ALERTENTERPRISE

WHITEPAPER

SECURITY IS THE NEW BUSINESS ENABLER TO ACCELERATE ENTERPRISE DIGITAL TRANSFORMATION

DIGITAL TRANSFORMATION HAS A NEW NAME – DX

As digital technology dramatically improves the economics and capabilities of every business, Digital Transformation or DX, is a quest for high-performance companies to gain further efficiencies/improve operational metrics and pull ahead of their competition. Recent studies found using hardware, software, algorithms and the internet DX is 10xs cheaper and faster to engage customers, create offerings, harness partners and operate business. It is now the job of digital-minded business leaders to apply rules to engage, compete and grow.

The emergence of the cloud and as-a-service platform economy have created a sense of urgency all the way up into the corporate boardroom. Business customers want the same Amazon-like experience for business-to-business transactions to perfect recurring business models, optimize the customer lifetime value and maximize Annual Recurring Revenue or ARR. DX helps bridge the gap between what the business customer expects and how the enterprise delivers it.

Studies have shown using hardware, software, algorithms and the internet DX is 10xs cheaper and faster to engage customers, create offerings, harness partners and operate business.

New Masters of Change. DX Transforms IT Roles

DX has transformed the IT role into master of change. No longer are they the ones applying controls. IT risk and compliance managers in the enterprise have seen their role as that of putting on the brakes. IT has been the one to make sure that separation of duties and segregation of access is enforced. IT breaks up the big picture into smaller pieces so that no one has the real view. The days of security by obscurity are over. A new paradigm has evolved and is here to stay.

By attaching roles-based access and identity intelligence to application and data access, we can make sure that only authorized individuals get access to applications, data and business information. We can also make sure that only authorized people and trusted devices transact. In the digitally transformed world trusted partnerships are established at the speed of light, transactions completed and then these partnerships end almost immediately to move on to the next transaction.

DX totally transforms our notion of risk. With the ability to use artificial intelligence and machine learning, risk is now brought into decision making at high speeds. This increases the reliance on threat intelligence based on machine learning and anomaly detection to make sure risk is minimized holistically for many more successful outcomes.

79% of organizations agree that having an enterprise security leader enhances the effectiveness of corporate security.

49% of organizations say that convergence has led to better alignment of security strategy with corporate goals.

The State of Security Convergence, 2019, ASIS Foundation

Embrace DX Across the Entire Enterprise – not just IT

DX helps enterprises become increasingly customer focused and outward facing. Organizations from all walks of life across a multitude of industries —banking, financial services, manufacturing, energy and utilities, transportation, life sciences and many more have realized the importance of bringing information from the operational aspects of the company to front of the house.

Customers are asking, when can I expect my order to be shipped? When will it arrive? Customers may want to place orders with a reseller instead of direct with the company. In this case they want to utilize asset-based financing for other lines of product that they are acquiring from a reseller and track their payment terms. The ability to setup payment dates, subscription services and add corporate users to SaaS services through a self-service portal are all examples of digitally enabled capabilities similar to what people are accustomed to in the consumer world. Making reliable, solid information available that customers can trust requires collaboration in real-time between various functions that extend beyond IT and include Operations, Production, Customer Experience, HR, Finance and others.

The Effectiveness of Holistic and Integrated Security Approaches

As on-premise applications are supplanted by cloud-based solutions, hybrid applications that operate on both mobile and cloud infrastructures become more prevalent. This also means more systems, applications and end-points need protection against cybersecurity threats.

Additionally, the proliferation of internet of Things (IoT) devices both inside and outside the enterprise has created an alarming growth in the attack surface from a security perspective. This is because they are connected to the cloud and ultimately to back-end systems in the enterprise. It has now become critical to be able to view the operational state of systems and applications in one place, resulting in a holistic view of the infrastructure and its data and information regardless of where it is physically located.

Digital rewrites the rules of business — digital innovators don't just bolt on a pretty digital face. They create new product and service offerings with both the experience and operations to support them. Key to creating a robust and growing following for any digital business is creating a notion of trust and a feeling of security on the platform conducting business.

The Critical Industry 2.0 DX Disruption

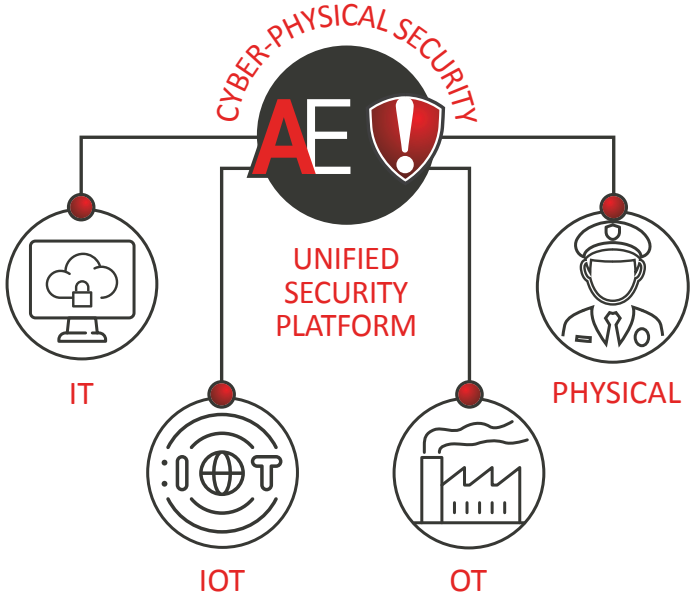
Unified Security Must Extend Beyond IT and Include OT and Physical Security Controls

As organizations proceed down the path of digital transformation they need to create a unified view of their processes and respond to business needs to expose more back-end systems and information to customer and partner facing processes.

Critical infrastructure companies and large asset operators in particular are now dealing with modernized operational systems that leverage IoT, mobile 4G/5G networks and cloud connectivity that extends beyond traditional enterprise network boundaries. Infrastructure regulations related to energy, utilities, chemicals, financial services and more now have the additional dimension of tracking physical access controls to ensure that only permitted roles within the organization can access the systems containing sensitive data.

Employee or contractor control room access is tightly monitored to guard against insider threat as digital systems are controlling more and more of our critical infrastructure. Security Convergence now encompasses IT security, Information Security, Physical Security, Operational Technology (OT) Security and IoT Security, all rolled-up into Cyber-Physical security.

New converged cyber-physical security models are being adopted to detect security gaps that are otherwise impossible to detect by conventional IT-only security automation tools. Security convergence provides a common pane of glass to finally be able to visualize risk across IT, OT and physical security domains.



Digital Trust is at the Heart of Digital Transformation

For years security experts have predicted the death of the corporate perimeter. While the pronouncement might be a little stark, there is a lot of truth to the fact that today's workforce is constantly mobile, moving in and out of corporate and other locations with access to all the information previously restricted to the enterprise perimeter and kept behind four walls.

Security experts now agree that the most important aspects of security start with the identity of the people accessing applications and information related to the enterprise. Are they authorized? Do their privileges extend to transactional data? How long should access be granted? Who else can see the data? Are their connections secure from attack? And how can their access be turned off when they leave the organization?

What about IoT devices? With billions of IoT devices connected, how do I know if devices on my side of the cloud are connecting to validated, authorized devices on the other end?

The key is establishing Digital Trust and verifying identities to trusted identities of people, systems, applications and devices.

THE KEY...

to creating a robust and growing following for any digital business is establishing a notion of trust and a feeling of security on the platform conducting business.

Security Starts with Establishing a Digital Identity Backed By Trust

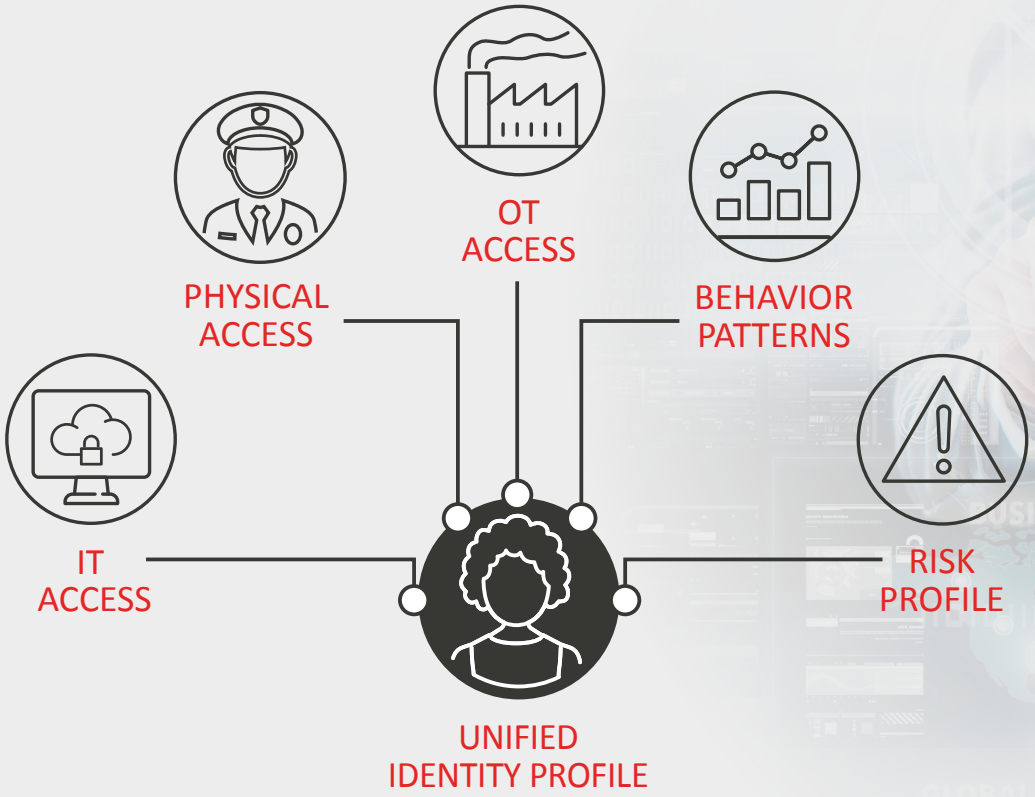
Identity and Access Management has come full-circle from being a practice area deep inside IT that defined how employees gain access to their applications based on their job function, to creating a complete picture of how employees, contractors, vendors, visitors and others interact with all business processes in the enterprise.

Enterprises must move beyond the siloed approach of multiple identity systems for different aspects of the company — one for directory services, another for corporate networks and email, a separate identity structure for those with physical access to the corporate and satellite facilities. Finally, yet another identity repository exists for those with access to operate and maintain industrial control systems, end-points and processes.

This unfettered proliferation of identities creates huge risk in the enterprise. For example, a company with some 10,000 employees may end up with 30,000 identities as a result of adding up IT identities, OT identities and physical access identities. It becomes much harder to manage and provides no way to attribute events to real identities, creating upfront security risks.

Security experts now advocate enterprises establish a **Common Digital Identity** for people and things. The digital identity is a starting point for provisioning system access, data access, network access and yes, even physical access. As roles and functions change in the organization overtime, these trust attributes can be automatically updated to minimize risk, control access and meet regulatory compliance requirements. New security convergence techniques delivered through innovative convergence platforms, either on premise or in the cloud, can deliver digital identity trust.

IDENTITY HAS MOVED TO THE CENTER OF SECURITY



NEXT STEPS

Security and risk management leaders should start by developing a compelling vision and strategy that will resonate with key company stakeholders. They can expand the visibility they have into workforce activity beyond things that happen on the network. Go beyond a data-centric approach to a people-centric approach through identity behavior analysis. Improving visibility into workforce activity and taking a more preventive approach are the best ways to manage risk of an incident. Develop an inside-out approach to security. By converging physical, cyber, IT and OT security you'll gain a holistic view of your enterprise-wide landscape.

The digital transformation and its impact on physical security are clear. It takes a new approach, focusing on bringing people, processes, data and technology together safely and securely. The future is here, and with AlertEnterprise organizations are now empowered to do more with less, create engaging employee experiences, increase compliance and reduce risk – all from a single, trusted security convergence platform. For more information, contact AlertEnterprise today at info@alertenterprise.com.

ALERTENTERPRISE