

# Transforming security

Five steps to secure digital transformation



```
modifier_
set mirror object to mir
mirror_mod.mirror_obje
operation == "MIRROR_X
mirror_mod.use_x = Tru
mirror_mod.use_y = Fal
mirror_mod.use_z = Fal
operation == "MIRROR
mirror_mod.use_x = Fal
mirror_mod.use_y = Tru
mirror_mod.use_z = Fal
operation == "MIRROR
mirror_mod.use_x = Fal
mirror_mod.use_y = Fal
mirror_mod.use_z = Tru

#selection at the end
mirror_ob.select= 1
modifier_ob.select=1
context.scene.objects.
("Selected" + str(mod
mirror_ob.select = 0
= bpy.context.selecte
.data.objects[one.name
print("please select e
-- OPERATOR CLASSES

types.Operator):
X mirror to the se
object.mirror_mirror_
mirror X"

context):
context.active_object i
```

# Could cyberattacks derail your digital transformation journey?

While companies are embracing digital transformation to drive fundamental improvements to business outcomes, cybercriminals are aiming for the underbelly, where new security risks are emerging through the rapid adoption of digital technologies.

Not only is today's digital environment more complex than ever and, hence, more difficult to secure, transformation is expanding the attack surface — giving attackers more targets from which to choose.

In this context, cyberattacks continue to escalate in scale, scope and sophistication. According to the 2019 Cyberthreat Defense Report from CyberEdge Group, nearly eight out of 10 organizations (78 percent) were victims of at least one successful cyberattack in 2018. Even more alarmingly, more than 50 percent of those organizations were victimized by ransomware, with 45 percent actually paying the ransom to recover their data, while 19 percent refused to pay and lost their data.

There is a way, however, for organizations to avoid becoming cyberattack victims on their digital transformation journey. They need to make a parallel journey, one that integrates security and risk governance into the digital core foundation that is the basis for transformation.

Highlighting some of the top insights from the Cyberthreat Defense Report, this ebook outlines how enterprises can address omnipresent cybersecurity challenges and achieve a secure digital core platform — one that protects their businesses against data breaches, ransomware attacks, distributed denial of service attacks, and other potentially devastating critical threats that can derail the transformation journey.

## Protecting the digital transformation journey

**1**

Improve the security posture of your digital core

**2**

Build security into the software development life cycle

**3**

Gain deeper insight into threats

**4**

Automate incident response and other security workflows with threat intelligence

**5**

Address industry-specific security and compliance requirements

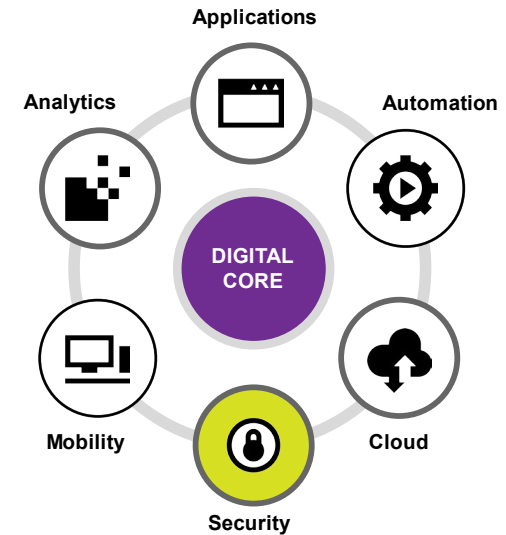
# 1 Improve the security posture of your digital core

Malware, spear phishing and ransomware top the list of cyberthreat concerns for IT security professionals and decision makers. While malware is responsible for some of the largest data breaches to date — including Marriott Starwood hotels (500 million records), Under Armour (150 million records), Google+ (52.5 million records), Panera (37 million records) and Facebook (30 million records) — ransomware is also on the rise.

Any of these threats can bring your digital transformation progress to a standstill, with significant financial and reputational risk to your business.

The secret to protecting your digital transformation success is starting with a secure digital core. A digital core is a secure and scalable cloud platform that enables the rapid development of applications and microservices, incorporating analytics and automation to deliver business model innovation, new customer experiences and optimized business processes.

Your parallel security journey must begin with a security platform within your digital core that creates resilient systems that can not only withstand cyberattacks, but also carry out mission-critical business operations after an attack.



## Essential capabilities for a secure digital core platform

DXC Technology and Micro Focus together deliver essential security capabilities to the digital core platform, including:



Visibility into enterprise defenses and compliance



Alignment with business risks



Support for informed decision making



Automated orchestration and response



Flexibility to transform with your business

## 2 Build security into the software development life cycle

Just as rapid, secure and modular code development (think microservices) can help drive digital transformation, insecure code can add risk and ultimately undermine digital transformation efforts. Yet, application development and testing is the IT security process that organizations around the world struggle with the most.

One reason they may be struggling is that they can no longer rely on bolted-on security at the end of development — not in a DevOps world with continuous integration/continuous delivery as a central tenet. Instead, enterprises need to integrate security and risk management throughout the development life cycle.

The best way to do that is with a comprehensive DevSecOps model for secure digital transformation. DevSecOps supports faster release schedules and innovation while applying security policies and procedures at each stage of the development process. This model bolsters cyber resilience while reducing friction during accelerated software development.

## A strong DevSecOps model

DXC Technology and Micro Focus can help you develop a secure software development life cycle and move to a robust DevSecOps approach to digital transformation by:

- Embedding security procedures and policies into the continuous integration and delivery pipeline, including testing as a service embedded into every stage of the software development life cycle
- Deploying automation, frameworks, and strong policy and governance to align the three groups: development, security and operations

# 3 Gain deeper insight into threats

Every year since 2016, IT security leaders and practitioners have reported that too much data to analyze was one of three top obstacles to achieving effective cyberthreat defenses. In 2019, the data tsunami problem hit the number one spot.

Security analytics can help enterprise security teams “cut through the noise” of enormous amounts of data by applying sophisticated algorithms and analysis techniques to the security data available in their environments. That’s a compelling reason why advanced security analytics topped 2019’s most-wanted list for all technologies, with user and entity

behavior analytics (UEBA), full-packet capture and analysis, and threat intelligence services following close behind.

An essential component of any digital core security platform is deep analytics that leverage machine learning (ML) and artificial intelligence (AI) to efficiently process data, uncover threats and reduce the frequency of false positives. In the Cyberthreat Defense Report, 81 percent of respondents generally agree that ML and AI technologies are helping to defeat advanced cyberthreats.



## Proven services and technology for taming the data deluge

DXC Technology and Micro Focus can complement the knowledge and resources of your current security team with third-party forensic and analytical skills and technology to help you contend with known and unknown threats:

- **Advisory services** can help you improve security operations, threat intelligence, incident response and forensic analysis.
- **Managed SIEM services** give you a holistic view of your security posture, identify security threats and ensure a risk-prioritized approach.
- **Intelligent Security Operations** include monitoring, threat intelligence, incident response and forensic expertise to mitigate breaches and help you fully understand the threats you face.



# 4 Automate incident response and other security workflows with threat intelligence

IT security practitioners report that the second biggest obstacle to effective cyberthreat defenses is the lack of skilled security personnel. Numerous studies highlight the growing security talent gap. The 2019 Cyberthreat Defense Report shows that 84.2 percent of organizations are experiencing an IT security skills shortage.

While the talent shortage is a significant barrier on its own and limits effective response and remediation, silos and manual efforts exacerbate the problem. Minimal integration and lack of automation between silos create slower response through manual hand-offs, especially between security and IT.




To do more, faster and more effectively, enterprises are increasingly turning to security orchestration, automation, and response (SOAR) solutions. These capabilities, integrated into a digital core security platform, can automate security tasks, processes and workflows to improve response time, accuracy and standardization. DXC Technology and Micro Focus can help you achieve these benefits.

## Automation, analytics and processes

The DXC Security Platform is supported by Platform DXC™ — a next-generation service delivery platform. The platform includes leading-edge technologies from DXC partner Micro Focus and incorporates DXC Bionix™, which brings the pillars of intelligence, orchestration and automation to elevate the security posture and bridge traditional IT boundaries, the area where most digital initiatives fail.

# 5 Address industry-specific security and compliance requirements

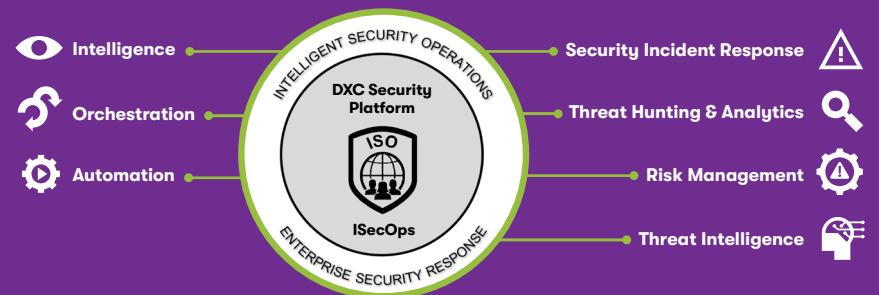
In addition to the cyberthreat challenges and concerns that every industry faces, each sector has unique issues and compliance requirements it must address while digitally transforming its business. Here are examples of three industries and their unique security and compliance challenges.

Digital transformation		Security transformation
 <b>Healthcare</b>	<p>A digital health platform enables healthcare providers to provide better integrated patient care and improve patient outcomes through interoperability between disparate environments, integrating data when and where it's needed across the healthcare system.</p>	<p>This new digital health platform must be secure, tapping into automation, intelligence, security technologies and analytics to protect patient privacy in accordance with standards such as HIPAA and protect the organization from cyberthreats.</p>
 <b>Transportation</b>	<p>Connected transportation is creating new opportunities for personal travel discovery and enrichment, as well as the efficient movement and tracking of goods. A connected transportation platform enables companies to look across a chain of travel events for an individual passenger or package to identify problems, predict the impact, and automatically develop and execute solutions that keep travelers and freight moving.</p>	<p>Every element of a connected travel or transportation journey must be protected by ubiquitous, software-defined, secure digital networks and supported by a secure digital core platform that protects the movement of people and goods from cyberthreats.</p>
 <b>Manufacturing</b>	<p>The fourth industrial revolution, known as Industry 4.0, refers to improved automation, machine-to-machine and human-to-machine communication, AI, technological improvements and digitization in manufacturing. For example, manufacturers are implementing more automation in their plants (operational technology) to improve production throughput and quality and reduce operating costs.</p>	<p>The convergence of operational technology (OT) and IT is driving manufacturing organizations to develop a holistic and harmonized approach to security, with security built into the digital core platform at the center of this strategy.</p>

## Secure industry platforms

The DXC Security Platform enables secure delivery of industry-specific platforms and solutions like the Digital Health Platform and the Connected Transportation Platform. These platforms bring together microservices that enable new experiences across a connected ecosystem of partners, with security built into the platform and microservices.

Regardless of the industry sector, DXC Technology and its partner Micro Focus can help you achieve your digital transformation goals faster, with less risk.



# Next steps

Together, DXC and Micro Focus help organizations worldwide transform their IT and business processes to reap the benefits of a secure, productive and profitable digital future.

**Learn more at [www.dxc.technology/microfocus](http://www.dxc.technology/microfocus).**

## About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to provide services across the Enterprise Technology Stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at [www.dxc.technology](http://www.dxc.technology).

## About Micro Focus

Micro Focus is one of the world's largest enterprise software providers, delivering mission-critical technology to more than 40,000 customers around the globe. With a broad portfolio underpinned by a deep inventory of advanced analytics, the company helps customers run and transform their business. This enables them to adapt to evolving market conditions and effectively compete in the digital economy over the long term. Micro Focus does this by delivering solutions that bridge the gap between existing and emerging technologies to protect IT investments. That is High Tech, Low Drama.

The source for all cyberthreat statistics and trends in this ebook is: "2019 Cyberthreat Defense Report," CyberEdge Group, LLC.

