

Lansweeper

Vulnerability Security Checklist



VULNERABILITY SECURITY CHECKLIST

As the frequency and severity of cyberattacks continue to escalate, reliable cybersecurity is more important than ever. CrowdStrike, in their 2024 Global Threat Report, observed a 60% year-over-year increase in the number of interactive intrusion campaigns in 2023. The rise of sophisticated ransomware gangs like RansomHub has created a need for more robust cybersecurity measures, as these groups exploit vulnerabilities with alarming speed, causing widespread disruption and financial damage.

Vulnerabilities in your technology infrastructure can provide gateways for malicious activity, putting your entire organization at risk. As the workplace becomes increasingly distributed, with employees working in hybrid environments, vulnerabilities become inevitable, leading to costly downtime and – worse yet – cybercrime.

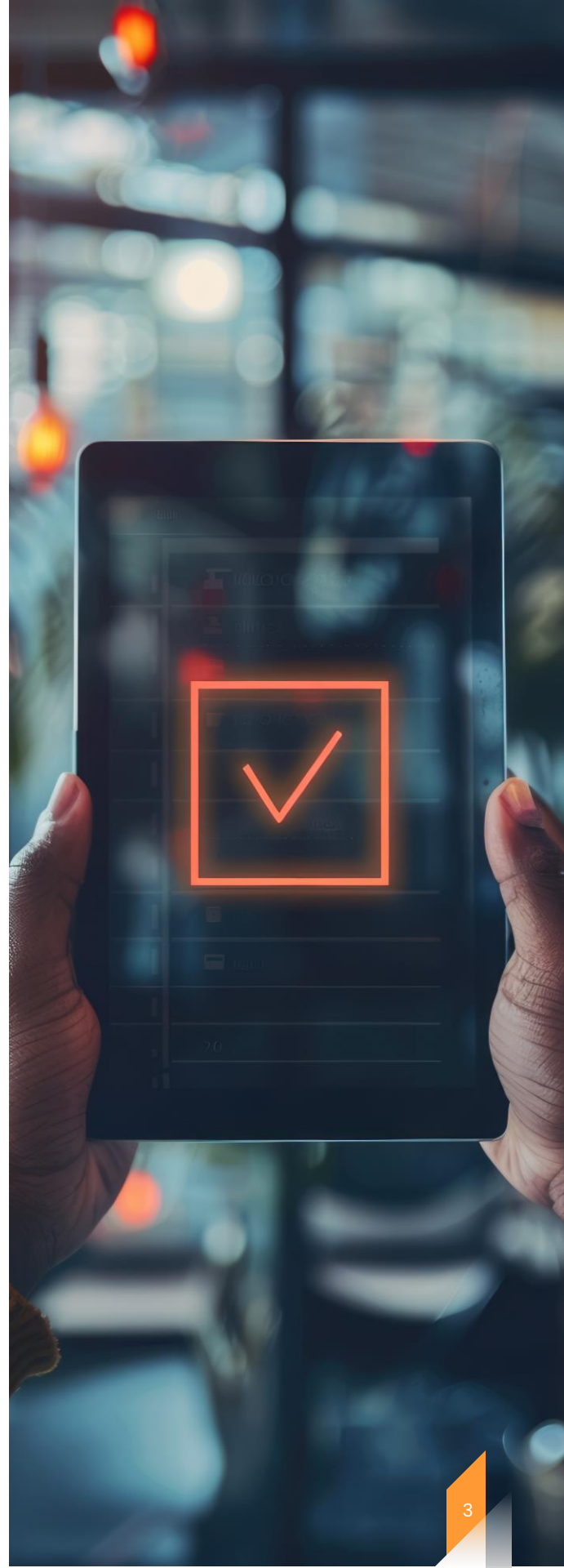




VULNERABILITY SECURITY CHECKLIST


The most common attack vector is **unmanaged network appliances**. Their exposure to both internal and external networks makes them highly vulnerable to exploitation. In 2023, unmanaged edge gateway devices were routinely observed as the primary initial access vector for exploitation. Most organizations struggle to track and monitor every technology asset that connects to their network, especially in hybrid environments and home offices, making it nearly impossible to ensure that all vulnerabilities are addressed.

Another major security risk is **end-of-life products**. Once a product reaches its end-of-life or end-of-support date, it no longer receives any updates or security patches from the manufacturer, making it an easy target for attackers. These unsupported operating systems and legacy gateway appliances provide easy access by effectively leaving the door open for attackers.





CHECKLIST

Use this checklist to ensure you have the right technologies, tools and processes in place to reduce the risk of vulnerabilities in your technology estate and enhance your ability to:

 **Identify** potential vulnerabilities and risks.

 **Prioritize** responding to the vulnerabilities that pose the greatest threat to your IT infrastructure.

 **Mitigate** the impact of potential breaches through proactive security measures and swift response.

 **Track** the status and effectiveness of your mitigation efforts





CHECKLIST



Identify

Do you have a complete inventory of your **physical** technology assets?

Do you have a complete inventory of your **virtual** technology assets?

Do you have a complete inventory of your **software** assets?

Do you have a complete inventory of your **users**?

Do you have **insight into the configuration and status of your IT assets**?

Do you track the **lifecycle** of your hardware and software assets?

Do you collect cyber threat intelligence from one or multiple credible sources (e.g. **threat intelligence, penetration testing, bug bounty programs**)?

Do you actively monitor your network for **potential cybersecurity threats**?

Do you actively monitor and manage **unauthorized personnel, connections, devices, and software**?

Are critical events logged and analyzed?





CHECKLIST



Prioritize

- Are threats **prioritized** based on their **risk level** and **business impact**?

- Do you have tools and processes in place to leverage vulnerability information and determine the **risk** each issue poses to your organization?

- Do you have tools and processes to leverage **vulnerability information** and **analyze your environment's exposure**?

- Do you have tools and processes in place to **report on your IT asset and network data**?

- Do you have insight into **the connections and (inter)dependencies** of your IT assets?

- Do you have adequate **communication channels and information-sharing** practices to facilitate collaboration between coworkers and teams?



Mitigate

- Do you have an overview of user access **permissions and authorizations**?

- Are all users trained in **cybersecurity awareness**?

- Do privileged users understand **their roles and responsibilities**?

- Do you have a strategy to back up **critical data**?

- Do you have a process in place for **upgrading or replacing outdated assets**?

- Do you have a plan, tools, and processes in place to **receive, analyze, and respond to vulnerabilities**?

- Do you have tools and processes to manage and monitor the **vulnerability mitigation process**?



CHECKLIST

Do you have tools and processes in place to **mitigate configuration vulnerabilities**?

Do you have tools and processes in place to **mitigate software vulnerabilities**?

Do you have a **cyber threat recovery** plan to ensure the restoration of systems or assets affected by cybersecurity incidents?



Track

Do you have tools and processes in place to **evaluate the impact of cybersecurity breaches**?

Do you have tools and processes in place to **track the status and impact of your mitigation efforts**?



Is a **retrospective evaluation** included in your **recovery plan** to assess and improve the organization's **cybersecurity posture**?


Do you regularly **report** on your security status and mitigation efforts for **audit and compliance purposes**?

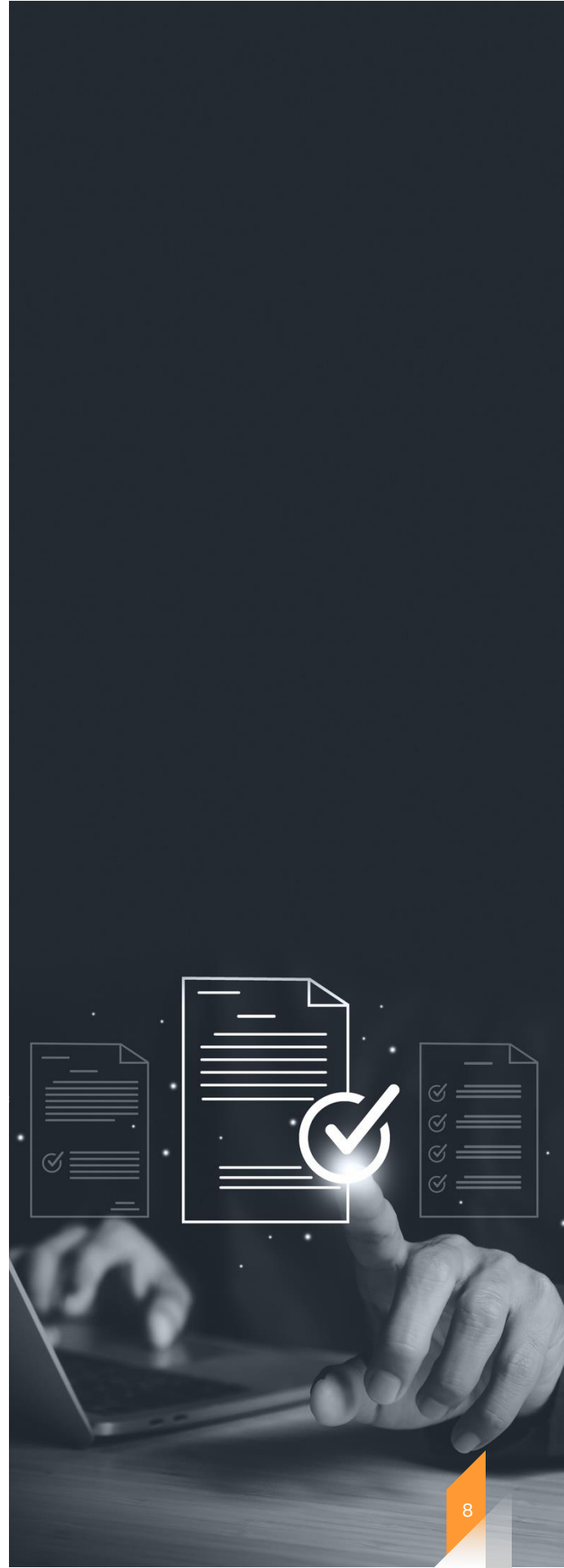


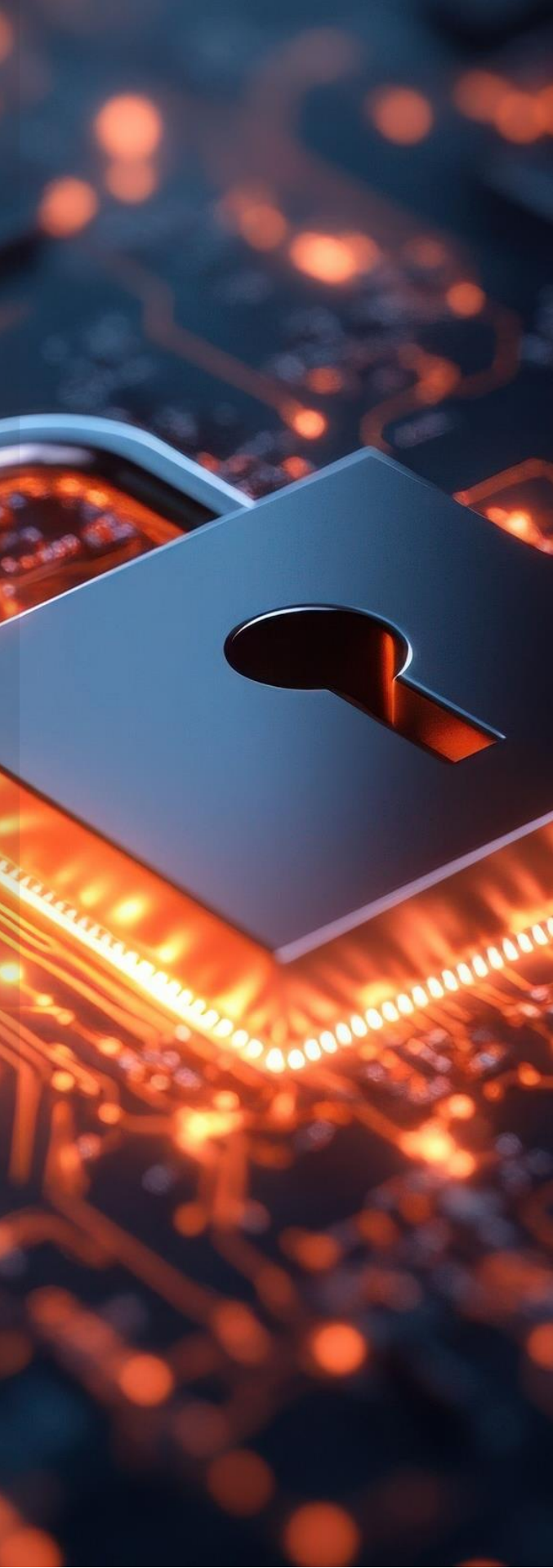
Why Lansweeper

As the industry's leading **technology asset intelligence platform**, Lansweeper automatically and continuously discovers IT assets across your infrastructure - servers, laptops, desktops, virtual machines, operating systems, software, OT, and IoT assets - to create an always-accurate, up-to-date inventory with detailed and granular IT asset data. Lansweeper discovers any device that so much as touches the network, no matter how briefly, picking up on rogue devices, shadow IT, and forgotten, idle devices, identifying them accurately while delivering the data to bring them under control.

Lansweeper's **Risk Insights**  feature provides you with a list of all at-risk devices in your network and the vulnerabilities threatening them, as well as additional information like severity and patch availability. You can also find **lifecycle information**  for your software, firmware, and operating systems. Identify where vulnerabilities exist in your IT environment and deploy appropriate patches and updates to mitigate risk.

Thanks to detailed **network diagrams**  you can easily assess how a vulnerable device could affect other parts of your network. Lansweeper can also shed light on configuration vulnerabilities by scanning registry keys, AD properties, user privileges, and certificates, and provides detailed information about installed software, including version, installation data, and software history.





▲ Why Lansweeper

Organizations have leveraged Lansweeper data to combat significant vulnerabilities, in leading technologies and software such as Google Chrome, several Linux distributions, Veeam, vCenter Server, and Apple products, avoiding substantial downtime and financial losses.

Lansweeper also regularly releases **vulnerability** and **end-of-life reports** so users can easily check whether their technology assets are running on the latest security patches and updates as well as a monthly **Patch Tuesday Report**

We also provide access to a report builder to create more so you can always easily retrieve the asset data you need and access to more than **400 built-in network reports**

Lansweeper

Lansweeper is an IT asset management software provider that helps businesses better understand, manage, and protect their IT assets and network. Lansweeper helps customers minimize risks and optimize their IT assets by providing actionable insight into their IT infrastructure at all times, offering trustworthy, valuable, and accurate insights about the state of users, devices, and software. Since its launch in 2004, Lansweeper has been developing a solution that scans and inventories all types of IT devices, installed software, and active users on a network - allowing organizations to centrally manage their IT.

The Lansweeper platform currently discovers and monitors over 80 million connected devices from 28,000+ customers, including Mercedes, FC Barcelona, Michelin, Carlsberg, Nestle, IBM, and Samsung to governments, banks, NGOs, and universities, driven by its 320+ strong teams in Belgium, Spain, Italy, the UK and the USA.



Want to try Lansweeper now?

[Start Your Free 14-day Trial](#) 



Not ready yet?

[Watch the demo video](#) 