kaspersky

Paris Call for Trust and Security in Cyberspace

Kaspersky's proposal to enhance the Paris Call cooperation

July 2019

www.kaspersky.com

#truecybersecurity

Proven.
Transparent.
Independent.

Paris Call for Trust and Security in Cyberspace

We fully support President Emmanuel Macron's Paris Call for Trust and Security in Cyberspace, since we firmly believe that, as digital technologies make our life better, cybersecurity should complement the digitalization of society to ensure the safety and security of its citizens.

In response to the Call, which encourages collaboration between public authorities, the private sector and civil society to strengthen cyber-protection, and as an early supporter and signatory, Kaspersky would like to present its thoughts regarding combining efforts for the implementation of the ideas and values that the Call promotes.

"Verifiable Trust" Paradigm

The importance of trust in cybersecurity

We believe that trust is the foundation of all positive human relations and the key to our security and wellbeing. But for cybersecurity trust is even more important: it doesn't merely require trust – it depends on it. Digital trust is defined as the combination of cybersecurity, effective data protection, accountability and traceability, and ethical treatment, inspiring customers' trust in a company – or citizens' trust in a public actor.

It is generally thought that international norms and rules can help reach the desired level of trust in cybersecurity among actors in international relations, bring cyber-stability, make the world less chaotic, and minimize the risk of conflict. While we support the further active development of such 'cyber norms', we understand that it requires much effort and time and a strong will of states to create enforcement measures to ensure that such norms are followed. At the same time, such norms can be followed by states only, while non-state actors remain in a legal 'grey area' without a direct obligation to meet certain norms of behavior.

While diplomatic efforts continue at international forums, we, as a representative of the private sector, would like to propose a practical solution: a solution to help achieve both the desired level of trust among actors and cyber-resilience from modern cyberthreats.

Generally, trust in a company is based largely on its reputation, on the long-term relationship built with its audiences. The decision to trust or not relies on the personal opinion of each individual, based for instance on past experience, culture and values. Trust in a company or particular product may therefore be based on a number of factors, where fear of potential risks might prevail over a more evidence-based approach.

In the strategic field of digital technology, should we not think about a new approach that is more evidence-based than impression-based? In this perspective, **we propose to shift to a paradigm of 'verifiable trust'**. The main way to do this is through the development of a new framework and mindset – digital trust and digital ethics – which provide clear and practical verification measures to assess risk.

Defining together the conditions of trust

The Paris Call represents an opportunity to bring together industry experts, academia, the public sector and civil society to work together to develop a shared comprehensive framework to assess the trustworthiness of IT products.

Such a framework would address IT supply chain risks to the benefit of all stakeholders: businesses, civil society, governments and citizens by helping assess what is an appropriate level of risk within the risk-based approach paradigm.

Kaspersky is ready to provide its infrastructure and systems, including its source code for evaluations needed to make the framework work (see next page).

Two primary factors would be the focus:

- **Product integrity assessments:** Do IT products contain any unintended functionalities?
- **Data collection and processing assessments:** How IT products collect, process, store, and protect user data?

We also support the following ideas:

- **To establish a consultation platform through physical meetings** to collect ideas and create collaboration streamlining between signatories. Such streamlining might focus on discussion of our (i) trustworthiness framework, (ii) cyber-norms and (iii) cyber-hygiene and education.
- **To establish a consultation mechanism through physical meetings for developing the standardization approach** and framework for cybersecurity products.
- **To prepare a high-level publication** with a more detailed analysis of possible steps to promote the values and achieve the goals the Call states.

The legitimacy of the framework and its acceptability, but also interplay and knowledge sharing, will be key issues for the success of such initiatives. Kaspersky is ready to engage in this effort with its partners.

Kaspersky Global Transparency Initiative:

A unique approach of independence and transparency for digital trust

Transparency, privacy and data security are especially important for our users, partners and the international cyber security community as a whole. This is why Kaspersky has developed a unique approach – the Global Transparency Initiative (GTI) – to strengthen the resilience of its IT infrastructure against any risk, even theoretical, that could undermine trust.

Under the GTI, the core of our **European users' data storage and processing infrastructure was transferred to Switzerland** in 2018. This effort will continue in the coming months for users in other regions of the world. The **opening of Transparency centers** in Switzerland and Spain also allows our partners to audit our products in a secure environment.

In addition, an independent trusted third party will audit our data storage and processing processes, our employees' access to data and software compilations, and our source code.

The "Bug bounty" program, which rewards the discovery of vulnerabilities in Kaspersky products, was also increased. Awards can now reach $100,000 to further encourage independent security researchers to complement our efforts to detect and mitigate vulnerabilities.

Key measures:

- Relocation of data processing and data storage to Switzerland
- Opening of Transparency centers in Zurich and Madrid for reviews of Kaspersky Lab source code and updates
- Audit of the Kaspersky's software development by independent one of the 'Big Four' third party
- Increasing Bug bounty awards

The GTI provides organizations with concrete tools to ensure that Kaspersky solutions meet and even exceed enterprise data security, protection and management policies. This is a long-term effort, because trust is never fully acquired: it must be constantly renewed.

We are convinced that the GTI as a positive trust-building measure might become a blueprint for the industry, and would contribute to building trust in the digital age.

GTI: the four pillars of trust

1 / Data care

- Relocation of data processing and data storage to Switzerland – a country globally known for its neutral status and strictest data protection regulation;
- Building data privacy cloud networks for heightened privacy (Kaspersky Private Security Network).

2 / Verification

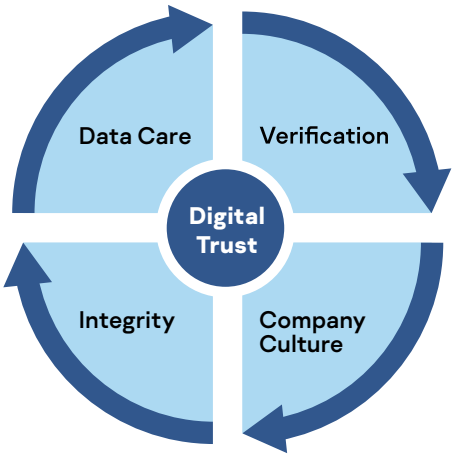
- Setting up dedicated Transparency Centers for reviews of Kaspersky source code, software updates, and threat detection rules;
- Vulnerabilities management via the Kaspersky's Bug Bounty Program;
- Maximum performance and efficiency based on the results of more than 70 tests;
- Independent Client Evaluation – Gartner Peer Insight.

3 / Integrity

- Integrity and security audit of Kaspersky software development through the independent audit by one of the 'Big Four' companies, to will confirm that Kaspersky has in place strong security controls for the development and release of its antivirus databases;
- A trustworthiness framework as a collaborative project with third parties.

4/ Company culture

- Independence: Kaspersky is a private company with more than 20 years of experience on the global market;
- The company's DNA: continuous development of new technologies;
- Research: Its Global Research and Analysis Team (GReAT) and one third of employees are R&D specialists;
- Knowledge sharing: the Security Analysts Summit, a flagship global conference for cybersecurity experts.



kaspersky

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly being transformed into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters to them most.

Learn more:

www.kaspersky.com

www.kaspersky.com/transparency-center

https://www.kaspersky.com/transparency-center-offices