Autonomous Digital Defense
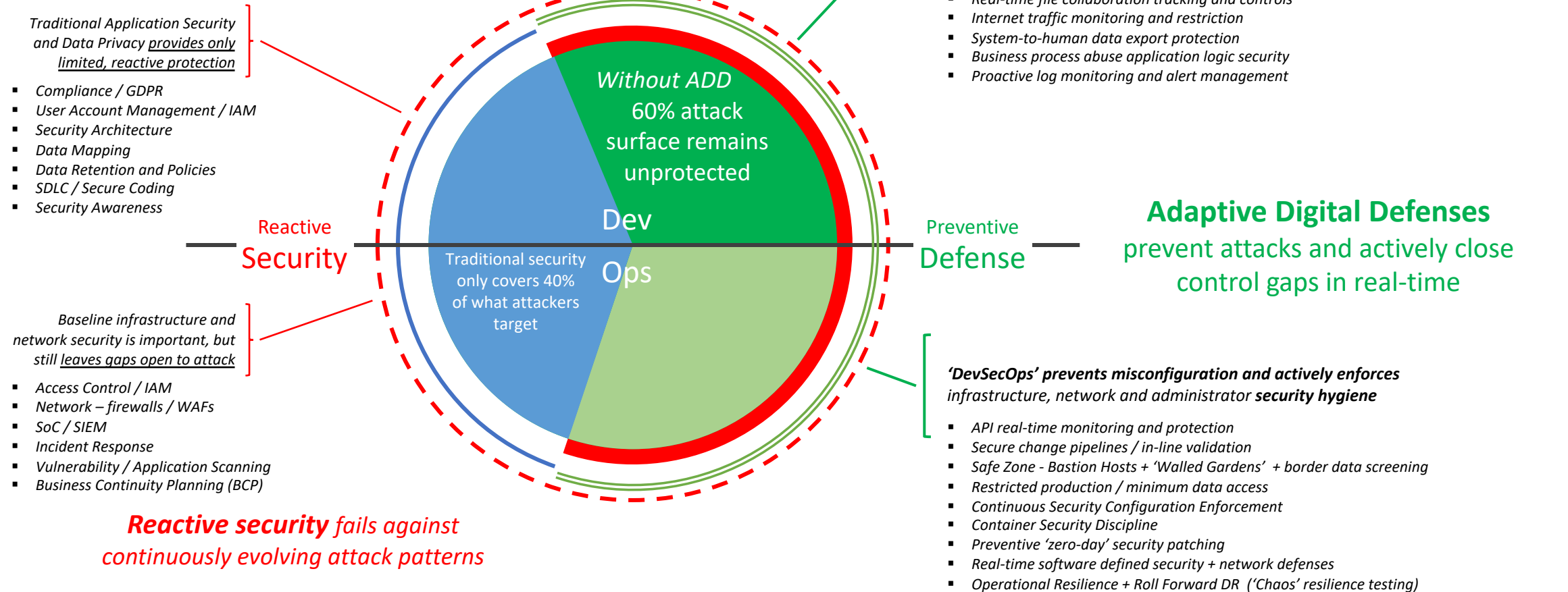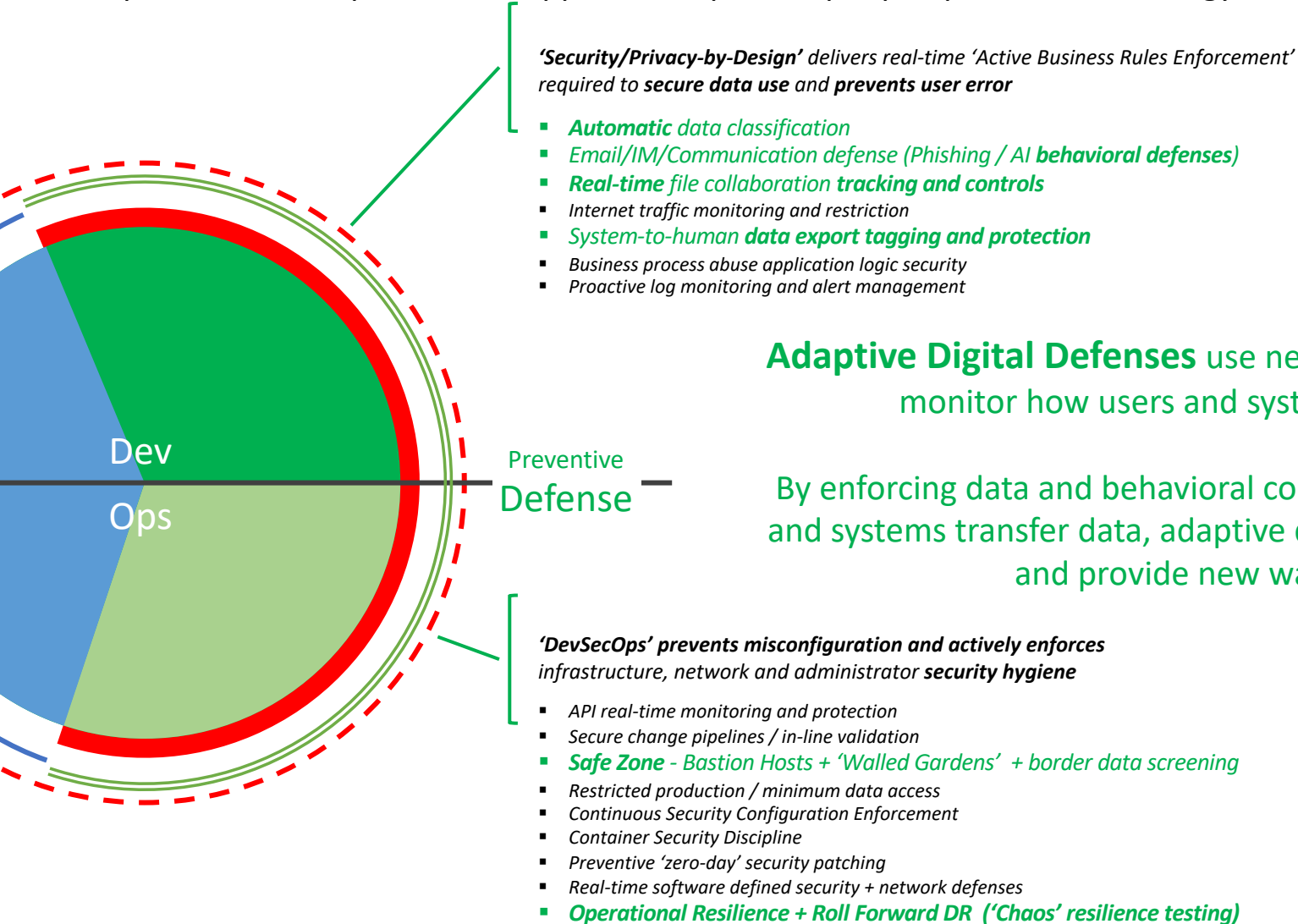
RFC – Opensource ideas for community feedback

Adaptive Digital Defenses

Adaptive Digital Defense (ADD) new approach
to security + privacy + resilience protection

'Security/Privacy-by-Design' delivers real-time 'Active Business Rules Enforcement'
required to **secure data use and prevents user error**

- Automatic data classification
- Email/IM/Communication defense (Phishing / AI behavioral defenses)
- Real-time file collaboration tracking and controls
- Internet traffic monitoring and restriction
- System-to-human data export protection
- Business process abuse application logic security
- Proactive log monitoring and alert management

*Traditional Application Security
and Data Privacy provides only
limited, reactive protection*

- Compliance / GDPR
- User Account Management / IAM
- Security Architecture
- Data Mapping
- Data Retention and Policies
- SDLC / Secure Coding
- Security Awareness

*Without ADD
60% attack
surface remains
unprotected*

Dev

Traditional security
only covers 40%
of what attackers
target

Ops

Reactive
Security

Preventive
Defense

Adaptive Digital Defenses
prevent attacks and actively close
control gaps in real-time

*Baseline infrastructure and
network security is important, but
still leaves gaps open to attack*

- Access Control / IAM
- Network – firewalls / WAFs
- SoC / SIEM
- Incident Response
- Vulnerability / Application Scanning
- Business Continuity Planning (BCP)

'DevSecOps' prevents misconfiguration and actively enforces
infrastructure, network and administrator **security hygiene**

- API real-time monitoring and protection
- Secure change pipelines / in-line validation
- Safe Zone - Bastion Hosts + 'Walled Gardens' + border data screening
- Restricted production / minimum data access
- Continuous Security Configuration Enforcement
- Container Security Discipline
- Preventive 'zero-day' security patching
- Real-time software defined security + network defenses
- Operational Resilience + Roll Forward DR ('Chaos' resilience testing)

***Reactive security** fails against
continuously evolving attack patterns*

Adaptive Digital Defenses

New places + techniques + tools approach to protect people, process, technology and data

'Security/Privacy-by-Design' *delivers real-time 'Active Business Rules Enforcement'
required to* **secure data use** *and* **prevents user error**

- *Automatic data classification*
- *Email/IM/Communication defense (Phishing / AI **behavioral defenses**)*
- ***Real-time** file collaboration **tracking and controls***
- *Internet traffic monitoring and restriction*
- *System-to-human **data export tagging and protection***
- *Business process abuse application logic security*
- *Proactive log monitoring and alert management*

Dev

Ops

Preventive
Defense

Adaptive Digital Defenses use new advanced and adapted change control to track and monitor how users and system use and move data around the network.

By enforcing data and behavioral control checks in the path where users use information and systems transfer data, adaptive digital defenses make existing controls more effective and provide new ways to protect the digital experience.

'DevSecOps' *prevents misconfiguration and actively enforces
infrastructure, network and administrator* **security hygiene**

- *API real-time monitoring and protection*
- *Secure change pipelines / in-line validation*
- ***Safe Zone** - Bastion Hosts + 'Walled Gardens' + border data screening*
- *Restricted production / minimum data access*
- *Continuous Security Configuration Enforcement*
- *Container Security Discipline*
- *Preventive 'zero-day' security patching*
- *Real-time software defined security + network defenses*
- ***Operational Resilience + Roll Forward DR ('Chaos' resilience testing)***

Document License

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

This is a human-readable summary of (and not a substitute for) the license. Disclaimer.

You are free to:

Share — copy and redistribute the material in any medium or format
Adapt — remix, transform, and build upon the material
for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.
No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Notices:

You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation.
No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material.
No warranties regarding the work under this license is provided, any materials licensed under these terms and conditions, or any related information to this work. The licensor disclaims all liability for damages resulting from the use of this work to the fullest extent possible.

We'd love to hear from you (ADD-cc@daveinthecity.uk).