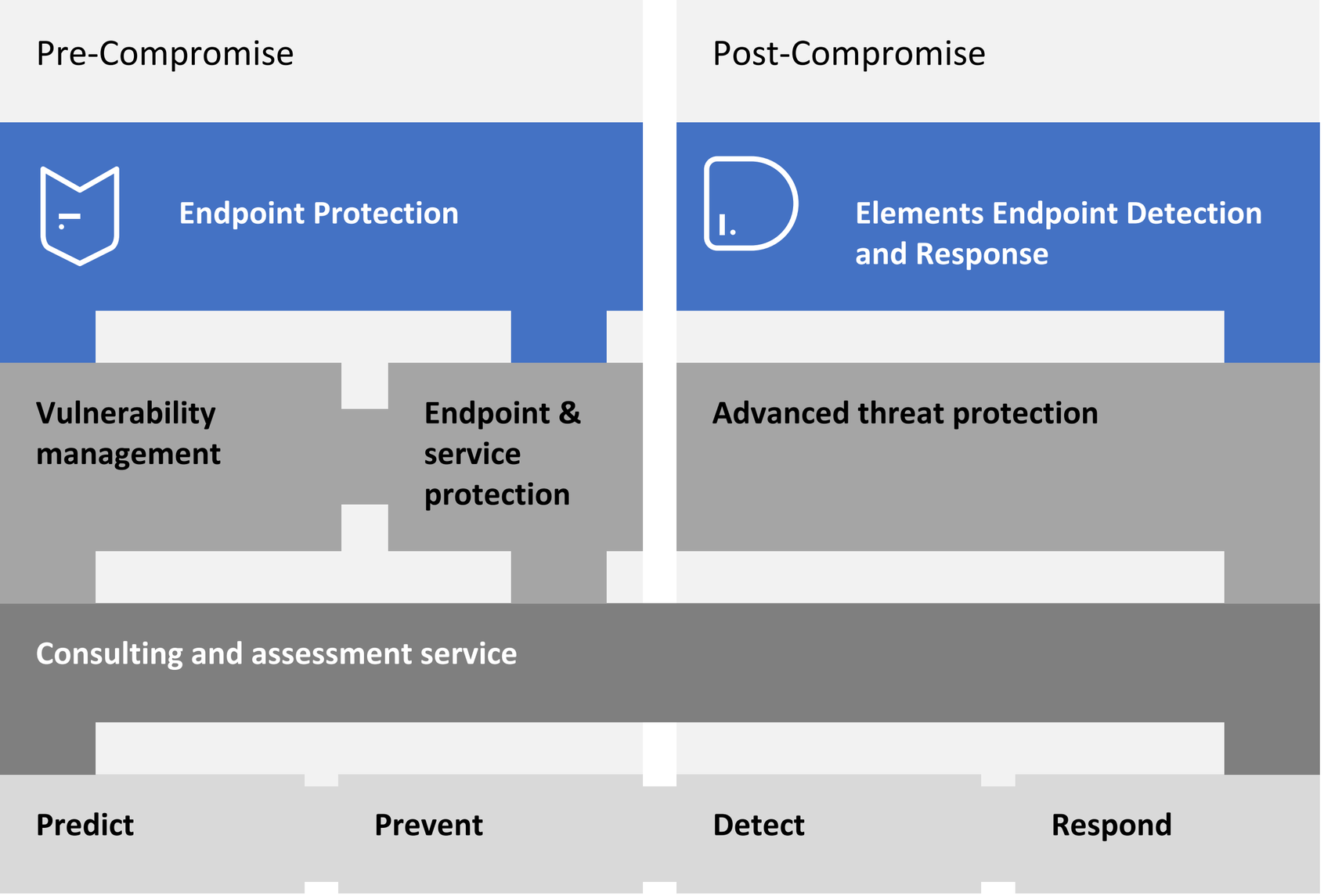
Call for a paradigm shift

BEFORE

From single-shot, point detections and binary (ON/OFF) responses

NOW

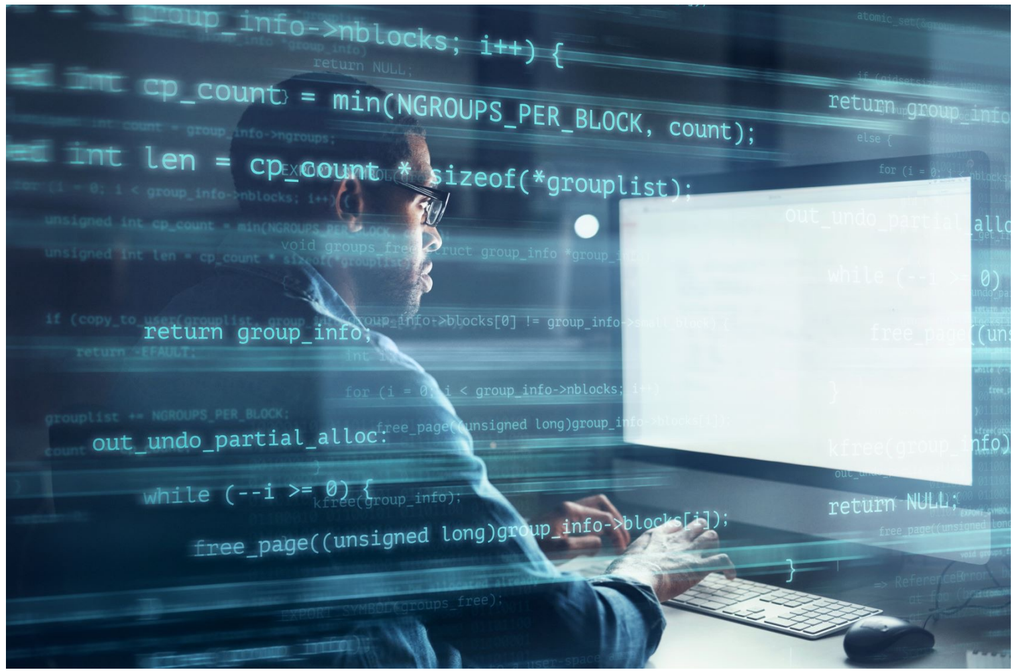
To event flow and context-based detections, and multifaceted, automated, risk-based responses



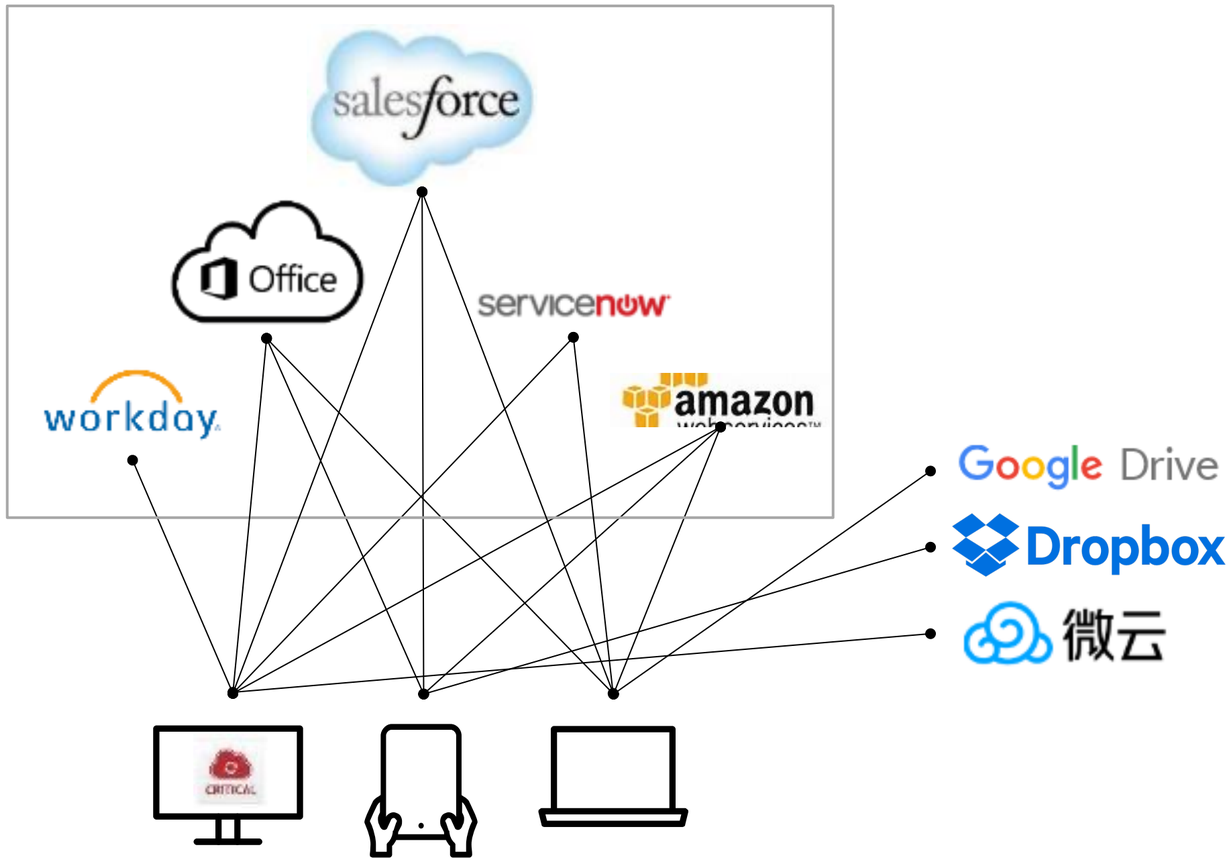
Endpoint Protection is crucial for cyber security but the threat landscape is rapidly evolving

2022 ANNO DI FERMENTO PER LA CYBER SECURITY

- **Imponenti attacchi** ai danni di importanti società e infrastrutture nazionali. Lapsus$ e Conti
- **Crescente minaccia** di organizzazioni criminali di profilo più basso che utilizzano tattiche come il ransomware mirato
- **I cyber attacchi** vengono sferrati soprattutto attraverso sistemi IT ed endpoint tradizionali.
- **Il numero crescente di aziende che trasferiscono l'infrastruttura e le operazioni nel cloud. Grandi quantità di dati preziosi e sensibili**
- **I controlli**, devono essere configurati correttamente dai clienti stessi per mettere al sicuro i loro dati, secondo il modello di responsabilità condivisa.



Modern IT infrastructure increases exposure to threats



What assets do we have ?
How critical are they ?
Who can access them ?
What services are being used by our employees ?
How do they connect to those services ?
… and many, many more

SHARED RESPONSABILITY

Learn / Azure / Sicurezza /

Responsabilità condivisa nel cloud

Articolo • 01/06/2023 • 3 contributori

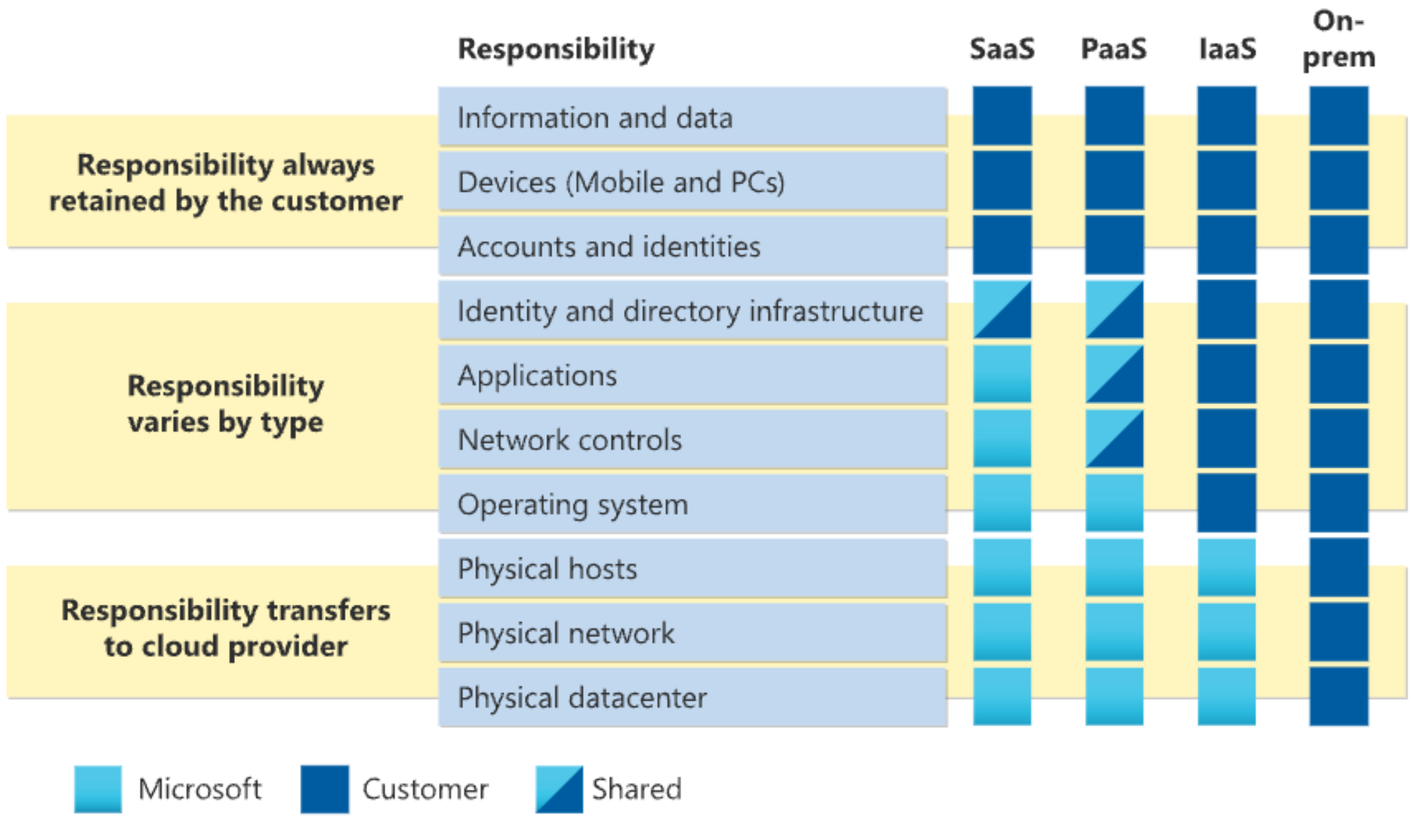
Commenti e suggerimenti

In questo articolo

Quando si considerano e valutano i servizi cloud pubblici, è fondamentale comprendere il modello di responsabilità condivisa e quali attività di sicurezza vengono gestite dal provider di cloud e dalle attività gestite dall'utente. Le responsabilità del carico di lavoro variano a seconda che il carico di lavoro sia ospitato in Software as a Service (SaaS), Platform as a Service (PaaS), Infrastruttura as a Service (IaaS) o in un data center locale

Suddivisione della responsabilità

In un data center locale è proprietario dell'intero stack. Quando si passa al cloud alcune responsabilità vengono trasferite a Microsoft. Il diagramma seguente illustra le aree di responsabilità tra l'utente e Microsoft, in base al tipo di distribuzione dello stack.



Cloud Transformation

Moving to the cloud solves many weaknesses of on-premise setups, but the new responsibility of companies for securing their cloud environment is challenging:

Cloud platforms are developed at a very fast pace

Multi-cloud IT setups

Scarcity of cloud security skills

Opportunistic cyber attacks look for mistakes

Complexity

Regulators, auditors and fines

Vocabulary comparison

Unfortunately, the vocabulary has not become yet standardized, thus AWS and Azure uses different terms to describe the same thing. Here is a comparison table between our, WithSecure terminology and AWS + Azure.

WithSecure terminology	AWS terminology	Azure terminology
Asset		Resource
Resource	Container instance	Resource
Service		Resource
	Cluster	Resource group

…But the IaaS clouds need to be controlled responsibly

DevOps

What tools and services do we have in the cloud?
How should we harden the security of our cloud infrastructure?
Do we have the right security policies implemented in the cloud?

Security Specialist

How can we track the security status of or cloud environments and alert of security issues?
How can we prove to auditors that we have sufficient controls in place and that those are effective?
Do we have the right security policies implemented in the cloud?

Through 2025, 90% of organizations with insufficient public cloud controls will share sensitive data in inappropriate ways and customers themselves will cause 99% of cloud security failures.

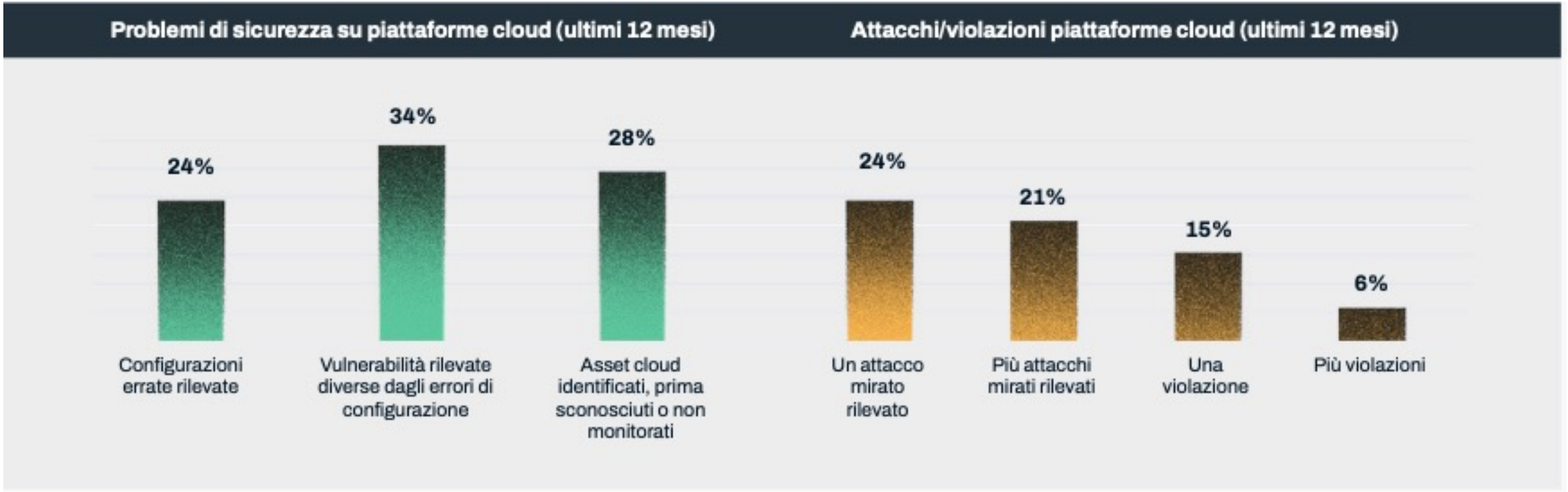
In our 2022 B2B market research…

24% of companies detected at least one targeted attack involving their cloud platform(s) within the last 12 months.

24% of companies had detected misconfigurations within the last 12 months.

? Is it possible to know the real numbers, as many customers may not have even tried?

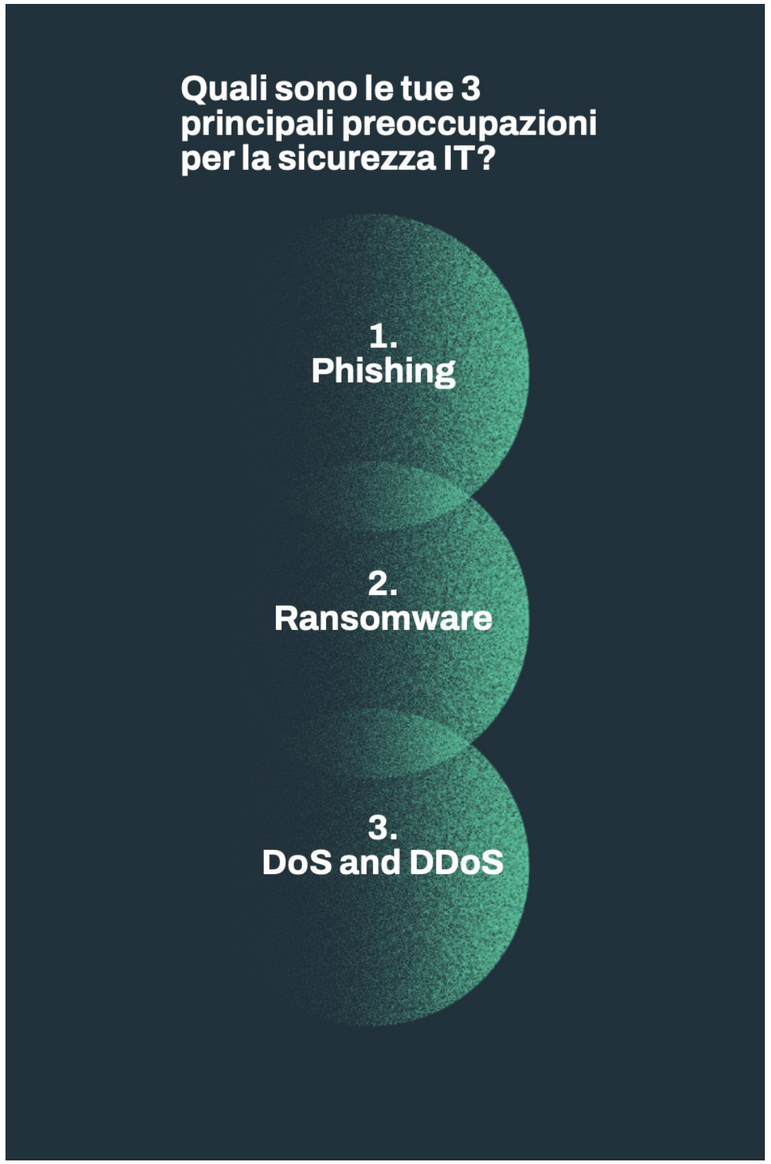
La minaccia rappresentata dagli errori di configurazione e dagli asset non monitorati



"La complessità è nemica della sicurezza. Più l'ambiente è complesso, più è probabile che qualcosa venga trascurato e non venga configurato correttamente.

Negli ultimi 18 mesi, quali sono stati i tre punti più critici nella gestione della sicurezza dei dati?

59%	Gestione della sicurezza di terze parti
53%	Restare al passo con le normative di conformità
49%	Sicurezza dei dispositivi mobili
38%	Vincoli di risorse
37%	Gestione delle vulnerabilità
28%	Gestione delle misure proattive di prevenzione degli attacchi
15%	Auditing
5%	Comportamento degli utenti



Ransomware e phishing

via email e gli attaccanti continuano effettivamente a usare l'email per questi attacchi...
Le paiattaforme in Cloud possono essere sfruttate per inviare file e link malevoli ai sistemi target.

Visibilità e controllo degli accessi
, i nostri esperti hanno evidenziato anche l'importanza della visibilità e del controllo delle connessioni di rete. Le aziende devono comprendere a fondo il modo in cui gli utenti interni ed esterni possono accedere ai dati e ai sistemi critici e il modo in cui connette e interagisce con altri sistemi.

Gli attacchi alla **supply chain** hanno dominato il panorama generale della cyber security negli ultimi due anni

I FILE E GLI URL MALEVOLI SONO IN AUMENTO

Primi 5 rilevamenti e tipi di file dannosi

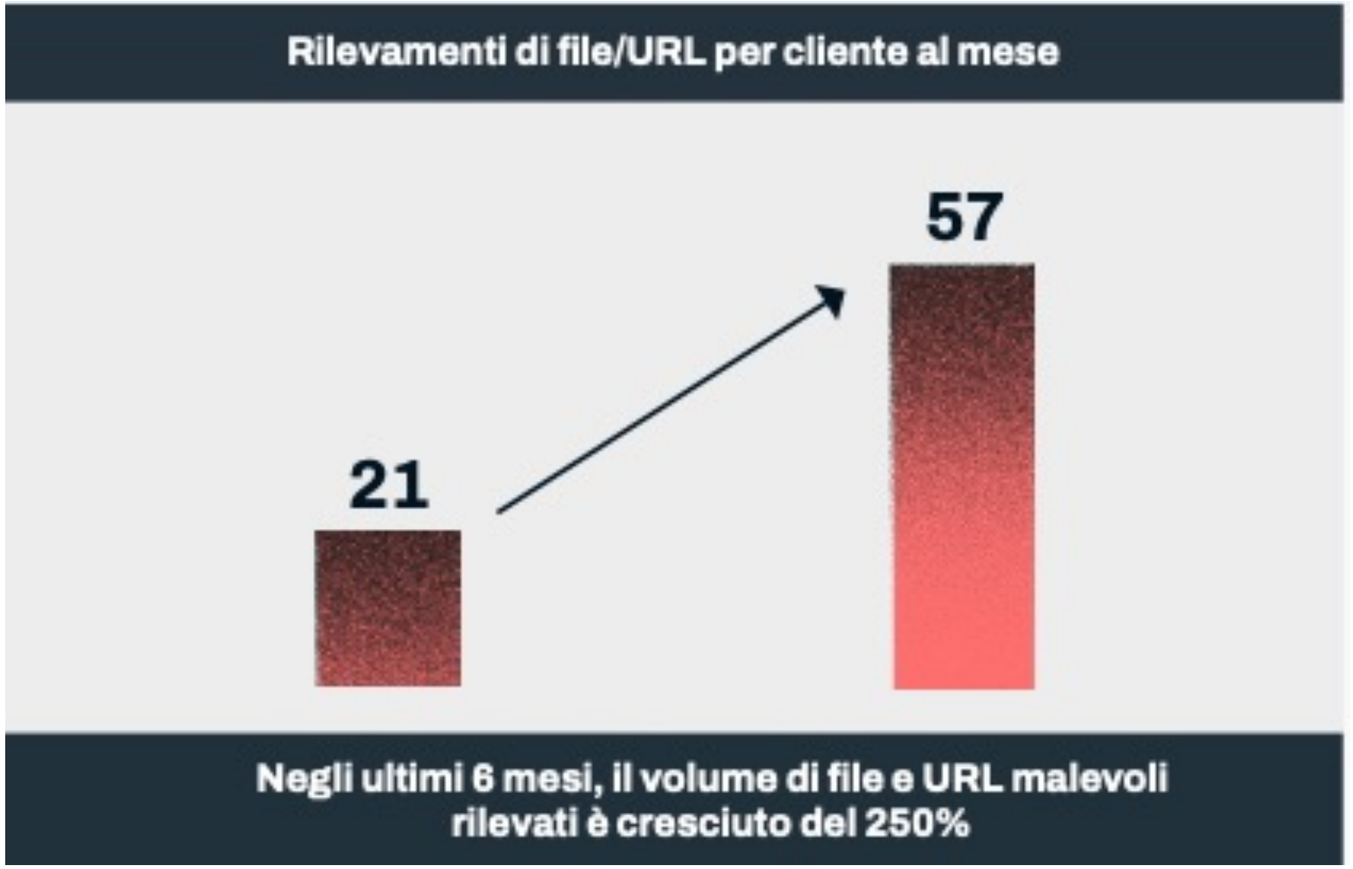
1. File HTML 49 %
2. Archivi RAR/ZIP 23 %
3. File Microsoft Office 10%
4. File exe/com 4 %
5. File PDF 3%

*ultimi 6 mesi

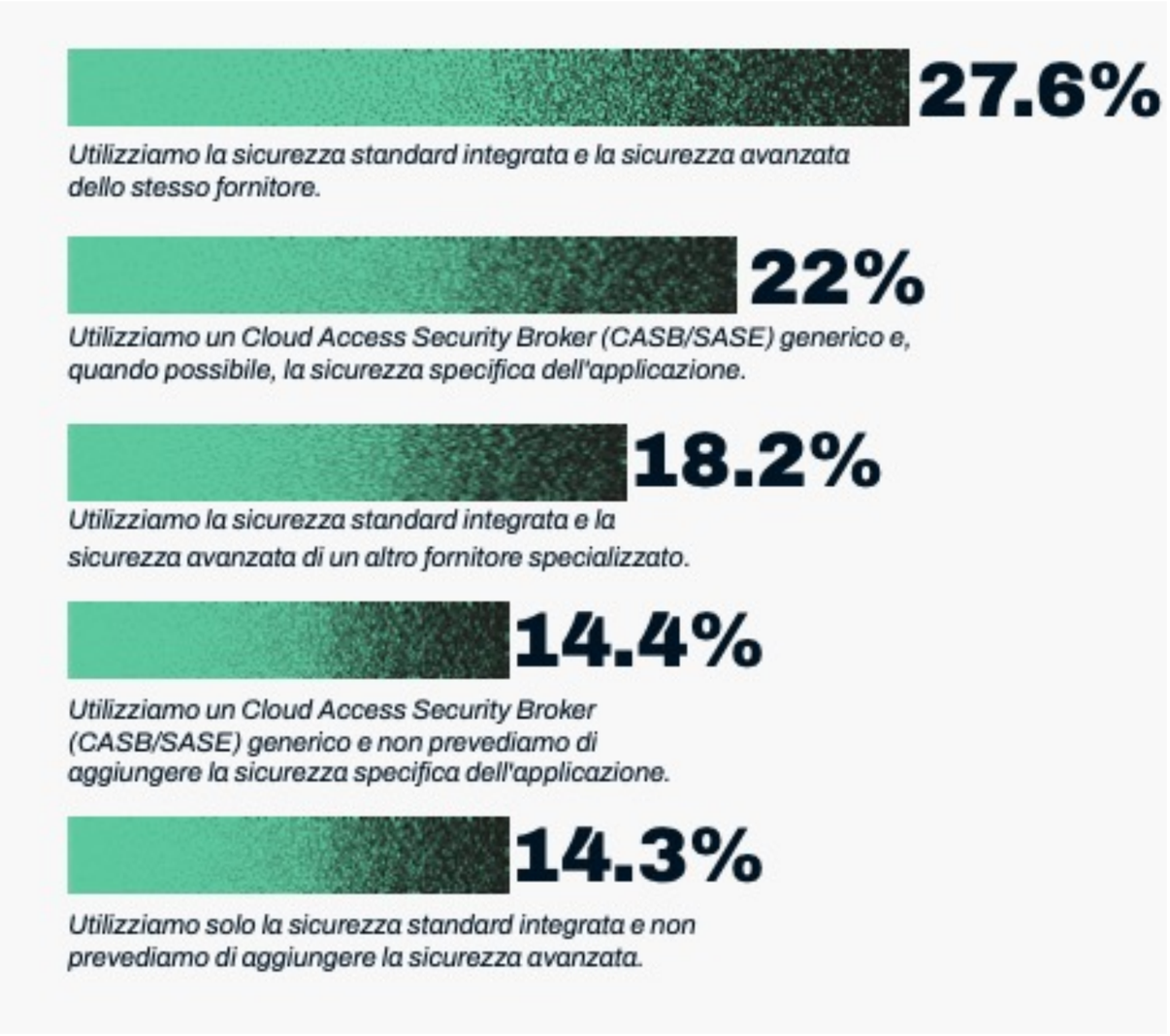
Primi 5 tipi di malware:

1. Trojan 54%
2. Adware 15%
3. Exploit 12%
4. Altro 12%
5. Downloader 2%

*ultimi 6 mesi



TROVARE I GIUSTI CONTROLLI DI SICUREZZA



Quali delle seguenti affermazioni sulla sicurezza delle applicazioni cloud si adattano meglio alla tua azienda/organizzazione?

Fortify your cloud security posture

Scan regularly

Conduct comprehensive cloud security posture scans that utilize the expertise of our research team about real-world threats.

Your cloud – secured

Coverage for AWS and Azure cloud platform infrastructures.

Prioritize efficiently

Review our visual CSPM dashboard to see important information which requires your attention, in easy-to-interpret graphs.

Risk-based guidance

Risk severity is calculated and ranked as high, medium, or low. Use risk-based guidance to remediate the cloud misconfigurations.

Simplified reporting

Easy-to-read reports visualize cloud security risks and empower correct response for administrators – as well as help to report on security practices to auditors and regulators.

Consolidated security management

Manage your cloud security posture from one easy-to-use portal along with endpoint security, collaboration protection and vulnerability management.

WithSecure™ Elements Cloud Security Posture Management

Spot mistakes before attackers do

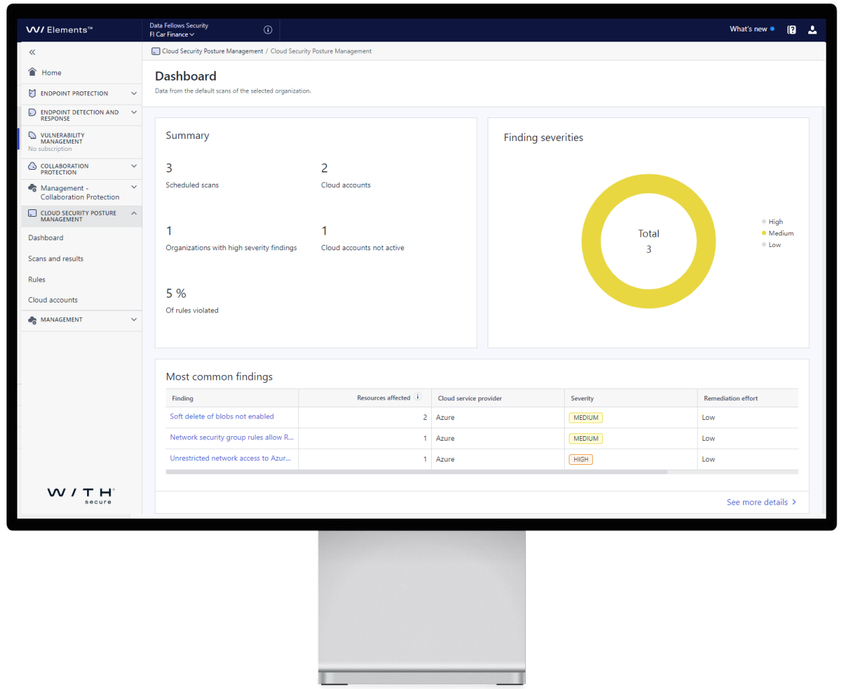
We cover end-to-end use cases and make the user's daily job easier with intuitive views summarizing the security posture, and clear flows which focus only on the essentials.

Identify misconfigurations quickly

We save customers' and partners' time through enabling efficient detection of misconfigurations and automated response actions. The scans are very fast, and you can easily see the evolution of the remediations.

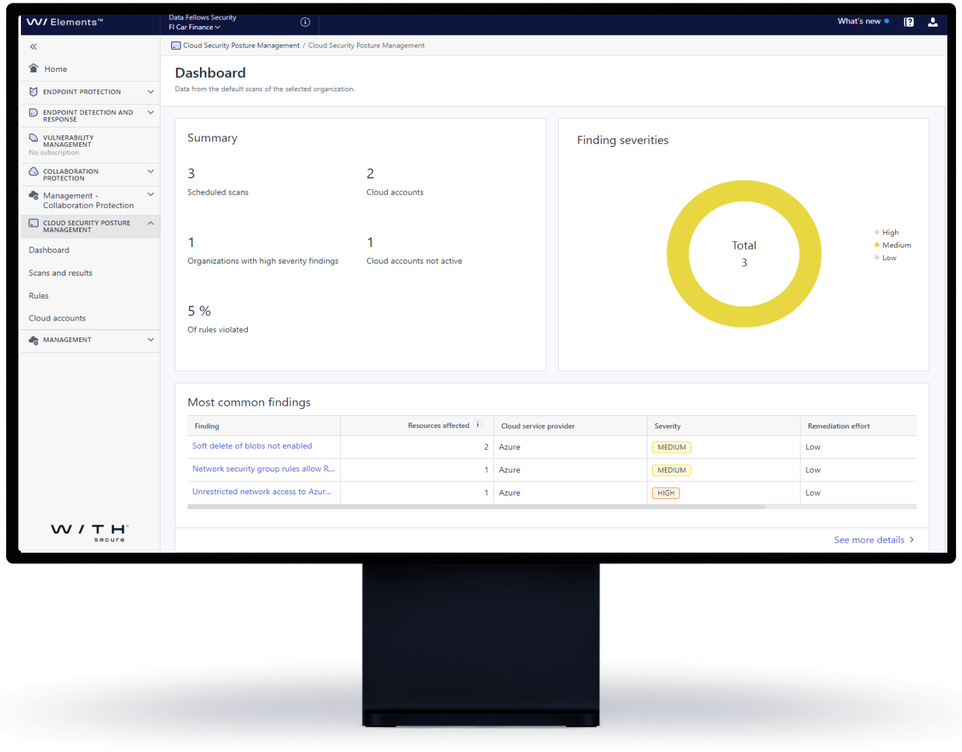
Reduce risk, complexity, and inefficiency

Prioritize remediation efficiently based on risk and effort level. Quickly remediate misconfigurations with helpful, actionable insights. Our visual reporting not only empowers administrators to make changes that improve security posture the most, but also helps provide evidence to auditors and regulators.



WithSecure™ Elements

Cloud Security Posture Management



Key features

- **Multi-company, multi-cloud management**
- **Cloud security posture visibility**
- **Basis in research and expertise**
- **Centralized management**
- **Fast scanning**
- **Automated scans**
- **Remediation guidance**
- **Visual tracking**
- **Highlight compliance issues**

Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT VERONA

A protection scenario

1. CSPM scan of your cloud environment

AWS

Azure

2. Finding EC2 has a public IP address

3. Review associated risks and remediation steps

4. Investigate whether the IP is required for business use

5. Action: Enforce the use of private IP.

By adding a load balancer as an additional layer of security.

GRAZIE

Q&A