Europe: Future of Trust

Trust is a nebulous concept. It has traditionally been viewed through one of two lenses: either in a broad sense, relating to equally nebulous themes such as perception and loyalty; or in a narrow sense relating to specific technical approaches such as the Zero Trust security architecture or silicon trust modules in chip design. IDC's Future of Trust research theme aims to bring together the specific and the general in an end-to-end approach. It encompasses a suite of top level 'elements' such as risk, compliance, security and ethics that are important at the board level. But it also explores how these across both internal governance level and across the ecosystem through supply chain management. This research theme will also explore the technologies that underpin trust programs, as well as the business benefits that they can drive.

Markets and Subjects Analyzed

- AI and Analytics
- Cloud (IaaS, PaaS, SaaS)
- Customer Experience
- Data Loss Prevention
- Data Management
- Data Protection
- Distributed Ledger Technologies
- Encryption
- Endpoint Protection
- Enterprise Comms
- Enterprise Mobility
- Identity & Digital Trust
- IoT
- IT Services
- IT/OT Convergence
- Network Lifecycle
- Network Security
- Partnering & Ecosystems
- Privacy
- SAIRO
- Web Security
- Security Services

Core Research

- IDC Perspective - How can European Enterprises Harness AI and UEBA Without Compromising Trust?
- Future of Trust Supplier Insights - Technology for Sustainability and Social Impact (TSSI)
- European Cloud Security Forecast - Supporting Trust Through Security 'of and from' the Cloud
- European PeerScape for Trusted IT/OT Convergence

In addition to the insight provided in this service, IDC may conduct research on specific topics or emerging market segments via research offerings that require additional IDC funding and client investment. To learn more about the analysts and published research, please visit: Europe: Future of Trust.

Key Questions Answered

1. How and why is Europe different when it comes to the Future of Trust?
2. How can European enterprises harness dynamic themes like AI and cloud without comptomising trust?
3. What do leading European enterprises prioritise when launching their trust programs (technologies and values) and why?
4. How can European enterprises assure trust in diversifying connected infrastructures - incl. IoT, IIoT & OT?
5. What are the inhibitors European enterprises must overcome to achieve the Future of Trust?

Companies Analyzed

This service reviews the strategies, market positioning, and future direction of several providers in the Future of Trust market, including:

Accenture, Akamai, Anonos, Apple, Arm, Atos, AT&T, AWS, Blackberry, Box.com, Broadcom, BT, Capgemini, CheckPoint, Cisco, Commvault, Dell, Deloitte, Deutsche Telekom, Digital Guardian, Digital Shadows, Dropbox, DXC, Entrust Datacard, Ericsson, EY, F5, FireEye, Forcepoint, Fortinet, Fujitsu, Google, Guardtime, HCL, Huawei, HP, IBM, Imperva, Intel, Jitsuin, Juniper, Kaspersky, KPMG, Lenovo, LogMeIn, LogRhythm, McAfee, Micro Focus, Microsoft, Mimecast, MobileIron, MongoDB, Netskope, Nokia, NTT, O2, Okta, OneTrust, Orange, Palo Alto Networks, Ping Identity, Positive Technologies, Proofpoint, PwC, Qualys, Rapid7, Retarus, Ricoh, SAP, SailPoint, Salesforce.com, Samsung, SecureWorks, Skurio, Snyk, Sophos, Splunk, Stormshield, Symantec, Tata Comms, TCS, Telefonica, Tenable, Thales, Trend Micro, Trust-Hub, Trustwave, Unisys, Utimaco, Veritas, Verizon, VMware, Vodafone, Wandera, Zscaler