SECURITY FIRST CHARTER

October 1, 2020

SECURITY FIRST

Reprivata's "Security First" guiding principle applies to **everything.**

In an interview on February 25, 2020, Katie Arrington, US Department of Defense Chief Information Security Officer made a statement that ***"everything today is digital"*** and she gave example after example that supported her statement.

At Reprivata, we have committed to making Security the first priority in everything; everything we think, everything we say, everything we do, everyone we partner with and everyone we serve.

That's why, we created the Reprivata Community of Trust® Platform.

COMMUNITY OF TRUST™

As witnessed with the WHO, CDC, Gates Foundation, NIH breach reported on April 21, 2020 and according to the Harvard Business Review's 2019 book on Cybersecurity…

"Cyber-attacks and data breaches are commonplace, increasing in volume, and becoming costlier by the year. We need to revise our expectations about our ability to mitigate these risks and accept that breaches are all but inevitable. If your mission critical systems are digital and connected, they can never be made fully safe."

We disagree with this HBR statement. In fact, we have proven that a "Security First" position is possible. For over 4 years, Reprivata's Community of Trust has provided Nation State-level cybersecurity to organizations - including continuous real-time monitoring of activities inside and outside of the private network - **to** change the mind-set and behavior of end users.

Also, in an iSMG interview on February 28, 2019, Retired General Keith Alexander (Director, National Security Agency; Chief of Central Security Service; Commander, US Cyber Command) speaking about the Nation-State threat says, "Most people think about Cybersecurity as I get a Firewall, SIEM, Endpoint security etc. The reality is if you don't have a comprehensive solution and you can't deal with Nation State like capabilities, then we will always be left with Incident Response and that is After-the-Fact. What we need is a ***New Framework***. We need a network to defend a network."

Watch General Alexander's full interview… https://www.inforisktoday.co.uk/ret-gen-keith-alexander-on-nation-state-threat-a-10885.

REPRIVATA IS THE NEW FRAMEWORK

Reprivata's patented Community of Trust™ (CoT™) platform is reprivatizing data networks, communications and digital identities through 5 integrated solutions:

1. Community of Trust™ Network – Reprivatizing data networks, communications and digital identities
    a. Reprivata's Community of Trust™ Network blocks/cloaks IP visibility – no public IP address, no "call home," no public DNS and no forced reliance on public Certificate Authority.
    b. This multi-layered encryption solution uses NSA's Commercial Solutions for Classified Software configured to sufficiently protect classified data while in transit
    c. Secure communications and Micro-Segmentation software certified by multiple independent third parties
    d. Rigid adherence to multiple standards including NIST Cyber Security Framework and CMMC
    e. Accessible via an application on any device
    f. Implementable as an image – highly scalable and affordable

2. Global Threat Intelligence – Real-time cyber threat identification and mitigation
    a. Enhances traditional perimeter security by adding a cyber version of RADAR, in true real-time, to detect and interdict incoming threats early in the cyber kill chain as they reach the perimeter but before they penetrate defenses.
    b. Scalable, Distributable Threat Detection and Information Sharing System
    c. Real-time SOC Active Defense
    d. Real-time monitoring of third-party risk and information sharing

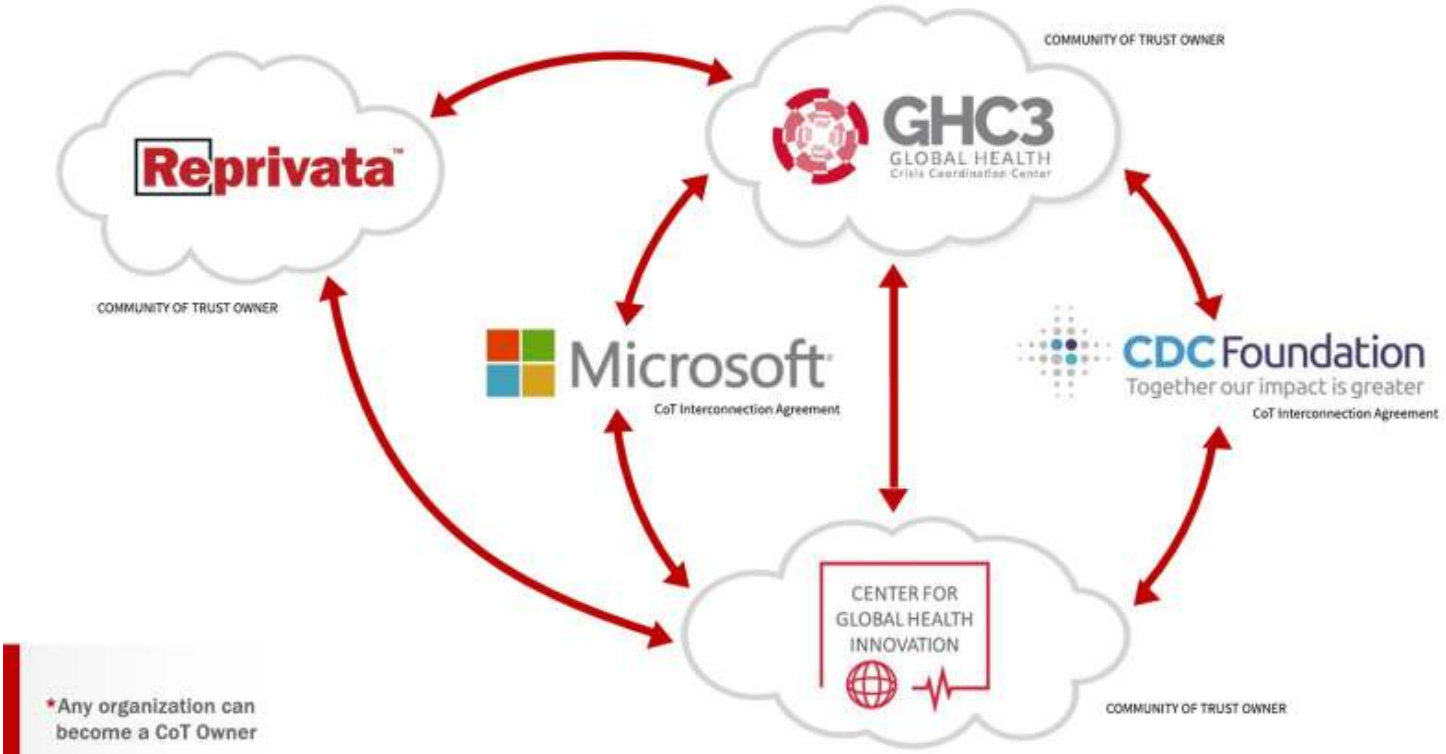
3. CoT™ Legal Framework – Integrates interconnection, data protection and information sharing agreements
    a. Provides a step-by-step plan that is designed to strengthen appropriate cybersecurity controls and achieve a higher maturity level over time for not only the Enterprise, but also its third parties.
    b. Cyber-focused uniform legal agreements (Master Agreements)
    c. Standardized Master Agreements – Cyber Interconnection Security, Privacy Data Protection, and Information Sharing Agreements
    d. Agreements encoded in a format that is both human and machine readable
    e. Contract Management System that scales globally to create, issue, log, administer, protect and defend (especially in judicial proceedings) every Agreement between Community of Trust™ Service Providers and their members including Employees, I3Ps (Independent Third Party's) and Devices (IoT, IIoT, Edge, BYOD)

4. **CoT™ Privacy Authority** – Collects, monitors and logs all data inside the CoT
    a. Reprivata's CoT™ Privacy Authority addresses all privacy regulations worldwide including GDPR and CCPA.
    b. Flexible CoT™ framework intended to span a variety of functions necessary to monitor and protect the Community of Trust Network, its members, and their private and personal data
    c. Log ingestion and analysis engine responsible for monitoring the system logs of all of the various subsystems; the operating system, the encrypted tunnel, the VoIP and XMPP switches, the file-sharing, and email services etc.
    d. Gives individuals a way to legally own their own digital identity

5. **Security First Academy** – Arms employees and contractors with the tools to protect the organization through Cybersecurity Education, Awareness and Phishing Simulation
    a. Reprivata's Learning Management System is designed to help organizations, their employees and partners learn about cyber risks, uncover existing security vulnerabilities and be ready to take action following the "Security to the 6th Power™" methodology
    b. Security to the 6th Power™
        1. Educate
        2. Calculate
        3. Assess
        4. Score
        5. Plan
        6. Secure

HOW A COMMUNITY OF TRUST™ WORKS

Real-World CoT initiated for GHC3



*Any organization can become a CoT Owner

HOW TO BECOME A MEMBER OF THE COMMUNITY OF TRUST™

CRAWL - INDIVIDUAL ACCESS | END-USER LICENSE AGREEMENT

The individual access option will allow you to provide access to any end users (employee, contractor, IoT device, IIoT device) with appropriate authorization. This would entail a setup of the user's device with the appropriate certifications to enter into your Community of Trust. No network auditing is required, but it requires a process to set up each individual.

WALK - EXISTING NETWORK INTERCONNECTION | INTERCONNECTION AGREEMENT

The Partner's Network will be set up to have all, or portions, of the network accessible much like an individual end-user. This effort would require an Interconnection Agreement between your Organization and the Partner Organization that defines the security standards required. Once the agreement has been accepted and signed, a networking engineer will provide assistance to seamlessly connect the two networks - effectively joining the Partner Network into your CoT™ (Community of Trust™).

RUN – PARTNER ORGANIZATION BECOMES A COMMUNITY OF TRUST™ OWNER

Reprivata can create a Community of Trust™ (CoT™) within Partner Organization's Network. Not only does this ensure the Partner organization's security, but it enforces security standards needed by other CoTs™. This leads the way for the Partner organization to become a CoT™ Owner and Service Provider that can operate independently and/or interconnected to another Community of Trust™ Owner which creates a completely private and secure interconnected network with your organization and provides access to all appropriate users.

KEY BENEFITS OF A COMMUNITY OF TRUST™

Not only does a CoT™ provide security, it provides a means of securely collaborating with other trusted third parties, provides transparency into network activity, and follows all international regulatory requirements.

Full benefits of setting up a Community of Trust™ are listed below within our Security First Deliverables.

COMMUNITY OF TRUST™

SECURITY FIRST DELIVERABLES

1. **Ownership for Cyber and IT security**
   Anchor the responsibility for cybersecurity at the highest governmental and business levels by leveraging specific ministries and CISOs as stakeholders. Establish clear measures and targets as well as the right mindset throughout organizations – "It is everyone's task."

2. **Responsibility Throughout the Digital Supply Chain**
   Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards, such as:

   - Identity and access management: Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.
   - Encryption: Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate.
   - Continuous protection: Companies must offer updates, upgrades, and patches throughout a reasonable lifecycle for their products, systems, and services via a secure update mechanism.

3. **Security by Default**
   Adopt the highest appropriate level of security and data protection and ensure that it is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures, and business models.

4. **User-Centricity**
   Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems, and services as well as guidance based on the customer's cybersecurity needs, impacts, and risks.

5. **Innovation and Co-Creation**
   Combine domain know-how and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage i.e. contractual Public Private Partnerships.

6. **Education**
   Include dedicated cybersecurity courses, curricula – as degree courses in universities, professional education, and training – in order to lead the transformation of skills and job profiles needed for the future.

7. **Certification for Critical Infrastructure and Solutions**
   Companies – and if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions.

8. **Transparency and Response**
   Participate in a highly trusted information sharing community to share new insights on cyber threat activity in support of the nation's critical infrastructure providers.

9. **Regulatory Framework**
   Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs).

10. **Joint Initiatives**
    Drive joint initiatives including all relevant stakeholders in order to implement the above principles in the various parts of the digital world without undue delay.

NEXT STEPS

Select one of the options listed below and provide all necessary signed agreements. A Reprivata representative will then assist your organization in getting the Community of Trust™ infrastructure setup between parties.

INDIVIDUAL ACCESS | END-USER LICENSE AGREEMENT

EXISTING NETWORK INTERCONNECTION | INTERCONNECTION AGREEMENT

PARTNER ORGANIZATION BECOMES A COMMUNITY OF TRUST™ OWNER