EXECUTIVE BRIEF

IDC
ANALYZE THE FUTURE

Building Digital Trust With Privilege Management

Sponsored by:
BeyondTrust

Content

About this Executive Brief

This IDC Executive Brief is based on existing IDC research including the surveys IDC, European IT Security Survey (June 2020), IDC, Digital Future Reignition Survey (December 2020); the IDC Semi-annual Public Cloud Services Tracker (November 2020) and IDC FutureScape: Worldwide Future of Trust 2021 Predictions.

The research for this BeyondTrust: 'Building Digital Trust With Privilege Management' report was led by Anders Elbak, Associate Director, IDC Nordic.

IDC ANALYZE THE FUTURE

Preface – by BeyondTrust

The global pandemic touched our lives on many different levels and caused enormous changes to lifestyles and workplaces. The cybersecurity industry was no exception. Malware increased by 30,000% in 2020[1]. A number that is of particular concern given the fact that many organisations still rely on traditional antivirus software (AV) or Endpoint Detection and Response solutions (EDR) alone to secure their endpoints.

Alongside the significant increase in malware and expansion of the threat landscape the shift in lifestyle and workplace has propelled the need for organisations to build a solid foundation of Digital Trust. This means that the need to move from a reactive to a preventative approach is more important than ever before.

At BeyondTrust we advocate Endpoint Privilege Management as part of a layered, preventative approach to endpoint security, ensuring frictionless user experience by giving the right level of access at just the right time. We enable organizations to implement least privilege and allow pragmatic application control alongside other crucial elements of a complete endpoint security strategy.

In this IDC Executive Brief, we uncover insights from IT security professionals across the Nordics and Benelux and present the findings. Current challenges facing organizations are identified alongside recommendations of how organizations can adjust their security plans in response to the significant increase in malware whilst ensuring they support the move towards a more digitized organization that is underpinned by Digital Trust.

[1] www.zscaler.com/blogs/research/30000-percent-increase-covid-19-themed-attacks

BeyondTrust

IT Security Priorities Reflect How the Threat Landscape Evolves

IT Security has topped the list of priorities among IT decision makers in organisations across the Nordic and Benelux regions for at least a decade. However, the exact security priorities constantly change as technology evolves and the threat landscape develops. In addition to this, there is a wider acknowledgement that security is complex and much more than trying to establish an impenetrable perimeter protection.

From a security operations point of view, the most prevalent priorities are managing internal risk, addressing the skills shortage, and ensuring compliance[2]. Internal risk involves ensuring that employees do not deliberately or through negligence compromise security. To ensure this user access must be granted and evoked as needed, and applications inside the networks need to be secured against malicious attack for example against ransomware.

The most widespread technology priorities reported in 2020 centred on orchestration, IoT, cloud, consolidation, and IT/OT convergence[3]. This mirrors the expanding threat vector as the IT architecture increasingly extends to cloud environments, and devices and equipment beyond the traditional IT realm. It also highlights the fragmentation and lack of unified security tools that security professionals struggle to manage every day.

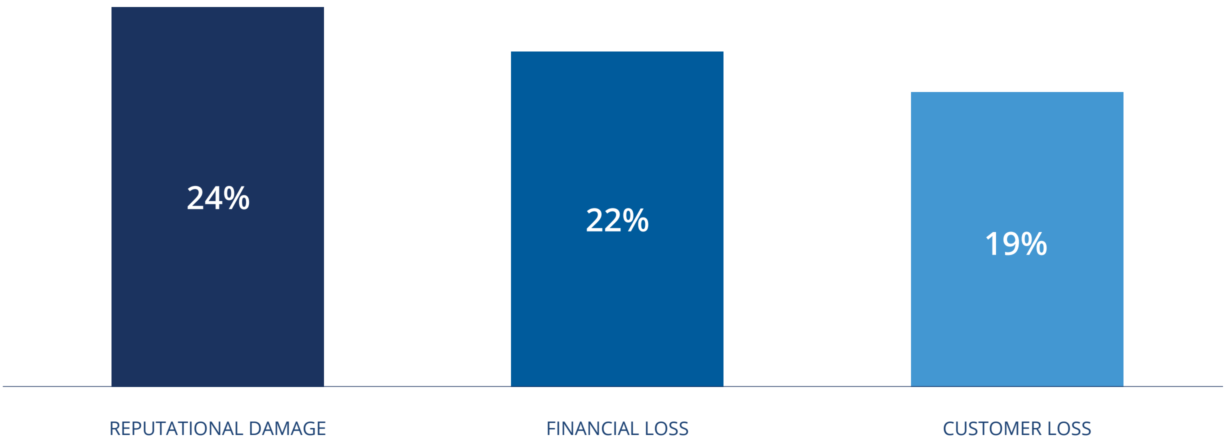
2-3) IDC, European IT Security Survey, June 2020

IT Security Breaches Hurt Businesses in New Ways

IT security breaches undoubtedly have negative consequences for the companies being hit. Traditionally the consequences were productivity loss from systems being down, or theft of sensitive corporate data.

Today, this has changed, and concerns are tied directly to the business performance. As illustrated in the figure below, security executives in the Nordic and Benelux region, point to reputational damage, financial loss, and loss of customers as the three most prevalent concerns.

Security Executives Greatest Concern Regarding IT Security Incidents in the Nordics and Benelux



Source: IDC, European IT Security Survey, June 2020 (N = 201)

In todays digitised world, customers – whether consumers or businesses – usually have an abundance of options when selecting a product, solution, or service. If the required product or service cannot be accessed due to a security breach, there is a genuine risk that the customer will shift to a competitive provider.

Direct financial loss is a genuine risk following a security breach today. Driven by the rise of increasingly more advanced and targeted ransomware attacks, and with companies' growing dependence on data availability, paying a ransom is often the cheapest and quickest option to ensure a prompt return to service.

The most prevalent concern reported in 2020 however was reputational damage. If a company is not considered proficient in terms of protecting data and handling inevitable security incidents, the company risks long term or even permanent damage as trust deteriorates.

Digital Trust Is a Multi-faceted Discipline

IT and business executives in the Nordic and Benelux countries expect that in just two years, nearly half the company revenue will be generated by digital products and services[4]. Trust is a key pillar in any business relationship, and in a digital economy, digital trust is paramount.

Digital trust is not a technology or a standalone project that has a clearly defined start and finish but is achieved through ongoing efforts to ensure that customers and business partners perceive your organisation as trustworthy. Establishing the necessary trust includes multiple layers of tools, processes, governance, and communication.

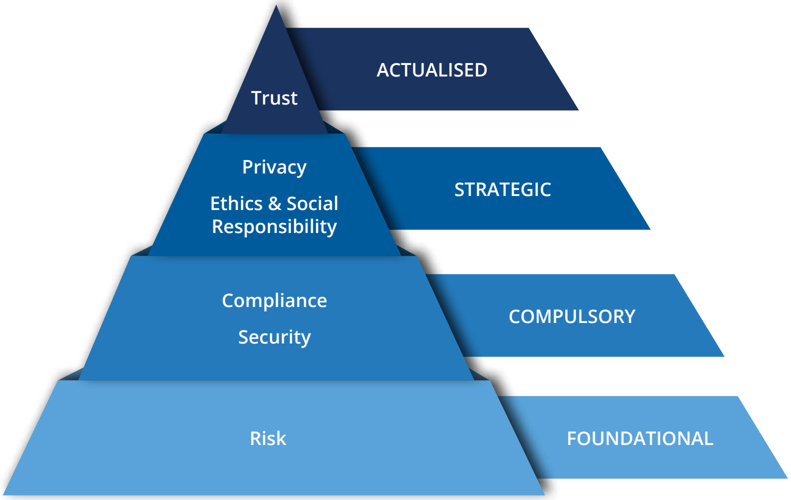
To illustrate this, IDC has developed the pyramid of digital trust which is depicted below. At the foundation is a sound risk assessment that continuously needs to be aligned with the ever-evolving digital business structure and threat landscape.

Layered on top of this is the obligatory IT security environment and the governance and documentation setup ensuring that all data storage and processing complies with legal requirements etc.

However, trust also requires appropriate strategies and mindsets. Customer data in particularly needs to be handled properly. This of course includes meeting privacy regulations, but also utilising the data in manners that customers and other market constituents perceive as being proper.

Neither of these elements can be omitted in the pursuit of digital trust, and it is important to acknowledge IT security in this context. IT security is not merely a necessary cost, a compliance nuisance, or a blocker of innovation. This is recognised by security executives in the Nordic and Benelux areas, where 7 out of 10 emphasise the IT security function as a driver of competitive differentiation or an enabler of business efficiency[5].

IDC's Pyramid of Digital Trust



Source:
The Future of Trust:
Defining Trust

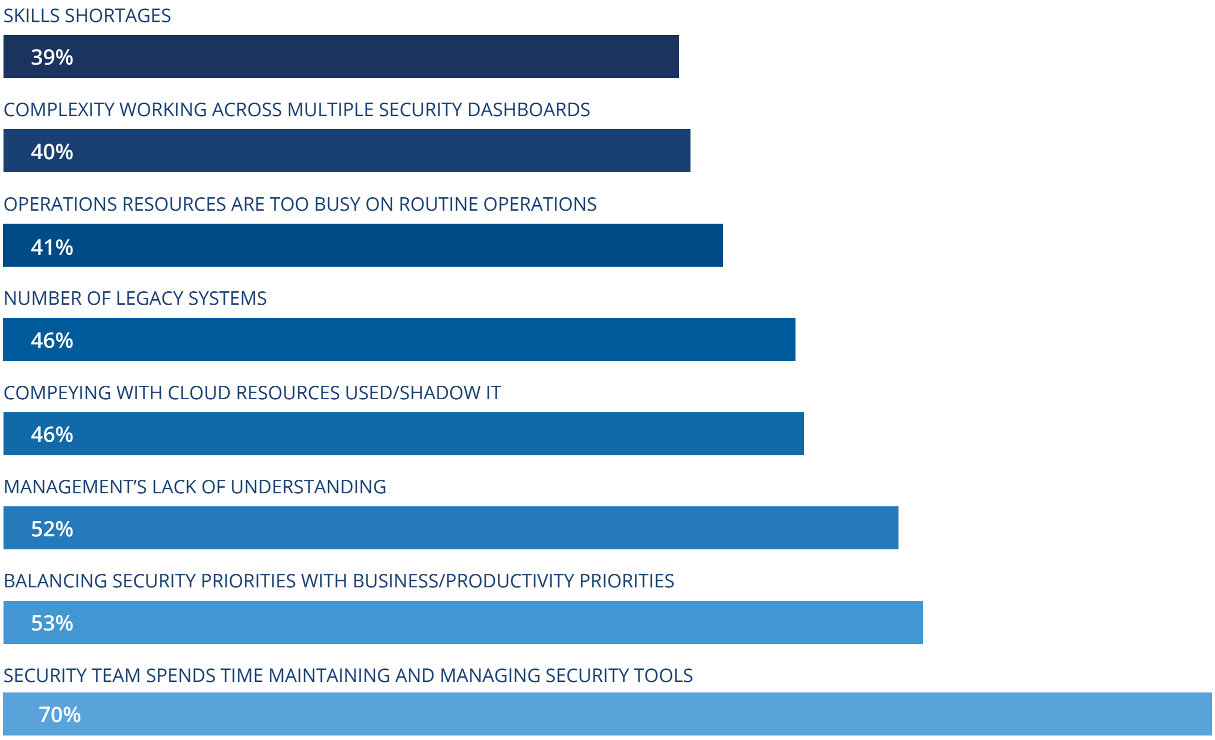
4) Digital Future Reignition Survey, December 2020
5) IDC, European IT Security Survey, June 2020

Business Requirements, Fragmentation, and Lack of Resources Keep Organisations from Improving Their Security Capabilities

Despite the obvious advantages of improving security capabilities, companies struggle. There can sometimes be a priority placed on maintaining and managing the status quo – leaving little room for improvements and changes.

As the survey results shown below confirm, the underlying reasons originate from the complexity of securing a fragmented IT environment where business requirements are constantly changing. In addition, significant security skills shortage in the region means that there is often a lack of resources and skills to implement and manage new security solutions.

Factors limiting Nordic and Benelux organization's ability to improve IT security capabilities



Source: IDC, European IT Security Survey, June 2020 (N = 201)

Overcoming these challenges is difficult and cannot be solved by simply adopting additional tools or implementing more processes. It requires communication, willingness and mandate to address the technology legacy, and to educate and re-skill people in both IT and business benefits.

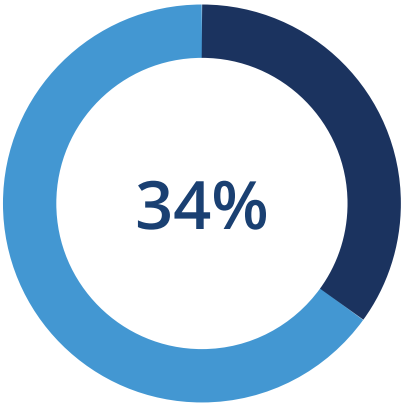
All in all, a completely different approach to IT security must be embraced.

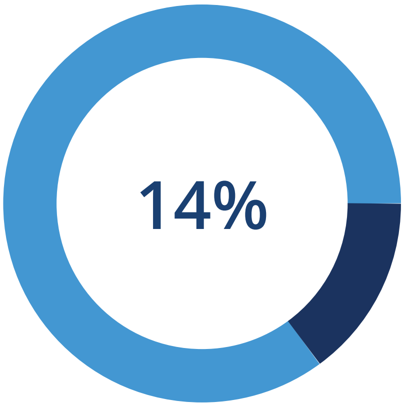
Organisations Need a Different Approach to IT Security

The need for a new approach to IT security is eminent and has been accelerated by the Covid-19 pandemic that has disrupted work processes and fast-tracked digitisation. As shown in the figure below, this is backed by the findings from IDC's Digital Future Reignition survey which finds that every other organisation has either established a digital strategy or accelerated the digital roadmap in the last 12 months.

The Impact of the Covid-19 Pandemic on Digital Transformation Initiatives

"The crisis has acclerated our digital roadmap and future digital plans"





"The crisis has forced us to develop a digital strategy to keep our operations running"

Source: Digital Future Reignition Survey, December 2020

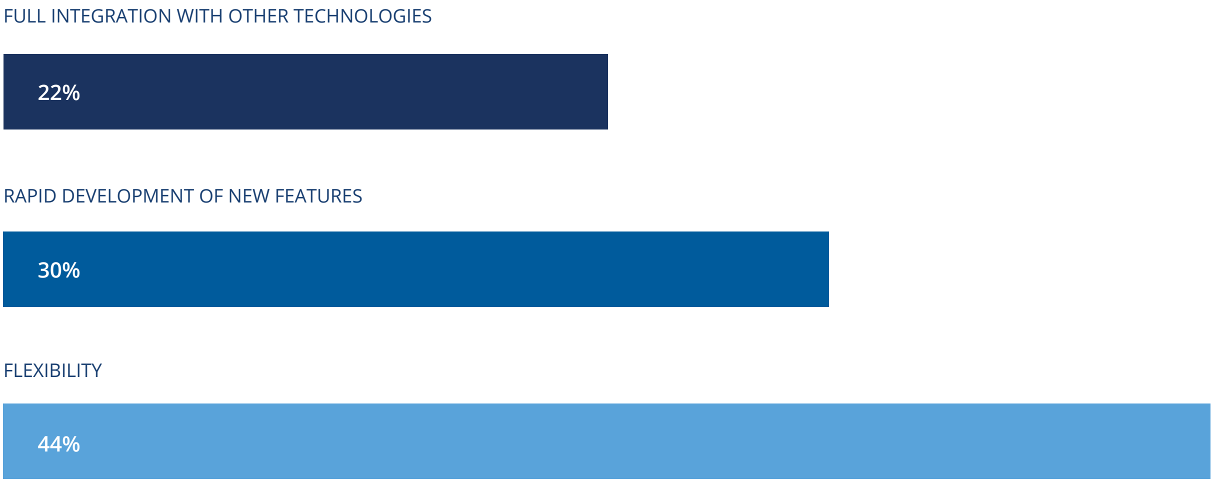
This acceleration to a digital first strategy combined with the technological evolution not only means that IT security must be addressed differently it also brings new possibilities for how IT security can drive overall cost savings, increase efficiency, and propel competitive differentiation.

The IT security framework cannot be changed overnight, but organisations need to start the transformation journey and not wait for individual parts of today's fragmented setup to fail. When defining the new structure, criteria like flexibility, agility, and user experiences need to be in focus, with technologies like cloud, APIs, Privilege Access Management and software defined secure access forming the foundation.

IT Security Must Address the Business Requirements of Tomorrow

A modern IT security setup is incomparable with the traditional "castle and moat" perimeter protection, as applications and data need to be made available to users with multiple devices and at various locations. The exact format varies depending on industry and business processes but there are some commonalities that reflect the overall technology investment drivers shown in the chart below.

Main drivers of technology investments in 2021



Source: Digital Future Reignition Survey, December 2020

Flexibility

As the chart shows, the need for flexibility is the number one driver of technology investments, and evidently this is also a mantra in IT security investments. As business models are digitised, and work processes evolve, there is a need for a flexible IT environment. This applies to much more than just an infrastructure that can scale up and down, and the ability to shift workloads between resources.

There is a need to change employees' access to data and applications – including for short-term and project-based employed – depending on need. The process of granting credentials when employees are hired and evoking them when they leave is a big task in many organisations. As cross-departmental collaboration increases and skills are sourced in new ways, managing credentials becomes even more complex. If a security solution consists of multiple point solutions that do not have the ability to dynamically adapt privileges, collaboration is impeded and access to skills more difficult.

Agility

Furthermore, the chart reveals that the second most reported IT investment driver is the need for fast development of new features, so the security framework must support tools and processes for agile methodologies etc. In addition to this the security solution itself must be fast to deploy from the perspective of initial implementation, ongoing maintenance and expansion, and deployment of new features.

An increasingly important element in ensuring business and IT agility is automation and the need for it to be able to be deployed in a growing number of use cases, as solutions become more intelligent.

User Experience

As previously mentioned, there is a perception that security and productivity are in conflict. As a result IT solutions often end up with a compromise in one area. Security may be compromised, in which instance users either circumvent the security measures, find alternative tools to accomplish the task at hand, or postpone or even skip the task completely.

Customer experience has been a priority in businesses in years, but more recently, internal user experiences has grown in importance for both productivity and employee retention reasons. However, this must be considered from an IT security perspective. It is paramount that security is as unintrusive as possible. Ideally it should be invisible to the user and certainly not cause additional steps in a process, affect performance, or restrict the user from working efficiently.

Zero Trust

It is generally acknowledged that the “moat and castle” model does not work today, as you need to allow continuous access to the systems on the inside. However, in many organisations we still find a legacy from the model and once inside, you are generally considered trustworthy and are free to roam around the castle. That means, if the network protection is breached, it is relatively easy for cyber criminals to access multiple systems.

Zero Trust on the other hand, assumes all connections are malicious unless predefined as secure and authenticated. This is a change in mindset, but it also necessitates the adoption of new technologies – including advanced authentication, risk modeling, network segmentation, and least privilege access.

Segmentation

When building and managing a security architecture, segmentation is essential when considering both systems and endpoints. Categorising the endpoints – IoT sensors as well as computing devices used by human beings – allows for granular control without having to manage privileges for individual users and devices. Micro segmentation on the other hand, is about dividing the datacentre into different logical zones that are independently protected through IT security policies.

New Technologies Are Needed to Deliver on the Criteria

A new approach to IT security must be accompanied by adopting new technologies. Depending on the existing security setup there are many relevant different new technologies available. However, some of the most common ones are:

CLOUD

While cloud security remains a key priority, the overall perception of cloud and security has changed. Traditionally, cloud was perceived as less secure than an on-premises datacentre, but today companies often adopt cloud to improve security.

Purchasing and consuming security as a cloud service is also becoming more prevalent. Just 3 years ago, only 20% of security software was delivered as a cloud service. Today, the same figure is 35% and in 3 years, the share will approach 50%[6].

SOFTWARE-DEFINED SECURE ACCESS

One of the key technologies underpinning a flexible security framework is software defined secure access. The migration to SDSA provides the opportunity to implement a fine-grained application-specific and identity-based approach to remote access and support the Zero Trust and segmented security methodology.

The adoption is driven by short comings of traditional VPN solutions as predicted in IDCs Future Scape for Digital Trust:

IDC Worldwide Future of Trust 2021 Prediction #1:

By 2022, budgets for modern software-defined secure access solutions will quadruple as flaws in legacy vpn remote access solutions are illuminated by the massive work-from-home migration.

[6] *IDC Semiannual Public Cloud Services Tracker, November 2020*

IDENTITY AND DIGITAL TRUST

One of the fastest growing segments in the IT security market is identity and digital trust software. The growing demand is fuelled by the need to manage users, identities, and access, which is a top priority for 28% of security executives in Nordic and Benelux organisations.

Digital transformation, the shift to cloud, application proliferation, and workforce enablement are all rendering legacy identity and access management solutions increasingly inadequate while demand for privileged access management solutions in particular is growing[7].

ECOSYSTEM INTEGRATION

Propelled by a desire to fight complexity and consolidate and integrate the individual security solutions to a holistic structure, there is a need to improve integration. The means to achieve this, is through the adoption of unified ecosystems and platforms.

IDC Worldwide Future of Trust 2021 Prediction #2:

By 2023, to reduce security complexity faced by limited staff, 55% of enterprise security investments will be on unified ecosystem and platform frameworks.

[7] *European Identity and Digital Trust Forecast, 2020-2024*

Key Takeaways

A Structured Approach is Needed

All in all, there are numerous elements that need to be considered when transforming the security setup for tomorrows digital first business environment. It is not an easy task, but with a structured approach, an openness towards new technologies, and a focus on limiting user access and privileges to the relevant data and applications needed, while protecting a good user experience, it is possible to build the foundation for the digital trust needed to succeed.

Specifically, IDC recommends:

- Assess your current and expected business setting and align the risk assessment and security roadmap with your digital business journey.
- Acknowledge that IT security is the foundation for digital trust and can contribute positively to the business performance.
- Embrace new approaches and technologies to ensure flexibility, agility, user experiences and integration – for example through Zero Trust, Software Defined Secure Access and Privilege Access Management.

About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com

BeyondTrust

EXECUTIVE BRIEF

IDC

ANALYZE THE FUTURE

About IDC Nordic

Bredgade 23A, 3.
DK-1260 Copenhagen K
nordic.idc.com

Copyright and Restrictions

This publication was produced by IDC Nordic. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC.