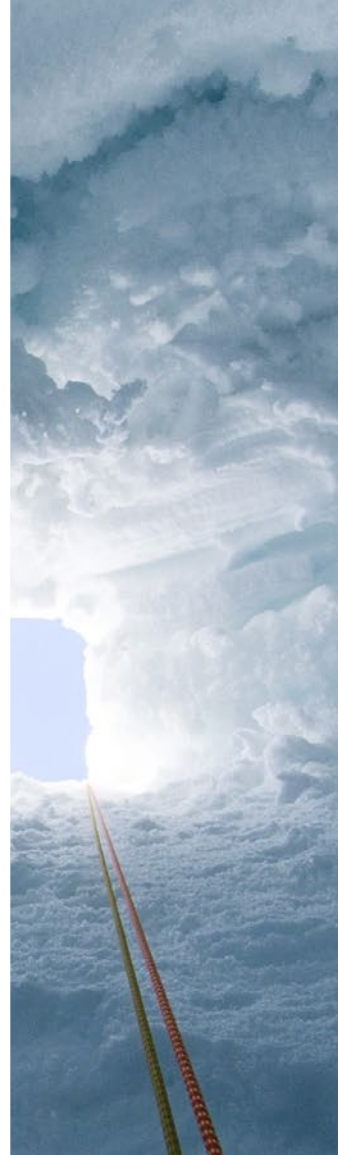


Zero Trust architecture: a paradigm shift in cybersecurity and privacy





Intro	3
Zero Trust architecture: towards data protection and compliance	4
Security architecture as an integrated part of enterprise architecture	5
Six steps towards implementing Zero Trust	6
1. Identifying and discovering sensitive data ('crown jewels')	6
2. Identifying sensitive data flows	7
3. Definition and architecture of micro-perimeters/data enclaves	7
4. Security policy and control framework	7
5. Continuous security monitoring and intelligent analysis	8
6. Security orchestration and automation	10
Conclusion and next steps	11
Contacts	12



Intro

Increasingly complex cyber-attacks and a reactive but sophisticated regulatory landscape are pushing companies' cybersecurity capabilities to the limits. A paradigm shift in IT security architecture – Zero Trust – has attracted increasing attention as a way of responding to these challenges. By enforcing a 'no trust without verification' policy, Zero Trust strengthens a company's cybersecurity posture by making cyber issues more visible and facilitating compliance with data protection requirements.

Given that cyberattacks can lead to devastating losses of money, trust and reputation, companies have an intrinsic incentive to strengthen their security set-up. The demand for an appropriate level of protection for specific data types is increasingly formulated in regulatory requirements that demand technical and organisational measures to ensure data confidentiality, integrity, availability and privacy.

As cyber threats increase and organisations simultaneously show continued deficiencies when it comes to data protection, the regulatory landscape is becoming more sophisticated and complex. According to PwC's 23rd CEO survey*, Swiss CEOs recognize this challenge. They consider cyber risks the third largest threat to their growth prospects and believe that regulation will become more fractured and complex. Even though Swiss firms show a certain level of awareness, they still maintain inadequate cybersecurity to be able to protect data, detect attacks in due time and be able to respond to an attack.

Fighting the symptoms rather than the causes is insufficient. Cyber-resilience starts at the root – the IT security architecture – which manifests and conceptualises information security. The IT security architecture determines how technical security measures are established within the overall enterprise architecture, aligning internal and external requirements. The security architecture addresses the entire life cycle of (electronic) data – from data generation, usage, transfer and storage to archiving and destruction – and it covers all components, including physical or virtualised client and server endpoints, IT and business applications, IT platforms and infrastructure, as well as the network that connects all the various resources together.

In the traditional approach to IT security, the network perimeter is used as the enforcement point for security controls. Once this point is passed, most resources can be accessed. This perimeter enforcement is, however, not sufficient any more, as many devices on a network have access to the internet. If a device is compromised, the attacker can access the corporate network without passing through the perimeter. A new paradigm is therefore required: Zero Trust.

* PwC's 23rd Annual Swiss CEO Survey 2019, PwC Switzerland, 2020
<https://www.pwc.ch/de/insights/ceo-survey-2020.html>

Zero Trust architecture: towards data protection and compliance

Unlike solely perimeter-based security, Zero Trust promotes a micro-perimeter approach based on user access, data location and an application hosting model. Within this micro-segmented network, sensitive data is protected, and any access is verified and requires authorisation. User behaviour analytics and real-time threat intelligence identify anomalies, and sandboxes ensure the isolation of potentially hostile data processing activities. The Zero Trust approach is not limited to the scope of the company's data centres, but also encompasses controlled access and monitoring of data traffic to cloud, web services and IT services outsourced to a provider. Zero Trust is thus a very good way of modernising network security in times of modern workforces and externally hosted IT services.

The term Zero Trust has attracted increasing attention for quite some time. The architectural design was first introduced in 1994 by the Jericho Forum. Later, the market

research company Forrester introduced the term Zero Trust Architecture. The security concept gained vast attention when Google announced the implementation of a Zero Trust network, BeyondCorp, a few years later. Google implemented this concept as a reaction to Operation Aurora, a series of sophisticated cyber-attacks that hit Google in 2009.

Zero Trust has now gone mainstream. The National Institute of Standards and Technology (NIST) in the US just recently published a Special Publication (SP 800-207) to formalise the approach, and the National Cybersecurity Center of Excellence is currently documenting an example Zero Trust architecture that aligns to the concepts and principles in NIST SP 800-207. But even though the concept seems to be on everyone's lips and is used to promote many product launches, it is not yet widely implemented at a corporate level. The visualisation below introduces the main building blocks of a Zero Trust architecture.

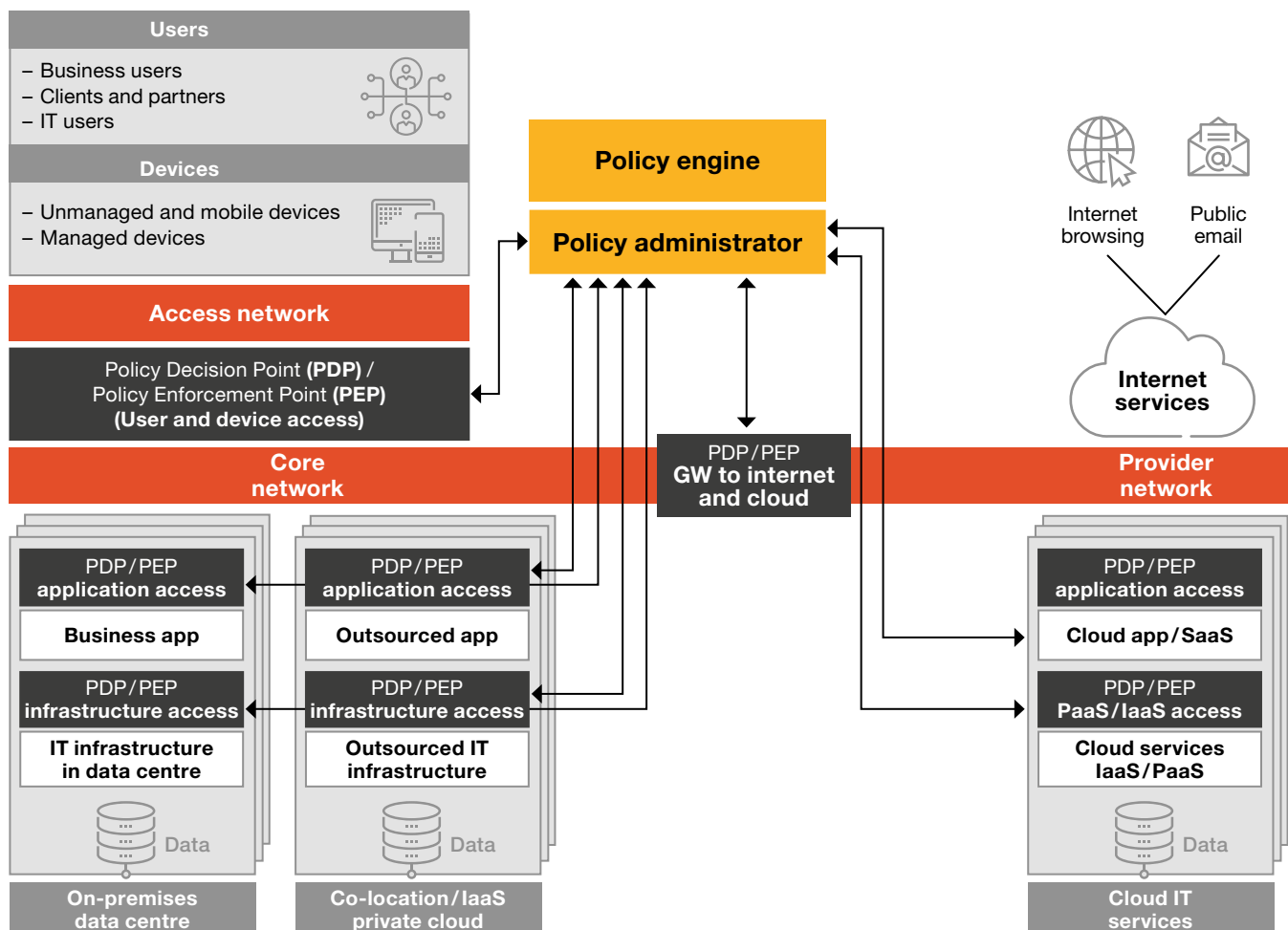


Figure 1: PwC Security Reference Architecture with Zero Trust Policy Decision / Policy Enforcement Points

The most important building blocks are the so-called policy decision points (PDPs) and policy enforcement points (PEPs) within the corporate network, used to build data enclaves and micro-perimeters. PDPs and PEPs are the points where security information is collected and used to either decide what path a transaction should take (PDP) or to enforce a specific policy, such as requesting an additional factor for authentication or blocking a transaction if it's considered non-trusted.

The diagram above shows that PDPs and PEPs aren't just on the external perimeter, but on many different points to segment the network into zones. Depending on the size of an organisation's IT estate, the segmentation of network zones might include several server zones to separate applications with different trust levels. Further segmentation is possible between the middle tier and the back-end data storage.

Security architecture as an integrated part of enterprise architecture

To make the right decisions on network segmentation and the positioning of PDPs and PEPs, the security architecture needs to be closely aligned with the business architecture in order to understand the data types processed, data classification applied and derived protection levels to be compliant with internal policies and external regulations. As a guiding principle, the business should drive IT, and IT security should be considered a quality aspect of IT. This means that the business needs to formalise requirements for IT and IT security to appropriately protect data processed along the business processes. The visualisation below shows how the business

architecture can be used as a starting point to identify sensitive electronic data and data with enhanced regulatory requirements processed in business services. Once this data is identified, data classification defines the protection level required to process, transfer and store sensitive data in an organisation. The business architecture is thus the starting point for identifying applications used along the business process to make use of electronic data in the specific context of an organisation, and data governance drives the process to classify data according to the applicable regulations.

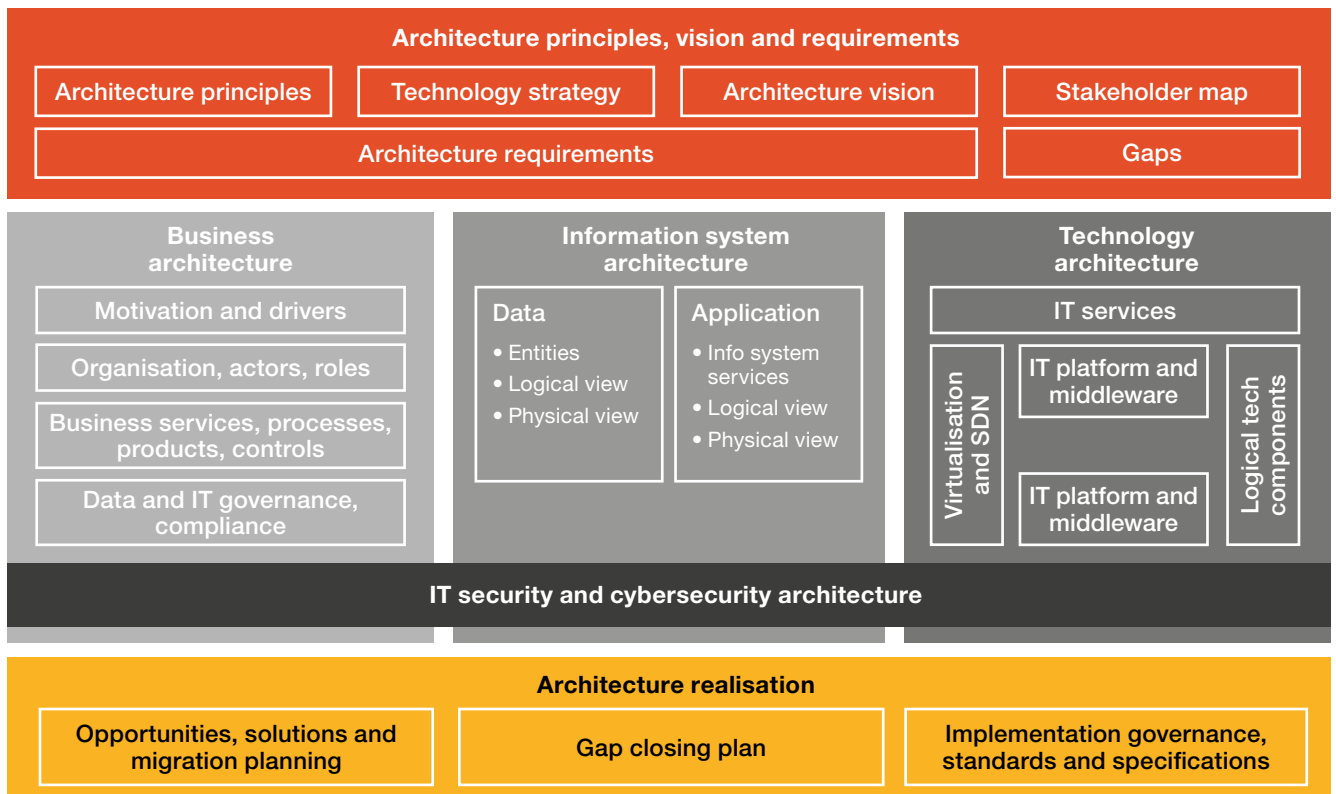


Figure 2: The security architecture as part of an enterprise architecture framework

Six steps towards implementing Zero Trust

Applying Zero Trust to a specific environment of an organisation requires six steps:

1. Identifying and discovering sensitive data ('crown jewels')

An organisation can outsource its entire IT infrastructure. However, the responsibility for data protection and compliance remains with the organisation. It's therefore crucial to set up an inventory of data repositories. This inventory will allow the organisation to identify the protection level and criticality of data, which is determined by internal (e.g. intellectual property and business value) and external (e.g. legal and regulatory compliance) requirements.

Depending on the different set of regulations and internal data requirements that apply, it's a good idea to distinguish between the following data types (the list isn't exhaustive):

- Personal identifiable data (PII) according to the Swiss regulations and the EU General Data Protection Regulation (including client identifying data, CID, as a subset of PII to comply with local banking regulations)

- Payment card industry data according to PCI DSS
- Business data such as financial statement information and tax-relevant data
- Business secrets concerning intellectual property and other sensitive data such as mergers and acquisitions (M&A) information.

You might consider the holistic micro-segmentation of all data to be too costly. At the minimum you should use application processing data with a certain criticality level – in terms of confidentiality, integrity, availability and privacy – to create data enclaves with segmented sub-perimeters (see step 3 below). To establish a data inventory, you need to discover all the data processing activities within the entire IT environment to be able to assign the data sets to a data inventory and verify that the categorisation and classification of the data set is correct and a data owner is assigned. You also need to do an inventory of all data processing applications, along with additional details to determine the underlying IT infrastructure and the sourcing option used. This should include data storage locations, backup locations, file shares and other storage locations. The data repository needs to be linked to the application inventory to inform the data owner where data processing activities take place and who has access to these data. This is the basis for identifying sensitive data traffic as outlined in step 2.



2. Identifying sensitive data flows

To properly design network segments and detect anomalous activities, your organisation needs to be aware of the flows of sensitive and critical data. This step has to involve IT and business staff to understand the dependencies between the applications required along the business processes, the involved IT components, the data traffic and the required access rights. The business architecture is a good starting point to understand the data types being processed by departments/corporate functions. The link to the IT applications that process these data allows you to understand the data flows.

A good way to document sensitive data flows is to use swimlanes indicating what roles (impersonated by business users) process sensitive data as a task to perform a relevant step of a business process by using an IT application. It needs to be clear whether a business application processing sensitive data is operated and hosted by the local IT unit, is outsourced to a partner, or is provided as a cloud service. This presumes adequate device management covering

- End-user devices (e.g. unmanaged, BYOD, mobile devices or corporate managed devices)
- Network devices (owned/managed by your IT organisation)
- Corporate IT devices in the data centre (servers, storage, etc., owned/managed by your IT organisation)
- Inventory of sourced IT services if SaaS, IaaS or PaaS from a public or private cloud is used

Verifying that all sensitive data flows are captured is a joint exercise. The business has the contextual information regarding data processing, and IT can ensure that all business applications, data repositories – as identified in step 1 – and devices are covered in the sensitive data traffic analysis. Once you have that you can deploy adequate measures determining how to protect data at rest, in motion or in use.

3. Definition and architecture of micro-perimeters/data enclaves

The definition of sub-perimeters depends on step 1 (the identification of sensitive data) and step 2 (flows of these data within networks, sites and IT systems). The identification of sensitive data repositories means implementing need-to-know/need-to-do, and is based on least privilege principles for access controls. This requires a data owner to understand and define what roles need to access data, approve access requests from users holding that role, and entitlement management. But user entitlements aren't a one-off exercise: access controls require continuous revisions and auditing. An adequate user management process handles the following broad groups of IT users separately:

- Business users with access to an IT application that processes sensitive data

- IT users with privileged access who are able to modify user access rights and security configurations, ending in the ability to access sensitive data
- Clients and partners with access to sensitive data.

For each user group – and potentially at sublevels – you have to define a set of controls that documents joiner-mover-leaver processes, user entitlements and regular recertification cycles.

In addition to user access management, data resources (storage and processing resources) with similar data protection requirements might be grouped in a dedicated 'enclave' that can only be accessed by end points with a certain trust level. Such policies can be enforced at the PEP by protecting access to the data enclave, thus offloading security enforcement from each IT system and IT application. A data enclave can either be a network segment in a data centre, in the cloud or with an IT service provider.

4. Security policy and control framework

In step 1, data types with specific regulatory requirements were identified, discovered and filed in an inventory of data repositories. Based on external and internal requirements applicable to the various data types, the criticality of data can be formalised along the criteria of confidentiality, integrity, availability and privacy. For PII additional considerations need to be applied to address also privacy requirements appropriately. In accordance with industry good practice standards, technical and organisational security controls are defined in a security policy framework.

The security policy framework is applied to the IT security architecture which implements policy enforcement. NIST SP 800-207 distinguishes between policy enforcement points (PEPs) and policy decision points (PDPs). This ensures that policies are enforced at all gateways and data enclaves or – in case of a policy violation – an action is triggered. As shown in Figure 1, the following network segments with PDPs/PEPs are suggested as a minimum:

- **PDPs/PEPs for user & device access:** Only users with an appropriate entitlement can access IT systems that process sensitive data. This can be achieved (i) via managed end user devices, (ii) by onboarding an unmanaged device (e.g. a bring your own device [BYOD]) at first via a mobile device management (MDM) system or (iii) by providing a virtual desktop infrastructure as a precondition to grant access to sensitive data.
- **PDPs/PEPs on the application level:** On the application level, access to sensitive data is granted based on the least privilege (need-to-know/need-to-do) principle. This means that application users only have access rights to data required for their daily work. Privileged roles are implemented via step-up mechanisms or via a separate login. In addition, application security controls and application logging are enforced, and logs are sent to a centralised log repository.

- **PDPs/PEPs on the IT infrastructure level:** This includes privileged IT roles on the platform and IT infrastructure level to operate and maintain IT platforms (operating systems, databases, storage, network and virtualisation). Access to sensitive data for privileged IT accounts should be limited to a minimum via access control, data encryption technology and break-glass procedures. In addition, you might use dedicated management zones with jump host and other security measures might to block management access via standard user access zones.
- **Access to data** is granted either via an application or an IT infrastructure. There is no direct access to data on storage level. Sensitive data should therefore not be downloadable to a personal device, personal storage device or public cloud storage outside the organisation's access management.
- **PDPs/PEPs to internet & cloud services:** This refers to gateways for specific protocols and IT services:
 - **Web browsing (outbound):** This gateway ensures that only legitimate sites and content are accessed, and that sensitive data are not uploaded to unauthorised cloud storage services or shared externally. In addition, there should be mechanisms to detect infected end-points contacting known command and control (C2C) infrastructure and detect the installation of malware at an end-point, along with other anomalies.
 - **Web access (inbound):** Access via the public internet, i.e. via a web application, needs a gateway referred to as web application firewall (WAF) or reverse proxy to enforce access policy for web services from the internet and enable malware detection.
 - **Secure email gateway:** This is the gateway separating internal and external email. It detects and protects against data leakage via email and ensures email security. This includes detecting spam, phishing and malware delivery via email.
 - **Cloud security gateway or cloud access security broker (CASB):** This gateway ensures that business data is only shared and processed with authorised cloud providers and that security measures for data protection, confidentiality and access control are applied accordingly. A CASB is usually able to encrypt sensitive data before it's sent and stored in a SaaS application such as Microsoft SharePoint, Microsoft Dynamics, Salesforce, etc.
 - **Remote access:** Remote access by business users, IT users and partners with privileged access to sensitive data needs to pass a special gateway for management access to IT infrastructure and policy administration. For privileged IT users a 'jump host' is used.

The security policy and control framework cover the entire IT scope, whether it's on-premises, outsourced or in the cloud. Trust is not given based on a concept or a service level agreement, but is verified before access to IT services and data is granted. Trust is conditional on a non-exclusive combination of the user's ID, the connecting device, the connecting location and the accessed service.

To ensure that the policy framework includes all the necessary safeguards, you need to do a threat assessment that simulates common threats along the critical data flows in the entire IT estate controlled by your organisation. This enables you to verify that any identified cyber risk is mitigated to an acceptable level, and helps ensure that detection measures are in place and effective.

5. Continuous security monitoring and intelligent analysis

All relevant end points, gateways (PDPs and PEPs) and all sensitive data traffic require logging and real-time inspection for malicious activities. Depending on the maturity and size of your organisation, monitoring functions can be distributed across several IT divisions, which is a challenge when it comes to reliably detecting security relevant incidents. You should make sure monitoring covers the following focus areas:

- **IT operations monitoring** usually refers to the availability of IT services, network components and communication links.
 - **Enterprise security monitoring** refers to all IT infrastructure components owned and managed by the corporate IT organisation. A centralised log repository with visualisation, dashboards and reporting provides a viewfinder into the organisation's IT security estate. In addition, a security information and event management system (SIEM) should be in place to process and correlate events to be able to reliably detect security incidents.
- Organisations with a higher level of maturity extend the scope of security monitoring from monitoring their own IT devices to a full view of their IT infrastructure, including public cloud services or wherever corporate data are processed, transferred to/from or stored.
- **Compliance monitoring** includes all aspects that are not covered by security monitoring or IT operations. Usually the following aspects are covered in compliance monitoring:
 - Security configuration baseline monitoring
 - File integrity monitoring/detection of unauthorised changes
 - IT asset discovery and vulnerability scanning
 - Data breach detection





Zero Trust introduces compliance monitoring as a subset of (enterprise) security monitoring, and assumes that event logs are a central service and available to all monitoring functions. In reality, logs, events and information are often duplicated and not shared among all monitoring functions. To ensure appropriate handling, your organisation therefore needs to determine which log information has to be retained and whether additional requirements for legal admissibility and e-discovery might apply for investigations and audit purposes. You also need to define whether additional measures are required to maintain integrity and avoid deletion or alternations. It's important to realise that the different aspects of enterprise security and compliance monitoring vary in terms of their focus areas and the immediacy with which alerts and deviations are responded to.

Security monitoring aspects

Usually the security operation centre (SOC) is in charge of analysing security-relevant events and verifying security incidents to detect cyberattacks at the IT infrastructure level, advanced persistent threats, lateral movement and other common cyber threats. Identifying attacks can be facilitated using information from end-point agents acting as PDPs and PEPs to enrich the network and device logs used by the SOC – usually processed in a SIEM. Security monitoring also requires access to the software package repository and configuration management database (CMDB) to verify that the applicable security configuration baseline is applied. Deploying user and entity behaviour analytics (UEBA) together with threat intelligence feeds of known bad IP addresses and domains, anomalies can be detected by correlating data from different sources in the SIEM and enriched to make use of automation to minimise human resources for manual verification by the SOC analysts.

Compliance monitoring aspects

The compliance aspect in security monitoring adds business awareness to data processing activities across the entire technology stack. It involves defining the regular/unsuspicious use of sensitive data within an organisation. The aim is to provide evidence to the data owner and to internal/external audit that all relevant security controls are in place and effective, and that the need-to-know principle for data access is enforced. The aspects current regulations require evidence for include:

	Compliance aspect	Details	Evidence
1	Security configuration baseline (SCB) monitoring 	Technical baselines are defined and applied to all IT infrastructure elements. SCBs are regularly monitored via a tool. Deviations are managed by a formal process.	Compliance report for all IT infrastructure elements in scope of regulations; process to manage SCB and deviations.
2	File integrity monitoring (FIM) 	On the application and platform level critical system parameters are identified and monitored for changes.	Authorised & unauthorised changes for each platform and app; change process; FIM alert handling procedure.
3	Vulnerability monitoring 	In all relevant network segments, IT assets are discovered and regular vulnerability scans are conducted.	List of IT assets with a status of known vulnerabilities; vulnerability management process.
4	Data breach detection 	PII/CID data leakage is detected or prevented at client end-points, application and relevant gateways.	Application logging; use cases for suspicious behaviour in application; upload, email security incident processes.

To have comprehensive compliance monitoring in place you first need to establish IT governance and data governance. Depending on the maturity of your enterprise security monitoring, tools, sensors and logs may already be in place, and it may only be necessary to create new reports, dashboards and visualisations. Many organisations are aware that they currently lack visibility and need to evaluate and deploy new tools.

The main difference between enterprise security monitoring and compliance monitoring is their response time to alerts and deviations. Security relevant alerts could trigger an immediate reaction from the computer security incident response team (CSIRT). Compliance monitoring, on the other hand, involves verifying IT hygiene and IT quality aspects to ensure that

relevant IT security controls are in place and effective. A compliance alert (e.g. an unauthorised change of a security-relevant configuration) would not require an immediate response from compliance monitoring if it is not caused by the lateral movement of a malicious threat actor.

Compliance monitoring therefore delivers valuable evidence for IT hygiene, internal and external audits, and speeds up the process of evidence collection for the auditor. If required, compliance monitoring tools can be used for continuous auditing to eliminate the need to provide ad-hoc evidence for the auditor.

6. Security orchestration and automation

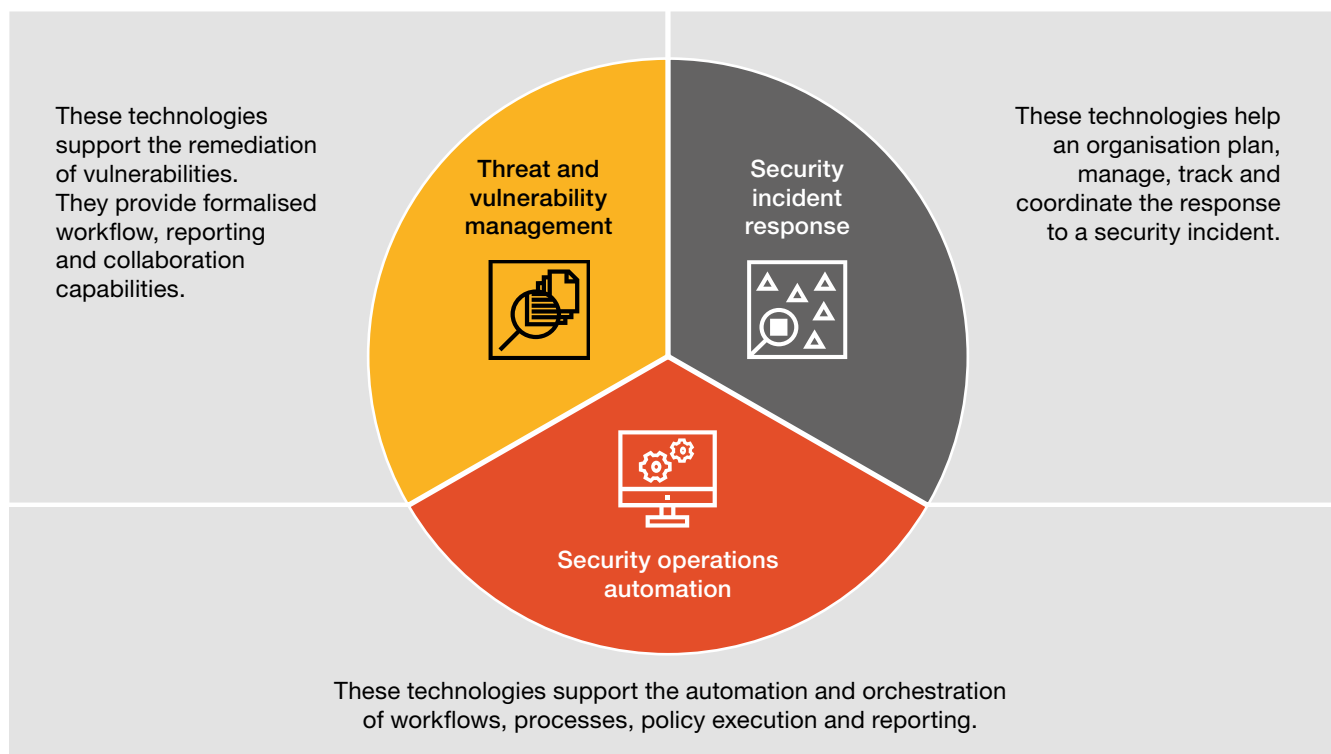
As soon as enterprise security monitoring and compliance monitoring are established and have reached a basic maturity level, successive improvements follow.

As speed is paramount for the detection and remediation of cyber-threats, your organisation may decide to implement automated security analytics to minimise exposure to vulnerabilities. For instance, if malicious behaviour is identified with a high degree of confidence, the user in question can automatically be isolated from the network. There's also great potential for automatically updating the rule and policy base for access controls by integrating it in your HR department's joiner-mover-leaver process to efficiently maintain trusted identities and assigned roles. To make use of automation, you need an orchestration layer combining all policy enforcement points with the policy administrator. The orchestration layer allows you to include additional aspects – such as threat intelligence feeds or DNS sink hole information – to increase confidence when identifying policy violations and suspicious processing of sensitive data.

If you opt for such an integration, you need to make sure different tools and data sources are interconnected. SOAR (security orchestration, automation and response) is a solution stack of compatible software programs that allow an organisation to collect data about security threats from multiple sources and respond to low-level security events without human assistance. The goal of using a SOAR stack is to improve the efficiency of security operations. The term, which was coined by the research firm Gartner, can be applied to compatible products and services that help define, prioritise, standardise and automate security incident response functions.

According to Gartner, the three most important capabilities of SOAR technologies are:

The transformation towards Zero Trust is a time-consuming and complex task. It's therefore advisable to initiate it in an area of the network that's well understood in terms of the data types and data flows it's attached to. Other parts can then be transformed successively without disrupting your business environment.



Conclusion and next steps

Zero Trust isn't a product or status. It's a concept that helps an organisation gain transparency on data processing activities, identify sensitive or critical data, and apply an adequate level of protective, detective and reactive security measures.

It's crucial to understand that trust isn't guaranteed merely on the basis of a promise made by a vendor or provider or a policy statement accepted by a user. Trust needs to be verified at policy enforcement points (PEPs) or policy decision points (PDPs) before access to a data enclave or a network segment is given. To do so it's necessary to segment the network and use of centrally managed next-generation firewalls – as policy enforcement points in front of data enclaves where sensitive data are stored and processed – regardless whether this in the cloud, on premises or at an IT provider's.

Finally, the best way of detecting cyberattacks and unauthorised access to sensitive data is to process all security relevant information and logs centrally to verify that data protection measures are in place. Comprehensive security monitoring allows you to identify suspicious data processing by learning from the legitimate day-to-day use of sensitive data, threat intelligence and correlation. PEPs and PDPs deliver the necessary information to correlate security-relevant information so that automation can be applied and suspicious transactions can be contained.

PwC is happy to support organisations and service providers with the implementation of Zero Trust and compliance monitoring by:

- **Helping them identify and discover critical or sensitive data types**
- **Defining and applying data categorisation and classification**
- **Providing architecture guidelines to integrate Zero Trust in security architecture and aligned enterprise architecture**
- **Helping them implement data protection solutions and processes**
- **Running compliance monitoring as a service or helping organisations operate compliance monitoring independently.**



Contacts

For more information please contact our experts



Urs Küderli
Partner, Leader Cybersecurity
and Privacy, PwC Switzerland
+41 58 792 42 21
urs.kuederli@pwc.ch



Fabian Faistauer
Head Cybersecurity Technology &
Transformation, PwC Switzerland
+41 58 792 13 33
fabian.faistauer@pwc.ch

PwC, Birchstrasse 160, 8050 Zurich, +41 58 792 44 00

© 2023 PwC. All rights reserved. "PwC" refers to PricewaterhouseCoopers AG, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.