Lookout®

As Organizations Evolve, So Does RANSOMWARE

How the RANSOMWARE ATTACKS of 2021 will impact the security strategies of 2022 and beyond

Ransomware is a threat to every industry and will continue to be a thorn in the side of IT, security and business teams as organizations continue to support hybrid work. The perimeter that once gave you visibility and control over data and how your users interact with it has all but disappeared.

This problem will continue to grow as the ransomware-as-a-service (RaaS) market becomes more lucrative and cybercrime gangs behind these attacks run themselves like businesses. In 2021, there were 68 different known ransomware variants – many of which are offered through the RaaS model. The most utilized in cyberattacks were REvil/Sodinokibi, Conti, DarkSide, Avaddon, and Phobos.[1]

For victims of these attacks, the question of whether to pay is made even more difficult by the fact that there's no guarantee they will get their data back intact. After payment was made, data was often found to be corrupted or otherwise compromised. To add to the complexity, many attackers are using double extortion, where data is exfiltrated and used as leverage if payment demands are not made.[2]

Most of your employees have access to sensitive cloud data, and now access it from personal unmanaged devices. This opens up opportunities for attackers to trick your employees with socially engineered phishing attacks, as employees are less security-conscious on personal devices. This is often how cybercriminals kick off the first steps of advanced cyberattacks like ransomware.

[1] https://www.forbes.com/sites/chuckbrooks/2021/10/24/more-alarming-cybersecurity-stats-for-2021-/?sh=13834a734a36
[2] https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

91%

of organizations aren't able to detect malware in mobile enterprise messaging apps.[3]

63%

of organizations aren't able to control connected cloud apps.[4]

IN 2021 ALONE, **37%**

of global organizations reported a ransomware attack.[5]

The average cost of ransomware recovery doubled from $761,000 in 2020 to

$1.85M USD IN 2021[6]

~X2

The percentage of companies purchasing cyber insurance nearly doubled over the previous five years.[7]

Three of the most common tactics that attackers use to initiate a ransomware attack are:

1. **Phishing schemes, vulnerability exploits, and purchasing credentials on the dark web:** These have become the three most common ways for attackers to gain initial access to your infrastructure. Once they have access, they're free to create a backdoor into your organization, observe existing security tools and behaviors, then move laterally to identify your most critical assets to encrypt.
2. **Risky apps and software vulnerabilities:** The software supply chain has also become a way for attackers to cast a wide net and gain access to a broader number of assets that could potentially be encrypted in the execution of a ransomware attack.
3. **Remote Desktop Protocol (RDP) vulnerabilities:** Securing remote access is the most critical way to mitigate the risk of ransomware and makes it easier to tie to your greater security strategy.

[3] https://www.helpnetsecurity.com/2020/07/09/byod-adoption-is-growing-rapidly-but-security-is-lagging/

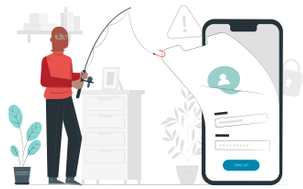
[4] https://www.helpnetsecurity.com/2020/07/09/byod-adoption-is-growing-rapidly-but-security-is-lagging/

[5] https://www.idc.com/getdoc.jsp?containerId=US48093721 as well as the largest ransomware payment ever recorded when an insurance company paid out a $40 million ransom.

[6] https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year

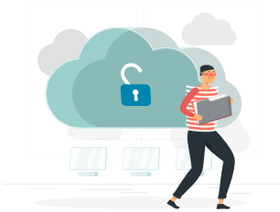
[7] https://themarkup.org/ask-the-markup/2021/06/15/why-is-ransomware-on-the-rise

How a Typical RANSOMWARE ATTACK Happens



1 Identification and Surveillance

2 Access



3 Execution

4 Persistence

5 Privilege escalation

6 Defense evasion

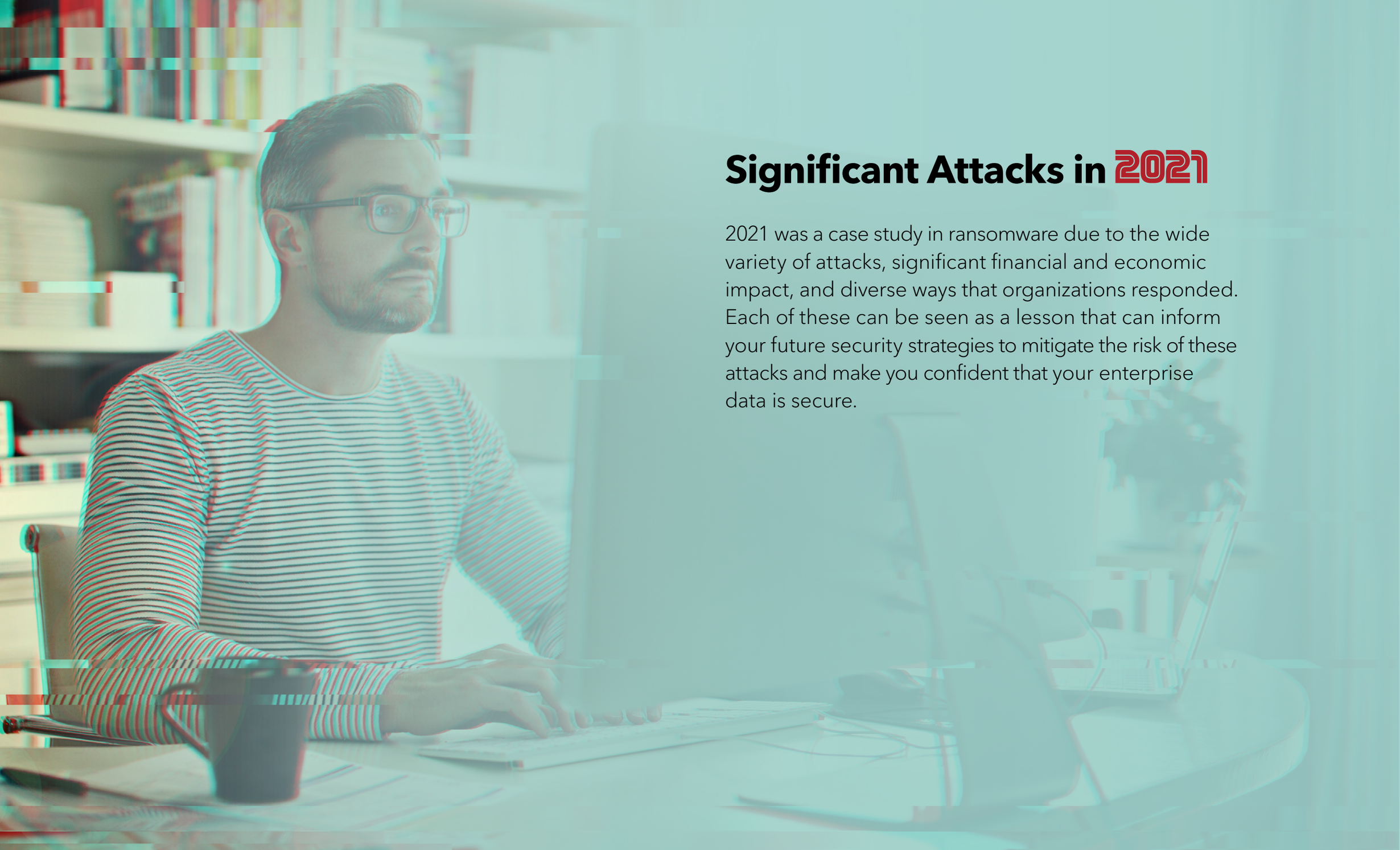
7 Discovery

8 Lateral movement

9 Command and control

10 Exfiltration

11 Impact



Significant Attacks in 2021

2021 was a case study in ransomware due to the wide variety of attacks, significant financial and economic impact, and diverse ways that organizations responded. Each of these can be seen as a lesson that can inform your future security strategies to mitigate the risk of these attacks and make you confident that your enterprise data is secure.

CNA Financial

CNA Financial, one of the top ten commercial insurers in the United States, suffered a ransomware attack at the hands of the Phoenix group. Employees were locked out of the network and data was both exfiltrated and encrypted. In order to continue operations and minimize losses, CNA eventually paid the ransom of $40 million.

Find patterns in the chaos with user and entity behavior analytics (UEBA).

READ THE BLOG →

JBS Foods

A few weeks after the Colonial Pipeline attack, the world's largest meat supplier, JBS Foods, was hit by a ransomware attack that forced the company to close nine of its plants in the United States. The multi-day closure also impacted several other plants across the globe and had a significant impact in Australia and Canada.[10] There was over 45 GB of data exfiltrated from JBS' infrastructure.

Data loss prevention and CASB can provide full visibility and protection for SaaS applications.

LEARN MORE →

CNA eventually paid the ransom of

$40 Million

Colonial Pipeline

The Colonial Pipeline attack shut down the largest pipeline in the U.S. for five days, causing significant disruption in the gasoline supply chain. DarkSide, the group responsible for the attack, targeted the billing system used by Colonial Pipeline.[8] The attackers gained access to systems with stolen employee credentials and used them to access a company VPN that didn't require multi-factor authentication.[9]

ZTNAs address requirements VPNs cannot. Here's why.

READ THE BLOG →

[8] https://www.lookout.com/blog/3-actions-to-take-based-on-the-colonial-pipeline-ransomware-attack.
[9] https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
[10] https://www.washingtonpost.com/technology/2021/06/09/jbs-11-million-ransom

AndroidOS/MalLocker.B

Ransomware isn't only an issue for computers and servers. A mobile ransomware variant called AndroidOS/MalLocker.B saw significant adoption in 2021. It appears to use machine learning in order to learn and evolve so that it can combat new security measures, which will ensure the survival and growth of this malware family far into the future.

Read threat advisory on AndroidOS/MalLocker.B.

LEARN MORE →

Authorities arrested 14
alleged members of the
Russia-based REvil ransomware
gang during police raids at 25
addresses in January 2022.

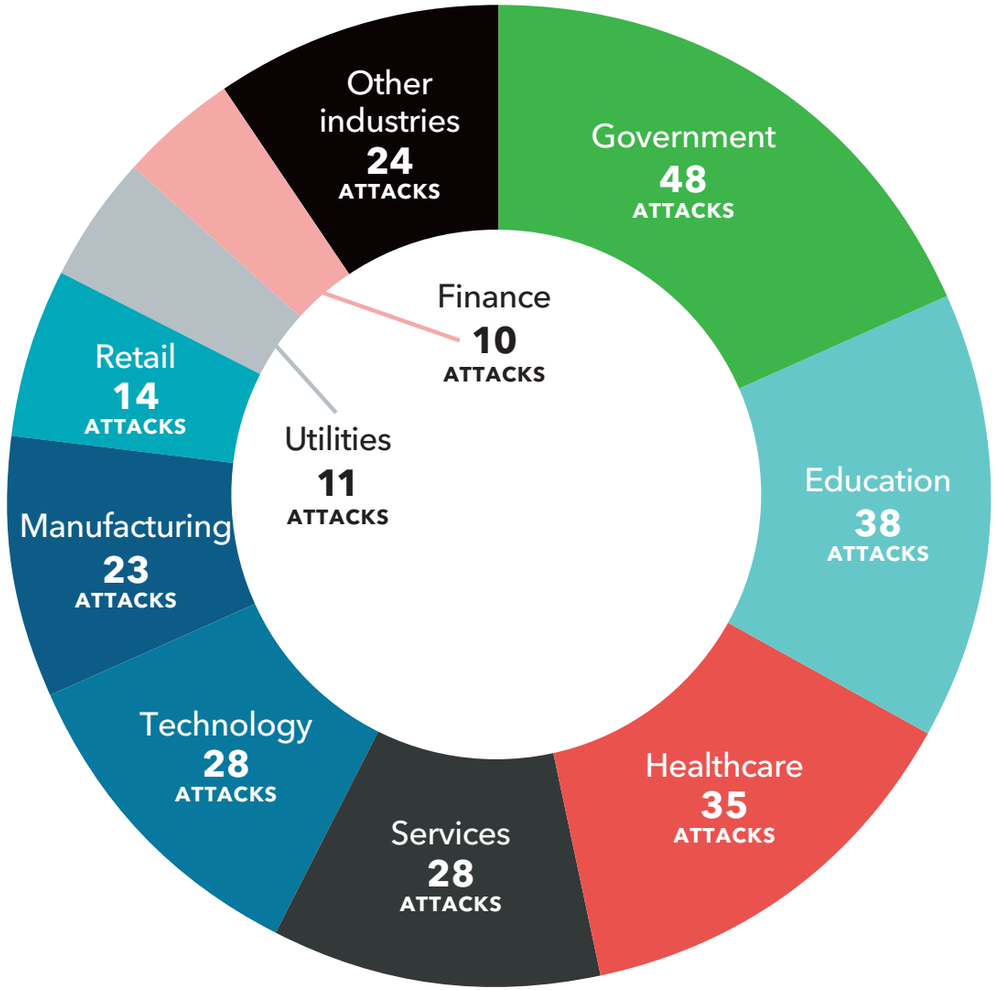
Kaseya

In early July, IT service provider Kaseya disclosed that its systems had been compromised and infiltrated by a ransomware attack from the REvil gang. This attack not only affected 50 direct customers of Kaseya but created a chain reaction that also impacted between 800 and 1,500 other organizations down the chain. Many of these organizations were also asked to pay ransoms.

Learn how security delivered from one unified cloud-delivered platform can defend your organization at each step of a ransomware attack.

GET THE INFOGRAPHIC →

Industries most susceptible to RANSOMWARE[11]



[11] https://www.nasdaq.com/articles/these-industries-are-most-susceptible-to-ransomware

4 KEY Actions to Take

Every cybersecurity event can inform how you can better secure your data and infrastructure in the future. There were nuances to each of these attacks in 2021 but looking at them together and identifying the commonalities between them leaves you with four key teaching points. These can each be put into action to better protect your organization against these type of attacks.

4 KEY ACTIONS TO TAKE

1. **Secure the edge** – wherever that may be

Detecting risky behavior and securing endpoints are crucial to reducing the impact of a ransomware attack. Protecting against initial compromise via web-based threats like phishing or exploiting web-facing private apps is critical. Furthermore, implementing multi factor authentication (MFA) will help protect your infrastructure even if the attacker gets access to legitimate credentials. Each of these protections can help prevent the attacker from entering the infrastructure, contain the attack and reduce the risk of lateral movement.

2. **Control access privileges** with tools and context

VPNs have their place, but the unbridled access they enable is risky. With users logging in from anywhere, it's critical to understand the context under which they're accessing your corporate apps and data. Clues such as location, device type, and the number of attempts can also quickly flag anomalous behavior and help you identify a compromised account - stopping the attacker before they can do any damage. If the attacker is able to enter, privilege access management (PAM) will make it harder for the attacker to gain admin privileges that could give them access to more sensitive data.

How to protect your data when ransomware strikes

READ THE BLOG →

3. **Prevent** data modification and exfiltration

Modern data loss prevention means protecting data both at rest and in motion. Modifications or duplications of data at rest can be indicative of a bad actor, and whatever data is exfiltrated should be encrypted regardless of whether the user is legitimate or not. This Zero Trust approach to data security will render exfiltrated data useless to ransomware actors.

4. **Protect** all endpoints

One compromised user or device can be detrimental to the security of the entire infrastructure. Beyond traditional endpoints, the inherent trust users have in smartphones and tablets can make them an attacker's easiest avenue of entry to corporate infrastructure. Protecting against mobile phishing attacks, malicious apps, and untrustworthy network connections can be the difference between secure functionality and a breach.

Ransomware will continue to evolve as you rely more heavily on the cloud, SaaS, remote work and unmanaged personal devices. Mitigate your risk of falling victim to a ransomware attack by safeguarding your sensitive information wherever it moves, however it moves.

Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO of Kaseya says.[12]

REUTERS

[12] https://www.reuters.com/technology/up-1500-businesses-affected-by-ransomware-attack-us-firms-ceo-says-2021-07-05/

Lookout®

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, VMware, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit: www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.

Identify areas that are exposing your data to risk

TAKE A FREE RISK ASSESSMENT →