DXC.technology | MICRO FOCUS

Be the Disrupter, Not the Disrupted

Overcome the security challenges of digital transformation

On the journey to digitally transform your business, don't forget the essentials: enterprise security and risk management. After all, disrupting the status quo with better business outcomes requires not falling prey to disruptions from cyberthreats such as ransomware and data breaches. Read on for the top challenges in cyberthreat defense and how you can overcome them.

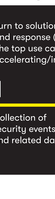
1 Too much data

IT security leaders and practitioners say the data tsunami is their top obstacle to achieving effective cyberthreat defenses.

#1 obstacle
Too much data to analyze

What you can do

Deploy security analytics with machine learning (ML) and artificial intelligence (AI) to efficiently process data, uncover threats and reduce the frequency of false positives.



81% agree:
ML and AI help detect advanced cyberthreats

#1 security management/operations technology planned for acquisition:
Advanced security analytics

2 Scarcity of security talent

What's the second biggest obstacle to effective cyberthreat defenses? The lack of skilled personnel.

84.2% of organizations
are experiencing an IT security skills shortage

What you can do

Turn to solutions such as security orchestration, automation and response (SOAR) to do more, faster and more accurately. The top use cases for SOAR in organizations include accelerating/improving:

1
Collection of security events and related data

2
Investigation and validation of security events

3
Prioritization of confirmed incidents

3 Lack of cloud security skills

The most frequently-used strategies for addressing cloud security needs focus on attaining new skills:

Augment staff with external consultants/ contractors

Educate/train existing IT staff on cloud security

Hire new staff dedicated to cloud security

What you can do

Integrate security and risk management into the development life cycle, including continuous integration and delivery processes. Engage experts like DXC Technology to supplement your inhouse cloud security skills.

4 The shift to new application architectures

As organizations move to microservices-based application architectures and external application services, they need to focus on securing access to protect sensitive data and the applications that rely on them. However, the IT security process that organizations struggle with the most is:

Application development and testing (SDLC)

What you can do

Make sure that your security strategy and technologies can flex as the business transforms and moves to more modern application environments. Seek out the appropriate technologies for modern applications that rely on application programming interfaces (APIs):

39% plan to acquire
an API gateway

6% year-over-year gain
in current deployment of API gateways

5 Too many successful cyberattacks

Cyberattacks continue unabated, with nearly eight out of 10 organizations being victims of at least one successful cyberattack in 2018.

78% of organizations
were cyberattack victims

What you can do

1
Create both a digital transformation and an enterprise security roadmap

2
Reengineer processes to enforce proactive security

3
Ensure you invest in the right software

4
Get help from experts

9 out of 10 organizations
turn to managed security service providers to pick up at least part of the workload

What's your strategy?

In parallel to your digital transformation journey, you should embark on a security transformation journey. For your roadmap, you'll need a strategy that addresses the people, processes and technology requirements to manage risk across the enterprise, including key capabilities such as:

Threat hunting and analytics

Threat intelligence

Security incident response

Automation

Download the full report at www.dxc.technology/cdr2019

Data source: 2019 Cyberthreat Defense Report, CyberEdge Group, LLC.