Secura
A BUREAU VERITAS COMPANY

# Ransomware Resilience Assessment

Most organizations are highly dependent on information technology to enable their daily operations and fulfill their mission. A successful ransomware attack can bring those operations to a grinding halt. Sensitive data can also be stolen and leaked in double extortion attacks. Secura's Ransomware Resilience Assessment shows our customers exactly **how vulnerable they are to ransomware attacks and provides an actionable roadmap of how they can improve their ransomware resilience.**

## The Rise and Risk of Ransomware

**In the last decade, ransomware has evolved from a nuisance for individuals to an existential threat for most organizations.** The prevalence of ransomware attacks can be explained by the cybercrime economics, as ransomware attacks result in substantial profit margins without a significant risk of apprehension. As long as the incentives to perform ransomware attacks continue to outweigh the risks for cyber criminals, the **threat of ransomware is expected to increase.**

A ransomware attack can start with an untargeted infection of an individual system with commodity malware. The access to infected systems within the networks of organizations can be sold multiple times in the cybercrime underground by initial access brokers. The value of initial access to networks varies depending on factors such as the privileges that have been obtained and the revenue of the organizations involved.

The level of access can first be expanded and ultimately monetized by encrypting files on all compatible assets in the IT infrastructure of an organization by a ransomware group or affiliate. Many ransomware groups specifically target critical business processes through double extortion, by targeting the availability of mission-critical systems and the confidentiality of sensitive data, to **impose the maximum costs to organizations.**

# How Does a Ransomware Attack Work?

**Ransomware attacks are typically phased progressions towards malicious objectives.** On a strategic level, threat actors will first try to get initial access to networks. Subsequently, they will try to hack through the systems within those networks to increase the impact of an attack. Lastly, they will typically adopt a seek and destroy strategy, by stealing sensitive data, destroying backups and rolling out ransomware.

IN
THROUGH
OUT

## IN

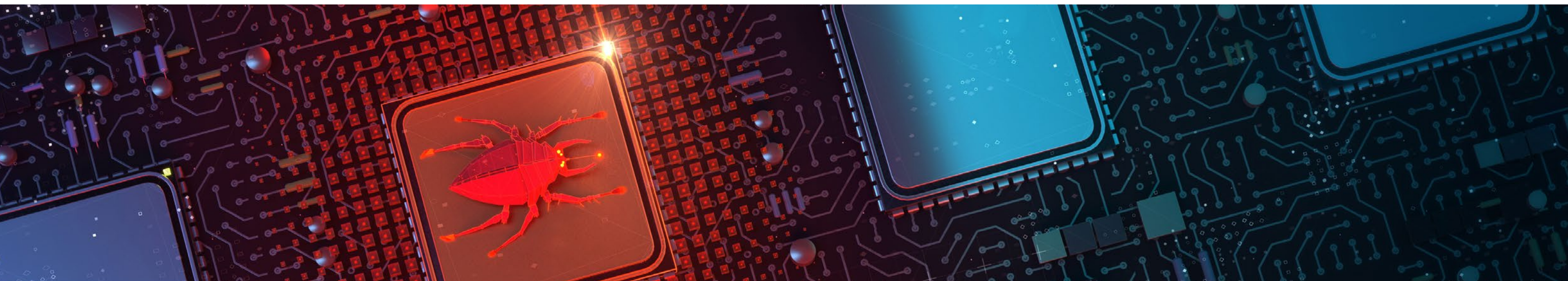
Threat actors will often try to leverage known attack vectors to compromise internet-connected systems indiscriminately with commodity malware, in order to get initial access to networks. A lack of security awareness of employees can allow threat actors to gain initial access to a network through phishing. Exposed authentication mechanisms for remote working services combined with insecure password practices can also be used to get in. Similarly, gaps in the asset management or patch management procedures may lead to the exploitation of vulnerabilities in public-facing applications. These **attack vectors arise from intricate interdependencies between people, processes and technology.** Exposure to any of these attack vectors is a precursor to ransomware attacks.

## THROUGH

Once initial access to a network has been obtained, threat actors can leverage that access to **hack through the systems in a network** in order to increase the impact of a ransomware attack. Insecure IT management practices, system misconfigurations and a variety of vulnerabilities can allow threat actors to escalate their privileges and to move laterally to other systems. The strategic objective of threat actors in this attack phase is to attain the highest privileges in the environment, such as those of a Windows Domain Administrator.

## OUT

Threat actors often abuse the access and privileges that they have obtained to **corrupt or destroy the backups** of the affected organizations. If the option to recover from backups is off the table, an organization is more likely to pay a higher ransom. Threat actors can also **collect and exfiltrate sensitive data** to raise the likelihood and price of a ransomware payout. Once their objectives within the network have been met, **ransomware will be rolled out** to all compatible systems to which the threat actor has obtained access.



# Secura’s Ransomware Resilience Assessment

Secura has developed a **client-centered and risk-based methodology** to assess how vulnerable organizations are to ransomware attacks and to provide actionable advice to raise their cyber resilience. The Ransomware Resilience Assessment consists of a tightly integrated combination of security services that are part of a **holistic approach** that takes people, process and technology into account.

## PEOPLE

Let’s start with the human factor! Employees can be the weakest link in the security of an organization, but they can also act as the first line of defense against ransomware attacks. In the Ransomware Resilience Assessment, the awareness of your employees can be assessed through **a controlled (simulated) phishing attack.**

Based on our extensive experience, we have developed various realistic phishing scenario’s. The phishing simulation provides a measurable and repeatable way to determine how employee (un)awareness is contributing to the overall ransomware resilience of your organization. Through the assessment we also provide guidance to employees how they can recognize and report phishing e-mails in the future.

## PROCESS

To secure an organization, one first needs to understand its business processes. To assess the resilience of your organization against ransomware, Secura’s experts can **ascertain how your business critical processes are entwined with IT and even OT assets** and how they depend on the broader IT environment through threat modeling.

Furthermore, we can perform an **assessment of your cyber security maturity** to provide clear insight into your current maturity scoring. The assessment builds on a **ransomware-specific profile of the NIST Cybersecurity Framework** and covers each of the stages of dealing with an attack: identify, protect, detect, respond and recover. Our security maturity assessment shows the gaps to attain the desired maturity level.

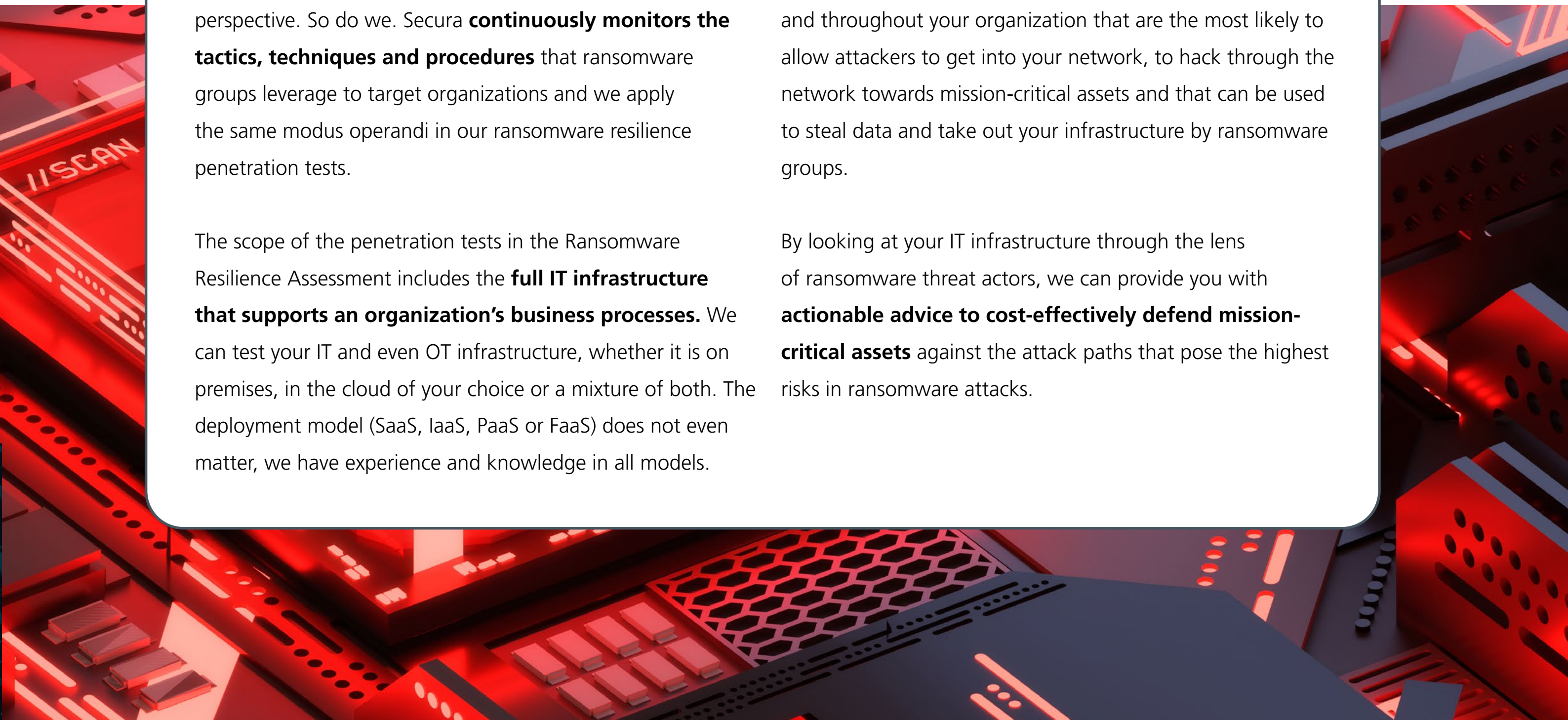
## TECHNOLOGY

Threat actors look at your IT infrastructure from a technical perspective. So do we. Secura **continuously monitors the tactics, techniques and procedures** that ransomware groups leverage to target organizations and we apply the same modus operandi in our ransomware resilience penetration tests.

The scope of the penetration tests in the Ransomware Resilience Assessment includes the **full IT infrastructure that supports an organization’s business processes.** We can test your IT and even OT infrastructure, whether it is on premises, in the cloud of your choice or a mixture of both. The deployment model (SaaS, IaaS, PaaS or FaaS) does not even matter, we have experience and knowledge in all models.

Our penetration tests will **prioritize the attack paths** into and throughout your organization that are the most likely to allow attackers to get into your network, to hack through the network towards mission-critical assets and that can be used to steal data and take out your infrastructure by ransomware groups.

By looking at your IT infrastructure through the lens of ransomware threat actors, we can provide you with **actionable advice to cost-effectively defend mission-critical assets** against the attack paths that pose the highest risks in ransomware attacks.



Secura
A BUREAU VERITAS COMPANY

## Our Related Services

Secura's Ransomware Resilience Assessment is designed to provide a wide variety of customers in various market sectors actionable insight into their resilience against ransomware attacks, but every customer's challenges are unique. Related services that can be relevant to raise your organization's ransomware resilience include:

### TABLETOP RANSOMWARE CRISIS MANAGEMENT

Assessing your ransomware resilience can help to reduce the risks involved with a ransomware attack and to plan accordingly. But few incident response plans survive first contact with an actual ransomware attack. In Secura's Tabletop Ransomware Crisis Management, the operating procedures for handling a ransomware incident are practiced and evaluated through a realistic scenario. Lessons learned provide valuable feedback to improve incident response plans and procedures.

### THREAT MODELING WORKSHOP

Applications and systems are usually part of a chain of information-processing systems. In the highly interactive threat modeling workshop with developers, architects, business owners and other stakeholders, Secura helps to identify possible threats per component and interface. Possible threats include but go beyond ransomware. The workshop raises security awareness and collaboration amongst the stakeholders and can help them to structurally identify risks that may otherwise remain hidden.

### EXTERNAL ATTACK SURFACE ASSESSMENT

Attackers are continuously looking for all kinds of information. From cybercrime gangs to nation state actors, they operate in targeted as well as opportunistic modus, scooping up what they can find and turning that into initial access to their victims' systems and networks. To protect your assets, you need to stay ahead of the game, and proactively assess (and possibly permanently monitor) your external attack surface. What can an attacker discover about your organisation's online exposure?

Secura
A BUREAU VERITAS COMPANY

**Interested?**

Contact us today:

Follow us:

+31 88 888 31 00

info@secura.com

secura.com

BUREAU VERITAS

**Shaping a World of Trust**