

Enterprises are investing in a patchwork of security technologies that don't interoperate and don't provide a holistic view into their security posture. Security practitioners know this perpetuates a fractured landscape that becomes more difficult and expensive to manage over time. What they don't realize is they can now choose data-centric security that extends with data as it travels across silos.

In our recent webcast **Five Steps To A Zero Trust Security Strategy**, we were joined by guest speaker **Stephanie Balaouras, Vice President, Research Director for Security & Risk at Forrester Research**. She provided the following insights to address audience queries.


What do you see as some of the biggest challenges in today's siloed security industry?

Balaouras: The challenges are three-fold. 1) With silos and various point products, companies wrangle with multiple policy consoles. This management sprawl is a burden on administrators who must manage these tools, increasing the likelihood for inconsistent policies across tools. 2) The amalgamation of security technologies within an organization don't necessarily play nice together, and integration and usability challenges hinder the use and optimization of tools. They may also wrestle with multiple analytics sources as a result. 3) Companies are likely to operate in a fractured landscape where they require protection across structured and unstructured data, as well as on-premise and cloud-based applications and data stores. Many technology offerings tend to specialize, and companies find themselves struggling to decide on the tradeoffs between best of breed vs best of suite.

Valuable personal data can often start in a structured database, like an application, migrate to an unstructured report exported from the application, backed up to a cloud storage location, and even find its way back to a structured database again.

In the context of a Zero Trust model, can you share your thoughts on how companies might take a forward-looking approach that would enable control, even as the data crosses multiple boundaries of trust?

Balaouras: Data security is one of the key pillars of a Zero Trust strategy – if not the key pillar. Before an organization works through identifying the appropriate technology controls, it needs to have an understanding of what is personal data, why it has this information, and what constitutes appropriate business use of this data. In a perimeterless world, a Zero Trust approach to data security requires visibility into the interaction between users, apps, and data; continuously assessing (and never assuming) "trust" through a risk-based analysis of available information and context about users, actions, and data; the ability to set and enforce policies regardless of whether the user is connected to the corporate network. This data-centric approach helps to ensure the data and its controls are travelling together. When we think of data-centric technology approaches to support this, we can map controls to the data's lifecycle. This could then include data flow mapping, data masking, encrypting data both at rest and in transit, rights management, and more as supporting technologies.



Can you talk about how having persistent data security controls could help a company to adhere to data protection responsibilities?

Balaouras: Persistent data security controls would help a company ensure the controls go wherever the data may go. This persistence can help an organization meet their data protection responsibilities from a security context, for example, with ensuring they meet business partner or third party partner requirements for secure handling of data. It could also ensure the right people who should have access to data are the only ones able to access and use it – with caveats. When we consider data protection responsibilities that involve data transfer or third party processing, context matters. For example, context such as consent for data use and transfer, data location and user access location, are things that can help to inform as well as enforce data access and use policies for data control. Just because personal data is encrypted, doesn't mean you are compliant with your EU GDPR obligations.

How are security leaders trying to change the privacy and data security message to one of opportunity and business enablement?

Balaouras: Enterprise security leaders emphasize a message of opportunity and business enablement when they demonstrate the value of privacy and data security for the organization. For example, robust security and privacy strategies, processes, and protections can help to build trusted customer relationships that drive loyalty and retention, capitalize on risks like workforce mobility or big data analytics that help drive growth, and protect future revenue streams by protecting corporate secrets and intellectual property. From a Zero Trust technology perspective, this requires an ecosystem where data visibility and security capabilities extend across existing data stores and access points (cloud, mobile, and more). This ecosystem includes data security at its core, but also includes protection considerations for identity, workloads, devices, and people, as well as the capability for overarching visibility and analytics, and automation and orchestration.



What would be a great way to get started on implementing a Zero Trust model now and make this achievable over the next six months?

Balaouras: Focus on five steps to get started with this data-centric Zero Trust security model:

1. Identify your sensitive data with classification and segment the network based on data sensitivity. You must know what it is that you're trying to protect, and what constitutes appropriate use of that sensitive data.
2. Map the data flows of your sensitive data and design a more optimal flow if needed. This helps you understand how data flows across your extended, not just internal, network and between people (employees, partners, and customers) and resources. Engage with multiple stakeholders to accomplish this.
3. Architect your Zero Trust microperimeters in several steps. Design and enforce microperimeters around sensitive data with physical or virtual security controls. Gain an understanding of user entitlements and limit and enforce access to these microperimeters where you have sensitive data. Create your automated rule and policy base for your control tools (e.g., DLP, email gateway, NGFW, etc) that help to enforce policies for data security and access. Use auditing and change control tools to help you continuously audit and optimize your rules, as well as manage and clean up unused rules.
4. Enable continuous monitoring of your Zero Trust ecosystem with security analytics. These are tools that can ingest and correlate information from disparate sources (such as applications, DLP, endpoints, IAM, and network flow data) to help you detect unknown threats and attacks and respond more quickly to attempts to steal data.
5. Embrace automation and orchestration where possible to improve your speed of responding to attackers attempting to exfiltrate sensitive data from your environment. To get started here, work with business leaders to define policies for automation (e.g., what does a legitimate business transaction with data look like) and tolerance for risk. Assess and document existing security operations center processes too, so you can evaluate maturity and standardize processes before automating them.