2026 Report

A year of CERT-Wavestone investigations and threat analysis

CERT
WAVESTONE



WAVESTONE

Who are we?

Wavestone, a global consulting powerhouse...

€950m

revenue

6,000+

employees

Note: Revenue relates to fiscal year 2025/26 (April 1, 2025, to March 31, 2026)

3 key regions

France, GSA(1), US/UK

High value

consulting services for tier-1 clients

(1) GSA: Germany - Switzerland - Austria



A 24/7 center of excellence for incident response and crisis management

40+ Experts
Supported by 1000+ cyber consultants worldwide

50+ Incident Responses
Every year covering all activity sectors and company sizes

10+ years
Recognized as a trusted actor (PRIS, TF-CSIRT, InterCert).

DURING INCIDENTS...

- **FORENSIC INVESTIGATIONS AND ANALYSIS**
  Analysis of systems, networks, and source code
- **CRISIS MANAGEMENT**
  Coordination, anticipation, support of internal & external communications, and assistance with regulatory obligations
- **DEFENSIVE STRATEGIES**
- **REMEDIATION AND REBUILDING**
- **THREAT IDENTIFICATION**

...AND PROACTIVELY

- **CYBER THREAT INTELLIGENCE**
- **CSIRT STRENGTHENING**
- **CRISIS EXERCISES**
- **CYBER ATTACK SIMULATION**
  RedTeam / Purple-team / Cyber Range
- **SOC & CSIRT ENHANCEMENT**
  Maturity assessment, training and action plans
- **PHISHING CAMPAIGNS**
- **CYBER RESILIENCE ASSESSMENT**
- **EXTERNAL ATTACK SURFACE ASSESSMENT**

VISA DE SÉCURITÉ – ANSSI

Wavestone was the first company to obtain and renew the ANSSI certification for Cybersecurity Incident Response Service Provider (PRIS-LPM) across all service scopes:

- **COMPROMISE INDICATOR HUNTING [REC]**
- **DIGITAL FORENSIC INVESTIGATIONS [INV]**
- **MALWARE CODE ANALYSIS [CODE]**
- **INVESTIGATION MANAGEMENT AND COORDINATION [PCI]**

This report presents an analysis of the 33 major cybersecurity incidents investigated by CERT-W between August 2025 and September 2026 across a diverse set of sectors, ranging from public administration and healthcare to financial services and industry.

Key shifts in the cyber threat landscape

Profit-driven motivations

57%
Financial gain, still the dominant motivation

Exploit-led attack methods

36%
Via vulnerability exploitation

A widening attack surface

< 24 h
Fastest attacker time-to-impact

141 days / 18 days
Average / median detection delay

The study at a glance

121
Incidents assessed by CERT-Wavestone

33
Major incident responses

15
Industry sectors

Aug 2025 – Sept 2026
observation period

Key takeaways

1. Ransomware is moving beyond encryption towards data theft and extortion.
2. AI is expanding the attack surface and accelerating attacks.

Key shifts in the cyber threat landscape

Profit-driven motivations

Exploit-led attack methods

A widening attack surface

Key takeaways

“Financial gain remains the primary driver, while espionage and reputational damage complete the threat picture”

OBSERVATIONS FROM CERT-WAVESTONE INCIDENT INVESTIGATIONS

Financially motivated attacks remain dominant

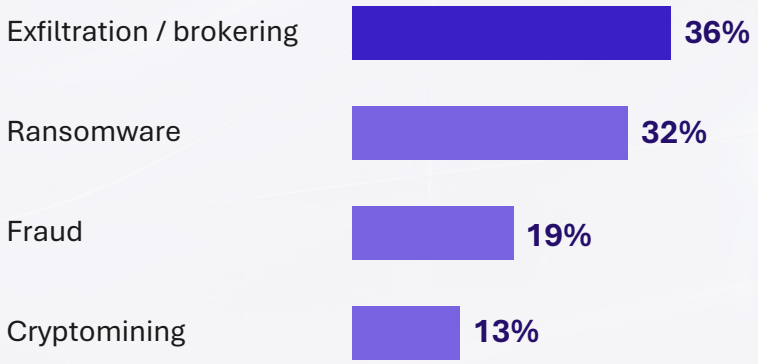
Ransomware and data exfiltration-related operations remain the top threats in 2026

Financial gain 57%

Attacks driven by direct financial returns: **extortion, fraudulent transfers** and **the sale of exfiltrated data or compromised access**.

vs. 65% in 2025

Breakdown of financially motivated attacks





Unknown 27%

Motives remain unclear due to limited impact, early disruption or insufficient evidence.

vs. 18% in 2025

Reputation 13%

Deliberate exfiltration and **full publication of sensitive data** to damage the victim's reputation and build the actor's notoriety.

Not tracked in 2025

Espionage 3%

Significantly underrepresented: inherently **difficult to detect and attribute**, these attacks can persist unnoticed for years or be contained before any visible impact.

vs. 17% in 2025

CERT-W Report

Key shifts in the cyber threat landscape

Profit-driven motivations

Exploit-led attack methods

A widening attack surface

Key takeaways



> **Vulnerability exploitation takes the lead, identity compromise follows, shifting from phishing to credential and session theft**

OBSERVATIONS FROM CERT-WAVESTONE INCIDENT INVESTIGATIONS

What intrusion vectors are attackers using?

Attackers are increasingly relying on vulnerability exploitation for initial access

Vulnerability exploitation is now the **leading intrusion vector** observed by our teams, in line with worldwide trends. **Email phishing is losing ground** against large enterprises, which are better equipped, but **social engineering is not receding: it is shifting channels**, towards voice, SMS and legitimate authentication flows. At the same time, **attacks targeting SaaS platforms, exposed services and third-party providers** are becoming increasingly prominent.

36%

(vs. 20% in 2025)

VULNERABILITY EXPLOITATION

Attackers exploit vulnerabilities affecting internet-facing systems to gain an initial foothold.

Observed cases involved VPN gateways, web applications and security appliances affected by both unpatched and zero-day vulnerabilities.

30%

(vs. 22% in 2025)

VALID ACCOUNTS

Attackers compromise legitimate employee accounts using stolen or brokered credentials, *allowing them to access business applications in 55% of cases and exposed infrastructure services in the remaining 45%*, making malicious activity difficult to differentiate from legitimate business operations.

15%

(vs. 38% in 2025)

PHISHING & SOCIAL ENGINEERING

Attackers manipulate users into revealing credentials or executing malicious actions.

Observed techniques include traditional phishing, Evilginx-style session hijacking and device code phishing, resulting in account compromise, fraud and further phishing campaigns.

3%

(not tracked in 2025)

THIRD-PARTY COMPROMISE

Attackers compromise trusted third parties, software providers or dependencies *(e.g. Shai-Hulud)*.

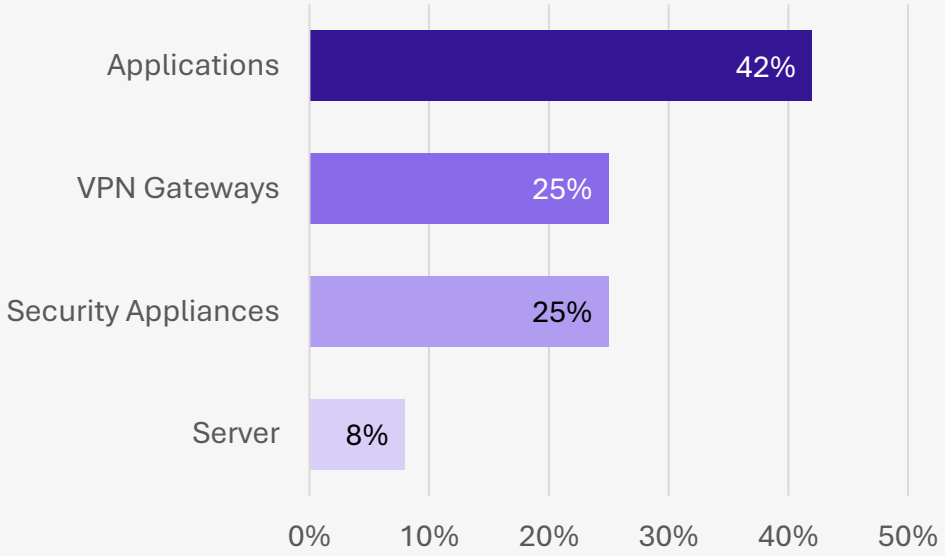
Vulnerability exploitation became the leading initial access vector



Nearly three-quarters of exploitation cases involved known vulnerabilities (N-days), emphasizing that the majority of successful intrusions still rely on weaknesses for which fixes are already available. Combined with the growing use of automation and AI to identify and prioritize vulnerable targets, this trend continues to shorten the remediation window available to organizations.

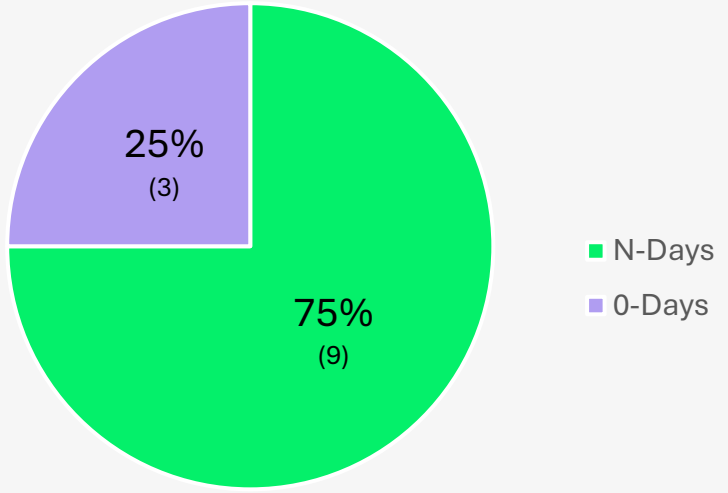
Attackers exploited a broad range of internet-facing assets...

Most targeted product categories



...using both unpatched N-days and previously unknown vulnerabilities.

Incidents involving 0-Days or N-Days vulnerability exploitation



**0-Days: a vulnerability exploited before a patch is available, or within three days of its release.*

Vulnerability exploitation focus

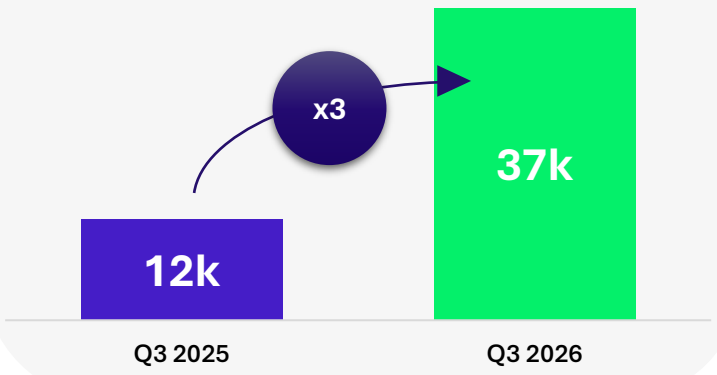
AI is accelerating vulnerability discovery and exploitation



In 2026, **Claude Mythos demonstrated the ability to identify and exploit zero-day vulnerabilities**, building end-to-end exploit chains, including a full Windows escalation chain in 31 minutes. Frontline data shows the same compression: **disclosure volumes have tripled, exploitation at disclosure is up by half, and patching everything is no longer an option**.

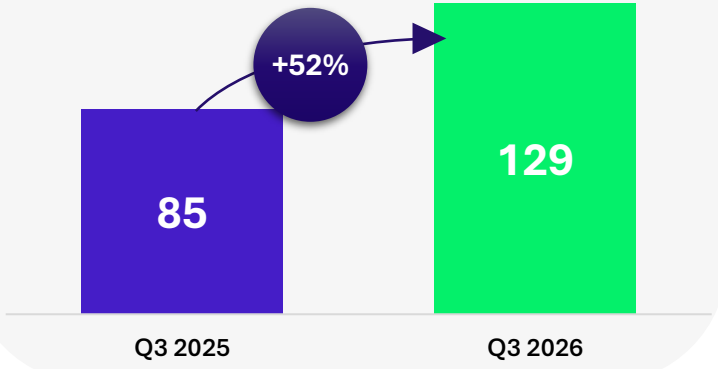
Disclosure volume has tripled

CVE records published, same quarter year on year



Exploitation at disclosure is accelerating

CVEs listed as exploited no later than their publication date



Prioritization decides coverage

Share of attacked CVEs covered by each patching rule, September 2026.

CISA KEV only **24%**

45 patches / month

Any KEV catalogue or EPSS ≥ 3% **79%**

629 patches / month

Patching everything = **14,872 patches / month**

*According to ZeroDayClock, 2026
*KEV: catalogues of vulnerabilities confirmed as exploited in the wild (CISA, ENISA, VulnCheck...).
*EPSS: daily score from FIRST estimating the probability of exploitation within 30 days.

BEC focus

From mailbox compromise to bank account fraud



A common fraud pattern observed across BEC incidents

Business Email Compromise (BEC) incidents investigated by the CERT-W often stem from the **compromise of Microsoft 365 email accounts**. After gaining access to a mailbox, attackers may monitor business communications, **identify financial transactions** and **key stakeholders**, and leverage the trust associated with legitimate exchanges to introduce **fraudulent bank account details** or validate **fake invoices**.

10%
of CERT incidents

€35k
average financial loss

8 days
fastest path to fraud
Up to 124 days

CERT-W CASE • TRANSPORTATION & STORAGE • OPPORTUNISTIC ATTACK • FINANCIAL MOTIVE

Anatomy of an incident

1. *Initial Access*

A user's **Microsoft 365 account** was **compromised** using **valid credentials**, in an opportunistic attack, giving access **to legitimate business communications**.

2. *Exploiting Trust*

Posing as a **legitimate trusted employee**, the attacker **engaged directly with a business partner** to initiate a **fraudulent bank account change** request.

3. *Evasion and Persistence*

Email forwarding rules and **typosquatted domains** were deployed to **maintain control** over communications while **avoiding detection**.

4. *Financial Fraud*

The fraudulent bank account details were accepted and used for **payment: funds were diverted** (€45k-55k) after 4 months of attacker presence.

Identity & SaaS focus

Compromised identities provide legitimate access to SaaS, cloud and business data



A compromised identity is often the gateway to the entire digital ecosystem

- Valid credentials, sessions or tokens give attackers **legitimate access** to mailboxes, SaaS platforms and business data, with no exploit required.
- They come from phishing, infostealers, credential reuse or **purchase on criminal markets**.

One purchased account, three ways to monetize it

CERT-W CASE • HEALTHCARE SME • OPPORTUNISTIC ATTACK • FINANCIAL MOTIVE

1. Legitimate access

Attacker logs in with **purchased credentials** of a user account on a medical platform. **No malware, no exploit.**

2. Data enumeration

The account is used to **enumerate patient data** available on the platform and **exfiltrate it**.

3. Resale

Multiple platform accounts are **sold on the dark web** for financial gain.

4. Follow-on phishing

Mass phishing SMS are sent **from the compromised account**, extending the impact to other victims.

Legitimate access makes malicious activity look normal. Detection must go beyond authentication: monitor **abnormal logins, data enumeration and bulk messaging** from legitimate accounts.

30%

of our CERT incidents involved SaaS, Microsoft 365 or CRM environments

Compromised credentials, valid sessions and OAuth tokens can provide access to business data and federated applications without directly compromising the SaaS platform.

900+

recipients targeted by phishing from a single compromised Microsoft 365 mailbox

A compromised account can lead to an extremely wide ripple effect within an organization

Device Code Phishing: the commoditization of an advanced identity attack



Phishing

Impersonating a trusted party (email, SMS, call, QR code) to steal credentials or gain access

Device code phishing

Abuses the OAuth 2.0 device authorization flow: the victim enters the attacker's code on Microsoft's genuine login page and hands over valid access and refresh tokens

Why attackers use device code phishing

Device code phishing abuses **legitimate authentication flow**, allowing attackers to gain access without having to fake the login page the victim sees.

Initially observed in state-linked operations, the **technique is now increasingly adopted by cybercriminals** and commoditized through Phishing-as-a-service (PhaaS).

Two leading kits drive the democratization of device code phishing

CERT-W CASE • SERVICES COMPANY • OPPORTUNISTIC ATTACK • FINANCIAL MOTIVE

1. Phishing lure

A third party sends a **phishing email with a PDF** whose link asks the user to open a document.

2. Device code

The user enters a **device code on the legitimate Microsoft page**, authorizing the attacker's application on their account.

3. Mailbox discovery

The attacker browses the mailbox, which **could expose sensitive documents** and third-party information.

4. Phishing relay

The mailbox launches a **new phishing campaign to 900+ addresses** of people who had interacted with the user.

What to look for and do

- Unexpected device code sign-ins in Entra ID logs
- Unusual sign-in IPs and User-Agents
- uniqueTokenIdentifier in non-interactive sign-ins
- Revoke sessions and tokens, not just passwords

CERT-W Report

Key shifts in the cyber threat landscape

Profit-driven motivations

Exploit-led attack methods

A widening attack surface

Key takeaways

> The attack surface now extends beyond IT to OT environments, identities and AI systems, while the pace of attacks leaves less time to detect and respond

OBSERVATIONS FROM CERT-WAVESTONE INCIDENT INVESTIGATIONS

Time to impact vs time to detect: a widening gap

FASTEST INCIDENT

< 24 hours

is the shortest time observed for attackers to achieve impact after an intrusion, compared to 1.5 days in 2025.

VS

ACROSS ALL 33 INCIDENTS

141 days

is the **average time** between an intrusion and detection across this year's incidents.

18 days

is the **median time** between an intrusion and detection across this year's incidents.

CERT-W CASE • ARTS & CULTURE • OPPORTUNISTIC ATTACK • FINANCIAL MOTIVE

How an attacker reaches impact in under a day

INSIDE ONE OF THIS YEAR'S FASTEST INCIDENTS

1. Initial access

Qilin exploited a CVE affecting the company's VPN *to gain initial access ...*

2. Privileged access

... then compromised **highly privileged accounts** *by brute force.*

3. Defense evasion

The attackers **disabled the antivirus**, *then created services and dropped executables.*

4. Impact

Workstations were **encrypted, data extracted** *and PowerShell, Security and System* **logs wiped.**

Getting in is no longer the hard part: **exposed VPNs and access brokers have commoditized initial access**. What matters is what happens next: the **most capable groups go from foothold to encryption in under a day**, while intrusions stay undetected for 141 days on average. Detection must therefore **target the post-compromise chain** (privileged account abuse, mass tool deployment, log clearing), not just the perimeter.

AI focus

AI Adoption: Accelerating innovation, expanding attack surfaces

40% of enterprises develop proprietary AI models

50% of enterprises design AI systems internally using existing frameworks or pre-trained models

Source: 2026 AI Cyber Benchmark – Wavestone, based on 30 large public and private sector clients

Securing AI in RUN

Rushed adoption
Rapid procurement, vibe-coded, late reviews.

Highly connected systems
Apps and AI gateways exposed, linked to models.

Privileged access
API keys, quotas, broad default permissions.

Autonomous data manipulation
Agents can read, alter or delete business data, and can be hijacked through prompt injection to do so on an attacker's behalf.

Securing vibe coding

Benefits	Risks
Faster development and prototyping	Vulnerabilities from weak security design
Non-developers can build with AI	Reduced code ownership and maintainability
Higher productivity on repetitive tasks	Compliance and data leakage risks
Encourages experimentation and innovation	Hallucinated packages and hardcoded secrets

AI used by attackers

AI-powered deception at scale
Charcoal Typhoon – Jasper Sleet

Faster vulnerability research
Coral Sleet – Emerald Sleet

AI-assisted and agentic malware
APT28 – GreyVibe – PunkSpider

AI adoption must be secured before scale outpaces control. Each agent connected to identities, data and APIs widens the attack surface, while attackers use the same AI to move faster. Security must scale ahead of adoption: AI assets inventoried, least-privileged and continuously monitored.

CERT-W Report

Key shifts in the cyber threat landscape

Profit-driven motivations

Exploit-led attack methods

A widening attack surface

Key takeaways



> **Latest attacks & AI raise the stakes on a few priorities, yet the core of the answer remains the fundamentals: exposure, identities, detection and recovery**

OBSERVATIONS FROM CERT-WAVESTONE INCIDENT INVESTIGATIONS

Key takeaways

Eight priorities to reduce exposure and accelerate response

Vulnerabilities & exposed assets

- Continuously inventory **internet-facing assets**: VPNs, applications, appliances.
- Prioritize patching by **active exploitation**, exposure and **business criticality**.
- Apply **compensating controls** when patching is not possible.

Identities & remote access

- Enforce **phishing-resistant MFA** on remote, privileged and SaaS access.
- Detect **compromised credentials** and unusual logins, **harden help desk resets**.
- **Reduce privileges** and disable **stale accounts** quickly.

Phishing, Device Code & OAuth

- Restrict or disable **Device Code Flow** where it is not required.
- Govern **OAuth consents** and monitor newly authorized apps.
- After compromise, **revoke sessions and tokens**, not just passwords.

Cloud, SaaS & BEC

- Inventory connected apps, **service accounts, API keys** and tokens.
- Monitor **forwarding rules**, mass exports and **abnormal API activity**.
- **Verify bank detail changes** out-of-band, using a known contact.



Ransomware & IT/OT

- **Segment access** between IT, OT and administration tiers.
- Protect **directories, hypervisors and admin tooling** first, and keep immutable, offline backups.
- Test **emergency isolation**, restoration and crisis scenarios with OT.

Detection & incident response

- Centralize critical logs off-host and retain them for at least 12 months.
- Detect recon, **lateral movement**, RMM use and **exfiltration**.
- Prepare for attacks reaching impact in **under 24 hours**.

AI adoption & offensive use

- **Security-review** AI solutions and **vibe-coded apps** before production.
- Protect **AI gateways, API keys**, agents and sensitive data.
- Factor **AI-accelerated phishing** and exploitation into threat scenarios.

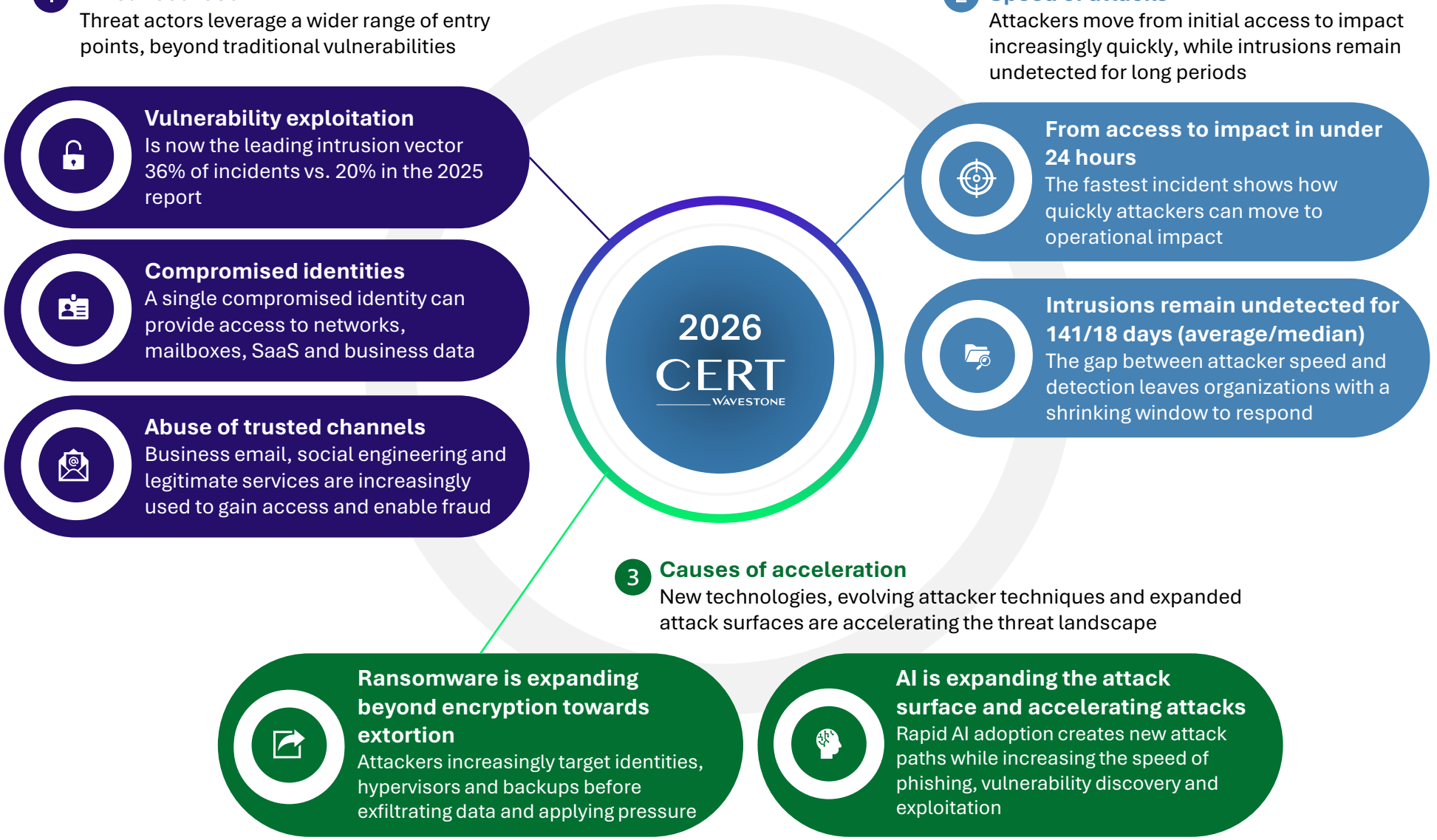
Third parties & supply chain

- Map **critical suppliers, MSPs** and remote maintenance access.
- Impose MFA, logging and least privilege on **third-party access**.
- Include key suppliers in **crisis exercises** and notification chains.

The Mythos era changes the defensive equation: when AI accelerates vulnerability discovery and attack development, resilience depends on reducing exposure, accelerating remediation and closing the gap between intelligence and action.

Executive summary

The threat landscape in 2026: key takeaways



Key takeaways

Threat sources are shifting

Attackers leverage a broader range of entry points, from vulnerabilities to identities, trusted services and interconnected environments

The defensive window is shrinking

Attackers increasingly move from initial access to impact faster than organizations can detect and contain them

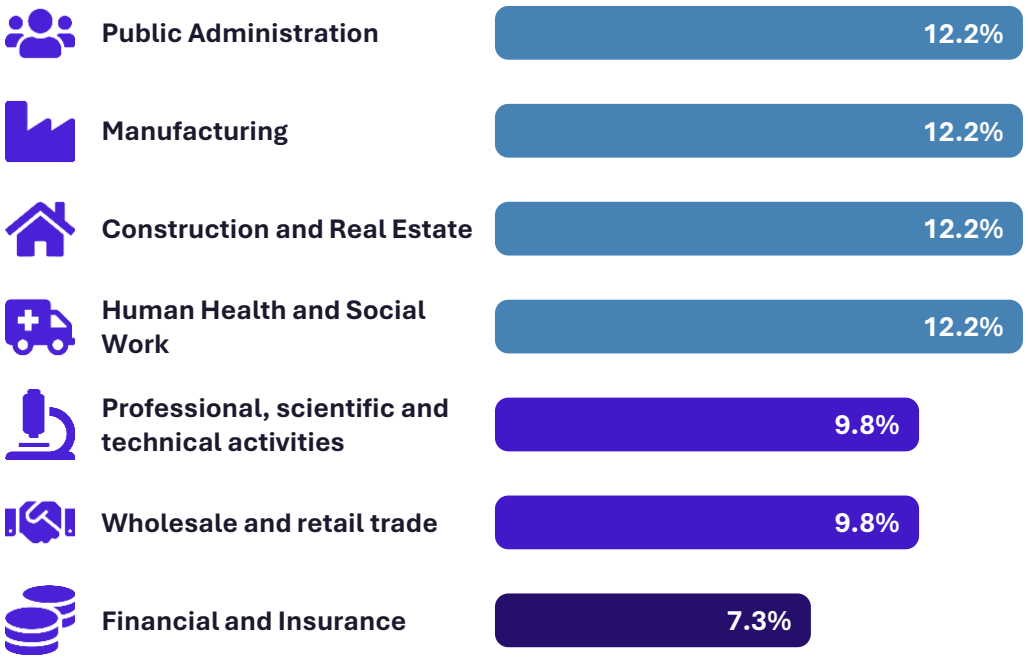
The attack surface is expanding

AI, cloud/SaaS, OT and increasingly connected environments are creating new opportunities for attackers

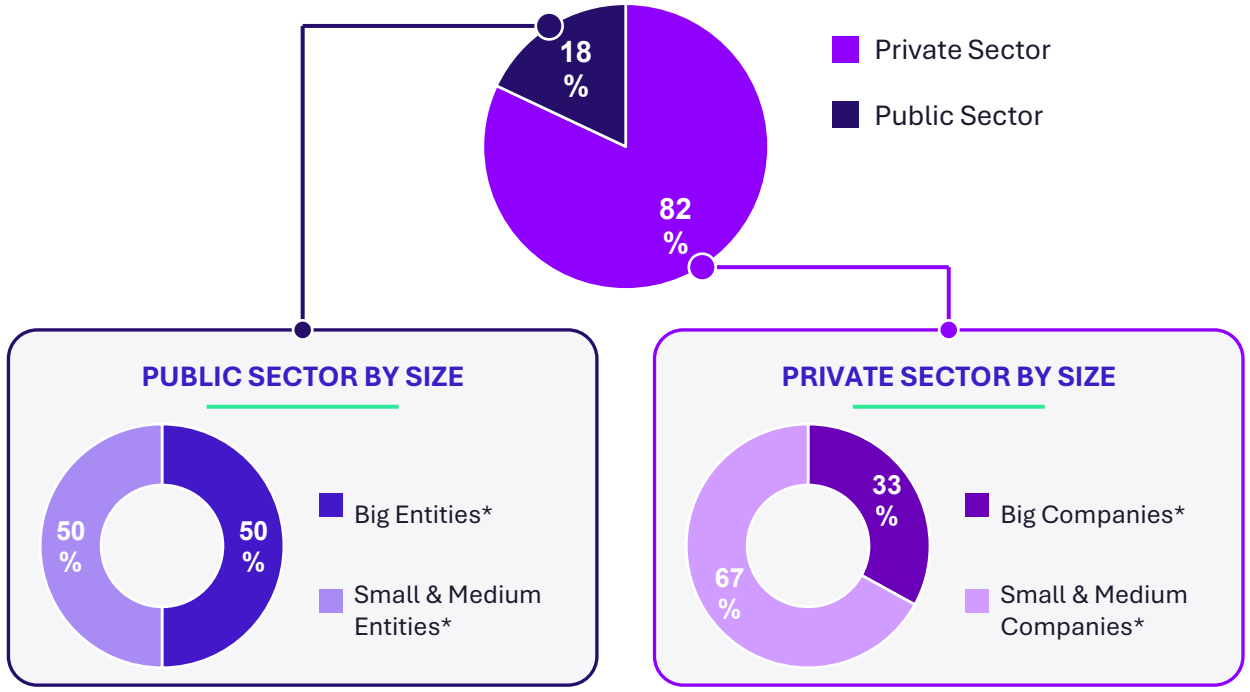
Cyber incidents handled by CERT-W across all sectors and company sizes

The report analyzes the incident response engagements handled by CERT-W between August 2025 and September 2026 across **major industry sectors**. It is based on **incident reports** produced by our analysts and consolidated within a single shared database, with additional insights from Wavestone's CTI team to contextualize these incidents.

MOST REPRESENTED SECTORS



BREAKDOWN BY SECTOR



*Public sector: big entities include ministries and affiliated agencies; small & medium entities include local authorities and other public organizations.
Private sector: big companies generate annual revenues above €1.5 billion with 5,000+ employees; small & medium companies are below.
Sectors are classified according to INSEE activity sections and reflect CERT-Wavestone investigations only, not the actual distribution of cyber incidents across sectors.

CERT-Wavestone Report

2026 Edition



Gérôme BILLOIS, Partner
gerome.billois@wavestone.com



Alexandre BENAC, Manager
alexandre.benac@wavestone.com



Valentine TAUZIN, Consultant
valentine.tauzin@wavestone.com

WAVESTONE


WAVESTONE