TuxCare
We Take Care of Linux

WHITEPAPER

# Gartner CARTA Operational Risk Model

www.tuxcare.com

Gartner's Continuous Adaptive Risks and Trust Assessment (CARTA) is an operational risk prioritization strategy that recommends continuous assessment of adaptive security controls.

The ability to establish continuous visibility into risk and prioritization of remediation while evaluating adaptive security capabilities is critical for an organization to protect its assets against the constantly changing threat landscape.

TuxCare's automation for live patching Linux OS, open source databases, and critical libraries provides security updates for current and advanced threats. Not only does TuxCare's live patching technology enable organizations to quickly deploy the latest vulnerability patches without needing to reboot, but it also supports the risk reduction strategy defined by the CARTA model – making it a valuable tool for companies who've adopted the CARTA approach.

# Prioritization of Vulnerabilities

The truth of running a digital business means that companies must be innovative, or they will fail. This extends into the protection of data – both their own and the data belonging to their users.

Security is particularly crucial in a digital business environment that involves technology, like public clouds, mobility, cloud-hosted applications and infrastructures, and blockchains. Insider threats, breakdowns in the level of trust, and outdated security policies continue to affect organizations, as they have since well before new-generation technologies had been introduced.

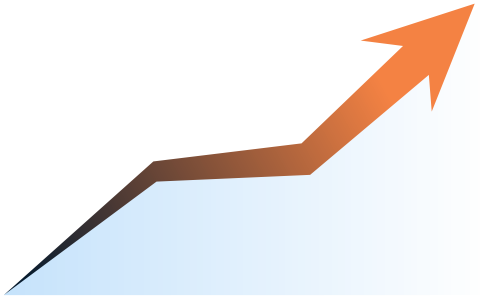
Security experts need to adapt their cybersecurity techniques for the new digital business era, including within Web 3.0 and blockchain technologies, to include establishing higher prioritization of remediating vulnerabilities to reduce the most impactful risk to the organization. This is especially true in the age of digital transformation, as each new transformation strategy brings a new level of risk to the organization.

Security vulnerabilities exist in every layer of business transformation. The cloud, mobile technology, and the internet of things (IoT) are often pieces of the digital transformation journey and make static approaches to enterprise cybersecurity completely irrelevant.

A dynamic and continual approach is required to handle the new attack surface facing additional risk with each rendition of a digital transformation strategy.

# Why CARTA?

As 68% of business leaders believe that cyberattacks threaten their organizations, they're not taking any chances. In fact, they're doubling down on security measures, investing in new technologies, and hiring top talent to keep them safe.



**According to Gartner, breach incidents have increased by**

**67%**

**between 2014 and 2022**

According to Gartner, breach incidents have increased by 67% between 2014 and 2022. Hackers target businesses across industries, including healthcare, retail, manufacturing, financial services, technology, energy, transportation, hospitality, and government. To stay ahead of the curve, companies must invest in continuous monitoring and automation to detect threats before they cause damage.

With the rise of cybercrime, businesses and governments alike have realized they must adapt to new threats and take advantage of new technologies to stay ahead of criminals. To do so, they've turned to the cloud, mobile devices, extensive analytics, and machine learning to help them identify and respond quickly to emerging threats. These solutions can help companies protect themselves against today's sophisticated attacks and prepare for tomorrow's threats.

Leveraging the CARTA approach helps IT security teams develop more of a consolidation of responsibility instead of a siloed support model to help manage the additional risks that arise from transformation strategies.

### Audit and Compliance Challenges

With the CARTA framework, organizations must continually assess their business partners, supply chain, and logistics risk posture and adjust accordingly. For ecosystems with a dominating partner, the only path into the ecosystem is through a security and compliance audit. If they deem your organization too risky, the partnership may be terminated. Continuous monitoring and assessment of crucial digital partners are critical.

In addition, the PCAOB has recently changed its audits' requirements to include assessing whether the auditor had access to sufficient information to perform the required tests.

# Understanding the Run, Build, and Plan Phases for CARTA

### Run

Concerning CARTA, companies must run traditional business intelligence (BI) tools and machine learning techniques.

On average, it takes 99 days for an enterprise to detect a security incident. Running automated analytics and automated responses enable enterprises to focus their limited security staff on happenings with the most significant potential impact.

### Build

To ensure that your application is secure, perform penetration testing on your software during each release and build cycle. You can do this manually or automate the entire test through an automated tool, such as AppScan. Penetration tests help identify vulnerabilities in your application so you can fix them before releasing new features or patches.

Organizations should build security into every aspect of application design and development. Developers must understand how to make secure software and ensure it can withstand attacks. They must also know how to test and validate the security of an application. In addition, they must understand how to integrate security controls into the overall architecture of an application. Finally, they must manage the security of an application.

### Planning

As part of the CARTA approach, organizations should also evaluate vendors' ability to provide secure and open APIs, support next-generation technologies (including cloud applications), support platforms (including containers), and support adaptive control policies.

### Adjusting to Content-Aware Security Controls

An essential component of the CARTA approach is to assist clients in moving away from a one-sided security decision based on single events. Many clients adjust their security posture based on a single event and often only make infrequent changes – unless a cybersecurity event has been discovered.

CARTA's continuous assessment risk model helps clients change their security posture based on various cybersecurity conditional changes, including a mixture of access control failures, location-based attacks, or specific attacks against individuals within the organization. By continuously assessing the enterprise landscape, organizations can make minor adjustments across several adaptive controls based on the outcome of the assessments recommended by the CARTA model.

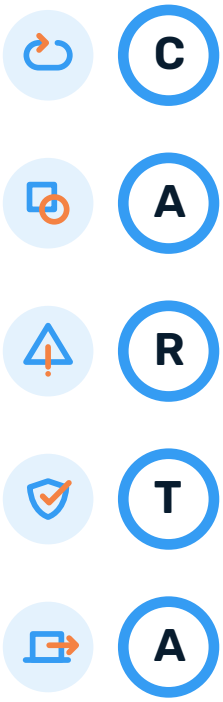
## How the TuxCare Live Patching Approach Supports the CARTA Model

The CARTA strategic approach stipulates that effective risk and cybersecurity management requires:

- 100% device visibility
- Continuous monitoring
- Micro-segmentation
- Evaluating products from multiple vendors
- Additional levels of SOAR
- Remediation of physical and virtual devices, cloud infrastructures, and workloads
- Effective security management of agentless IoT devices and cyber-physical OT systems

TuxCare's live patching technology, which enables organizations to automatically deploy the latest Linux vulnerability patches without rebooting or scheduling downtime, helps organizations adhere to the principles CARTA approach – as seen below.

# TuxCare Alignment to Gartner CARTA Model



**Continuous**
Automation of security updates to Linux, IoT, IIoT, and OT devices without the need to reboot.

**Adaptive**
TuxCare's global expertise in providing security patches and extended updates helps protect our client's critical hosts, libraries, and open-source databases.

**Risk**
TuxCare's live patching along with extended software updates for Python and PHP help lower the risk of cyber breaches against critical hosts and devices.

**Trust**
TuxCare has patched more than 80,000 vulnerabilities without reboots over the years. We assist clients in maintaining their compliance requeriments and regulatory mandates.

**Accessible**
TuxCare is approaching 1 million  production workloads secured and supported by our services

# Why TuxCare?

TuxCare is a global leader in open-source security, providing unmatched expertise in patching for your entire Linux estate. We deliver security patches to popular Linux distributions, end-of-life systems, programming languages, and more – offering a comprehensive security solution for all your infrastructure needs.

With over 80,000 patches – and counting – delivered to our users, TuxCare's solutions reduce vulnerability exposure, minimize downtime, eliminate patching-related disruptions, secure your open-source supply chain, and maintain system stability and compliance.

TuxCare protects the world's largest enterprises, government agencies, service providers, universities, and research institutions, safeguarding over a million workloads (and growing). Our mission is to drive continuous innovation through open-source technologies while minimizing the risk of cyber threats and serving as a trusted technology partner for innovative organizations across the globe.

LEARN MORE AT
**www.tuxcare.com**