FORTINET

2018 SECURITY IMPLICATIONS OF DIGITAL TRANSFORMATION REPORT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Fortinet's 2018 Security Implications of Digital Transformation Survey looks at the state of cybersecurity in organizations around the world from the lens of digital transformation (DX). Three hundred responses from CISOs and CSOs at large organizations helped us identify several current trends:

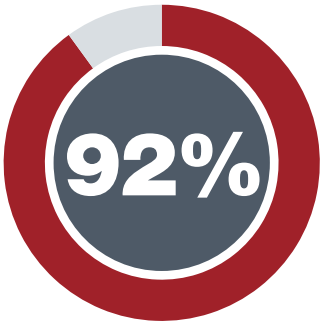
- Digital transformation is the most impactful IT trend on businesses today, with **92%** responding that it has a large impact today.
- Security is by far the biggest challenge to DX efforts, with **85%** of respondents saying it has a large impact.
- The typical organization saw **four attacks** that resulted in data loss, outages, or compliance events over two years.
- Many companies have automated some of their security procedures, but they are even further behind with other security best practices.
- Big chunks of infrastructure remain vulnerable in the typical organization, with **25%** of the infrastructure not adequately protected at the typical organization.

Looking more deeply into the data, we identified a subset of **"top-tier" organizations** that have not suffered a damaging attack in the past two years. Comparing these organizations' security practices with those from "bottom-tier" organizations, we found they are more likely to follow these practices:

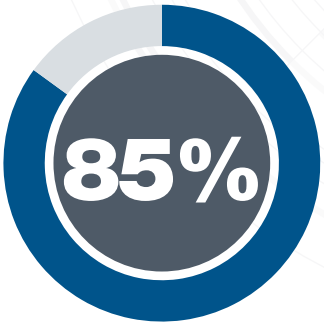
1. Integrate systems to create a unified security architecture
2. Share threat intelligence across the organization
3. Ensure safeguards work on all parts of the network
4. Use built-in compliance controls
5. Have end-to-end security visibility
6. Have automated more than half of their security practices

The implications are clear. **Holistic and integrated security strategies** are more effective than siloed, reactive ones. A strategic approach becomes increasingly important as an organization's attack surface increases with the proliferation of Internet of Things (IoT) devices, mobile connectivity, and cloud-based solutions. A comprehensive strategy that unifies IT tools and processes across all parts of the network is necessary for addressing advanced threats such as polymorphic attacks, as well as new vulnerabilities that sneak in because of DevOps. At the same time, integration of security elements is a foundational requisite for an organization seeking to automate workflows and threat-intelligence sharing.

INFOGRAPHIC: KEY FINDINGS



of CISOs say DX has a large impact on business.



of CISOs say that security is a large hurdle for implementing DX. Biggest security threats: polymorphic attacks and DevOps.

Top-tier organizations had **ZERO** attacks that caused damage in 2 years. Bottom-tier organizations had 16!

Top-tier organizations are:

76% more likely to use a unified security architecture approach

38% more likely to share threat intelligence internally

34% more likely to make sure safeguards work everywhere

24% more likely to automate most security practices

INTRODUCTION

WHAT IS DIGITAL TRANSFORMATION?

The concept of DX is a key driver of IT strategy for most organizations today. While the term has a standard abbreviation and is sometimes capitalized when not abbreviated, the definition of the term is less clear than one might expect. But regardless of the strategic and tactical details, the word "transformation" implies an ambitious goal: a fundamental change in the way a company does business using digital technology.

The following are some widely accepted elements of DX:

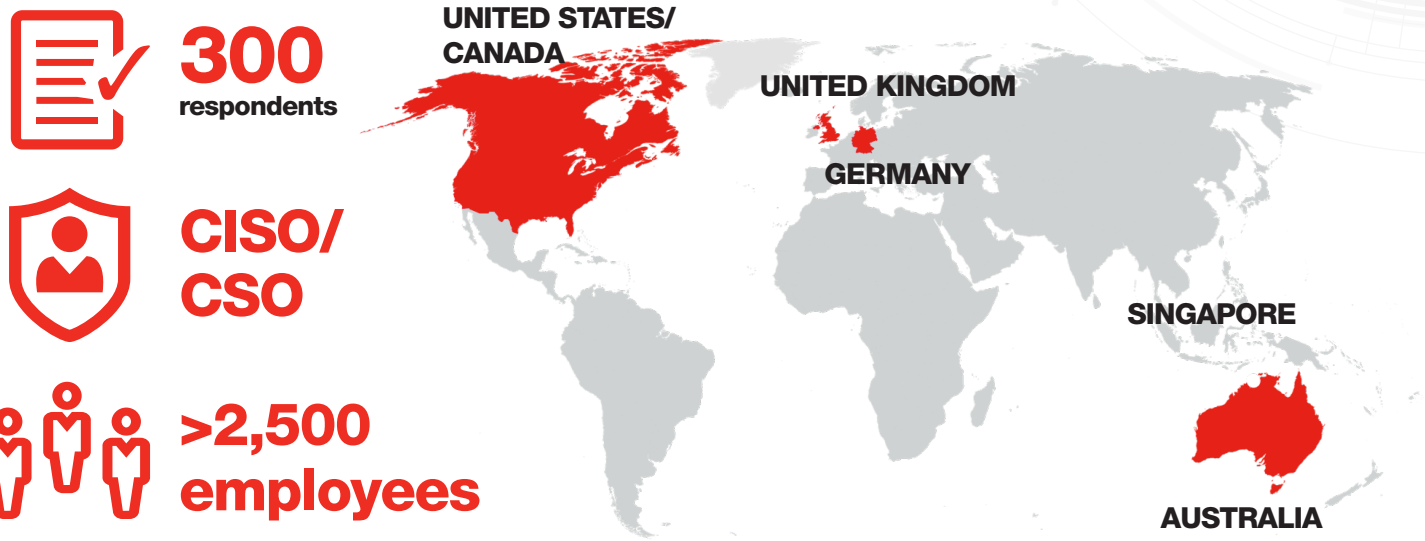
- **It is a journey rather than a product or solution.** The strategy "takes into account that end goals will continue to move as digital transformation de facto is an ongoing journey, as is change and digital innovation."[1]
- **It is customer-focused.** DX often means optimizing customers' online experience and engaging them at a more individual level—which in turn provides valuable insights that can help drive loyalty and additional monetization opportunities. In short, DX "closes the gap between what digital customers already expect and what analog businesses actually deliver."[2]
- **It requires more than just deploying technology.** DX will likely require major changes to internal processes and "a cultural change that requires organizations to continually challenge the status quo, experiment often, and get comfortable with failure."[3]
- **It builds in the ability to make rapid changes.** Companies embrace DX to help them be more agile in a rapidly evolving marketplace, and the DX approach means that "you design items so they can easily change; much of IT's [prior] digitization work has been to prevent change."[4]
- **It is about the convergence of a wide variety of technologies.** "In the digital enterprise, the strategic fusion of former silos (IT, industrial or operations technology [OT], audio-video [AV]) with transformational technologies (cloud, Internet of Things, AI, analytics, edge processing) leads to richer customer experiences, business acceleration, and operational agility."[5]

While the potential of DX is exciting from a business perspective, changes stemming from it can create anxiety for the cybersecurity team and IT organizations in general. Proliferating endpoints, increasingly distributed networks on multiple clouds, and exponentially increasing volumes of data and network traffic all serve to enlarge an organization's attack surface. And the infrastructure and process changes that enable companies to take advantage of the new technologies through DX often add another level of risk. This is perhaps especially true with changes in practice that are meant to speed up a business process such as DevOps.

METHODOLOGY FOR THIS STUDY

For this analysis, we surveyed 300 security leaders from organizations around the world. A few facts about our participants:

- All hold the CISO/CSO role at organizations with >2,500 employees.
- They are geographically distributed across North America, Europe, Asia, and Australia.
- They represent a wide variety of industries—including education, government, financial, retail, healthcare, technology, and energy.



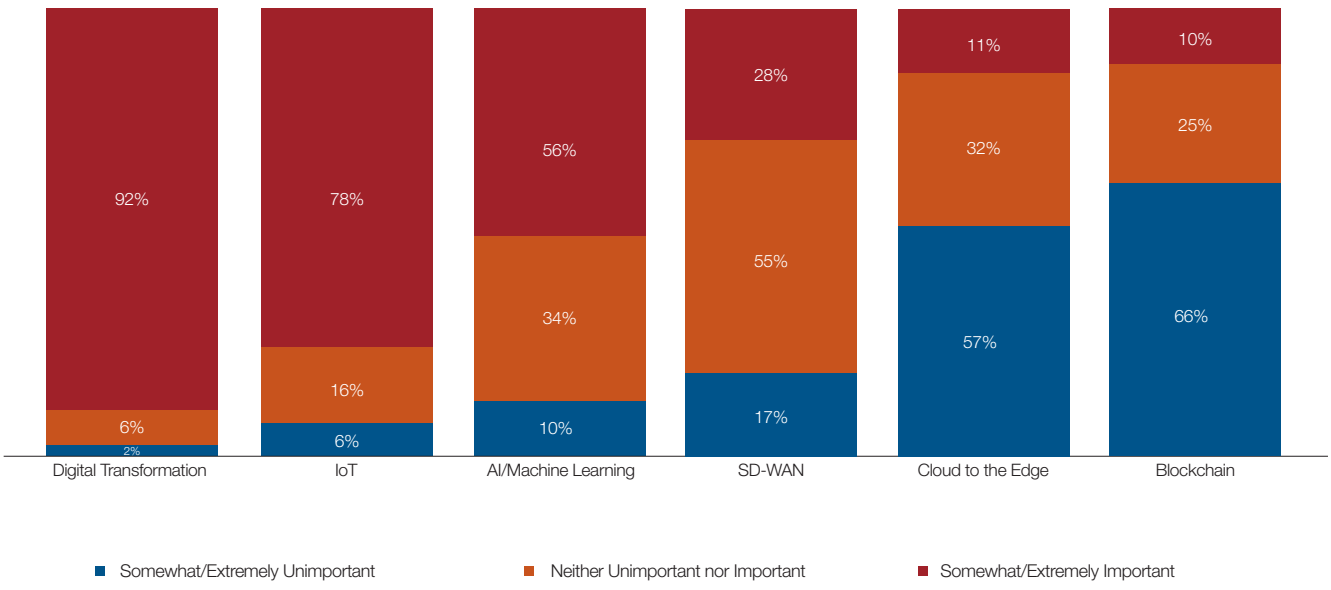
SURVEY PARTICIPANTS

This study utilizes data from the survey to identify a number of current trends around DX, particularly with regard to security. We then delve more deeply into the data to identify a subset of organizations that have not suffered downtime, data loss, or compliance events due to intrusions in the past two years. We then take a look at what these teams are doing differently.

DIGITAL TRANSFORMATION TRENDS

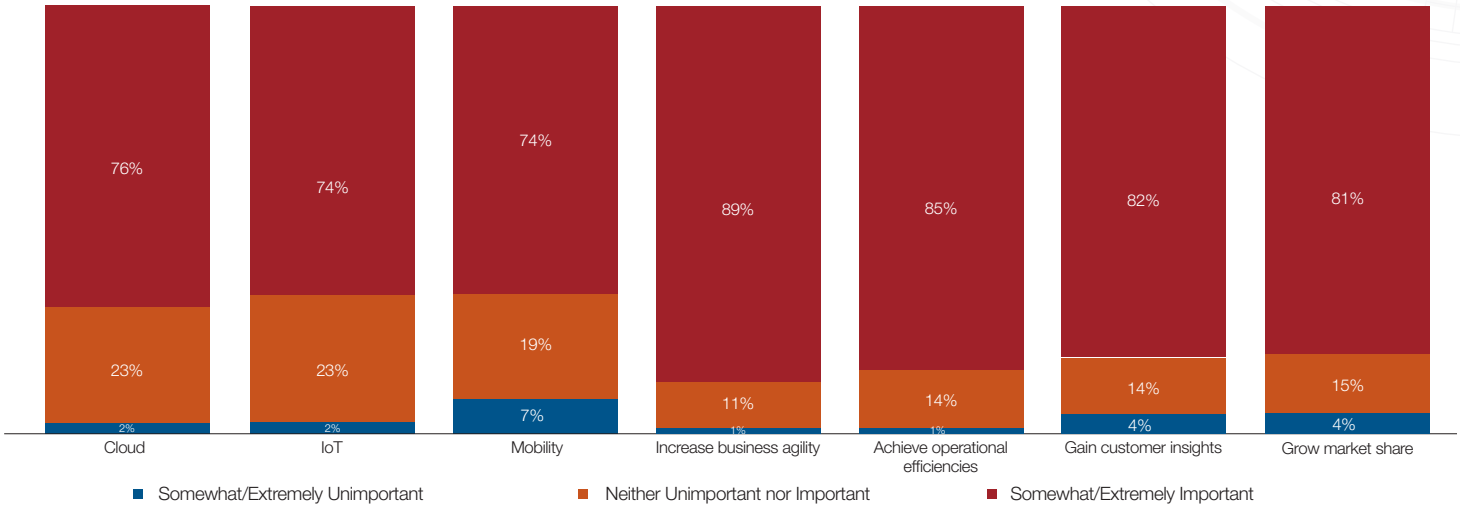
TREND: DIGITAL TRANSFORMATION IS SEEN AS THE MOST IMPACTFUL IT TREND ON BUSINESS

When asked to rate several current IT trends in terms of impact to the business, a remarkable **92%** of respondents rated DX as having a "somewhat large" or "extremely large" effect. Interestingly, the second- and third-highest scores for business impact went to two trends that are often considered to be elements of DX—**the IoT** (78%) and **Artificial Intelligence (AI)/Machine Learning** (56%).



BUSINESS IMPACT OF CURRENT IT TRENDS

Why is DX taking up so much "oxygen"? When asked to rate several potential business drivers on how much impact they had on the decision to pursue DX, respondents list cloud, IoT, and mobility as the most impactful. About **three-quarters** of respondents rate each of these as having a "somewhat large" or "extremely large" impact. This suggests that rather than bringing in these elements as a part of a DX strategy, they already existed (and were likely growing) in many organizations' infrastructure. IT and security leaders seek to maximize their value by defining a strategic framework into which they are plugged. A vast majority of respondents rate increased business agility, operational efficiencies, customer insights, and increased market share as important goals of their DX efforts.

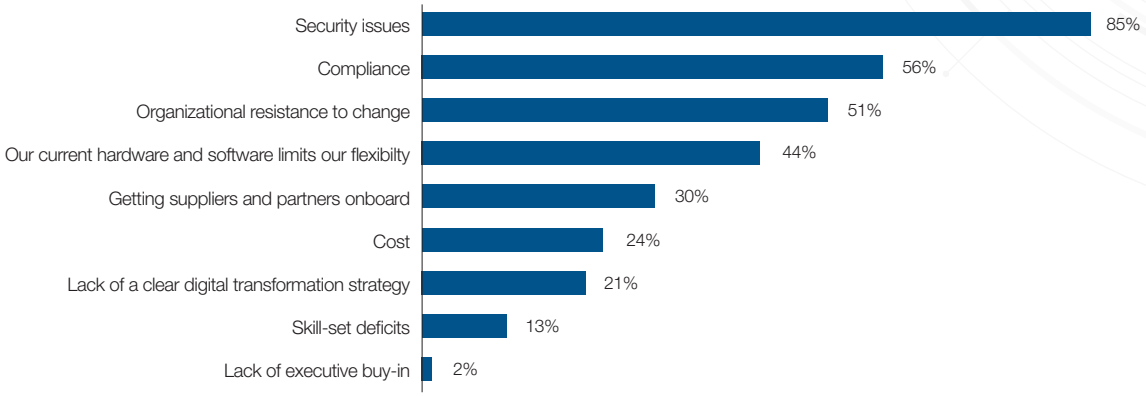


DX DRIVERS AND GOALS

Survey participants are quite optimistic about the progress they have made and are making with regard to DX. **67%** report that their organizations began implementing DX more than a year ago, and **95%** say that they are at least trialing a solution today. While the survey did not delve into the specifics, organizations view themselves as well underway on DX efforts.

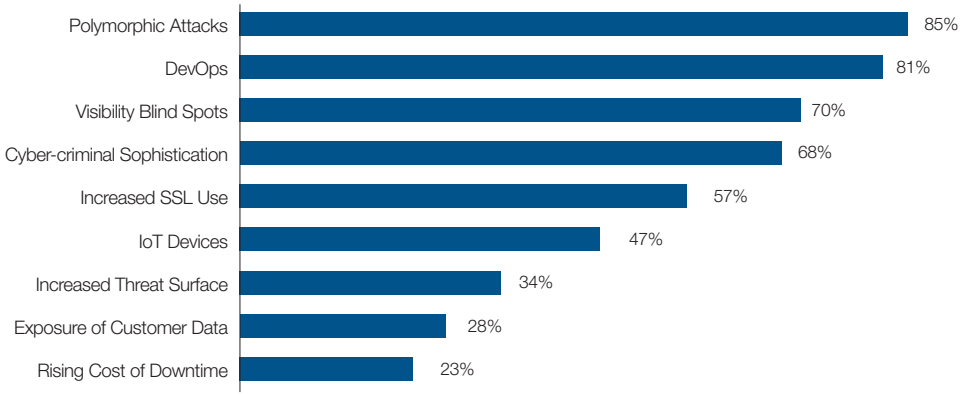
TREND: BY FAR THE BIGGEST CHALLENGE TO DIGITAL TRANSFORMATION EFFORTS IS SECURITY

While many online articles discuss organizational issues and legacy technology limitations as the biggest challenges to DX,[6] our CISO respondents are overwhelmingly clear that **security issues are the biggest barriers** to DX efforts. **85%** rate security issues as having a "somewhat large" or "extremely large" impact. Plus, the second most common answer (56%) is compliance-related.



HOW CHALLENGES IMPACT DX EFFORTS

Two sources of risk are of special concern to CISOs—one external and one internal. The rise of polymorphic attacks—threats that constantly morph or change to avoid detection—ranks as a "somewhat large" or "extremely large" challenge by **85%** of respondents. Not far behind, at **81%**, is the rise of DevOps, which respondents agreed is allowing vulnerabilities to slip in along with the faster pace of development—a trend that is starting to be documented.[7] Both of these threats can potentially intensify as the attack surface becomes more complex in the context of DX.

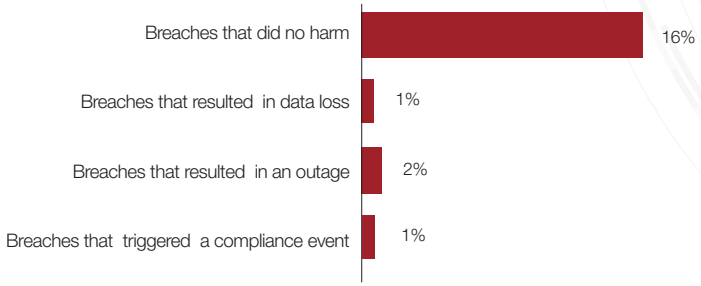


DX EFFECTS WITH SOMEWHAT/EXTREMELY LARGE IMPACT

Another big concern is a **lack of full visibility** for the security team (70%), given the increasingly complex computing framework that DX envisions. Even before DX, the default state of security in today's enterprise involves multiple silos, with on-premises services and multi-cloud deployments with different security tools. A DX strategy may result in an even more complex environment, with even more clouds and a proliferation of IoT devices—many of which were not designed with security in mind.

TREND: THE TYPICAL ORGANIZATION HAS SEEN ATTACKS RESULTING IN DATA LOSS, OUTAGES, OR COMPLIANCE EVENTS IN THE PAST TWO YEARS

The median organization in our survey experienced **20 breaches** in the past 24 months. **Four of these intrusions** resulted in outages, data loss, or compliance events—including two from ransomware and one from a distributed denial-of-service (DDoS) attack.



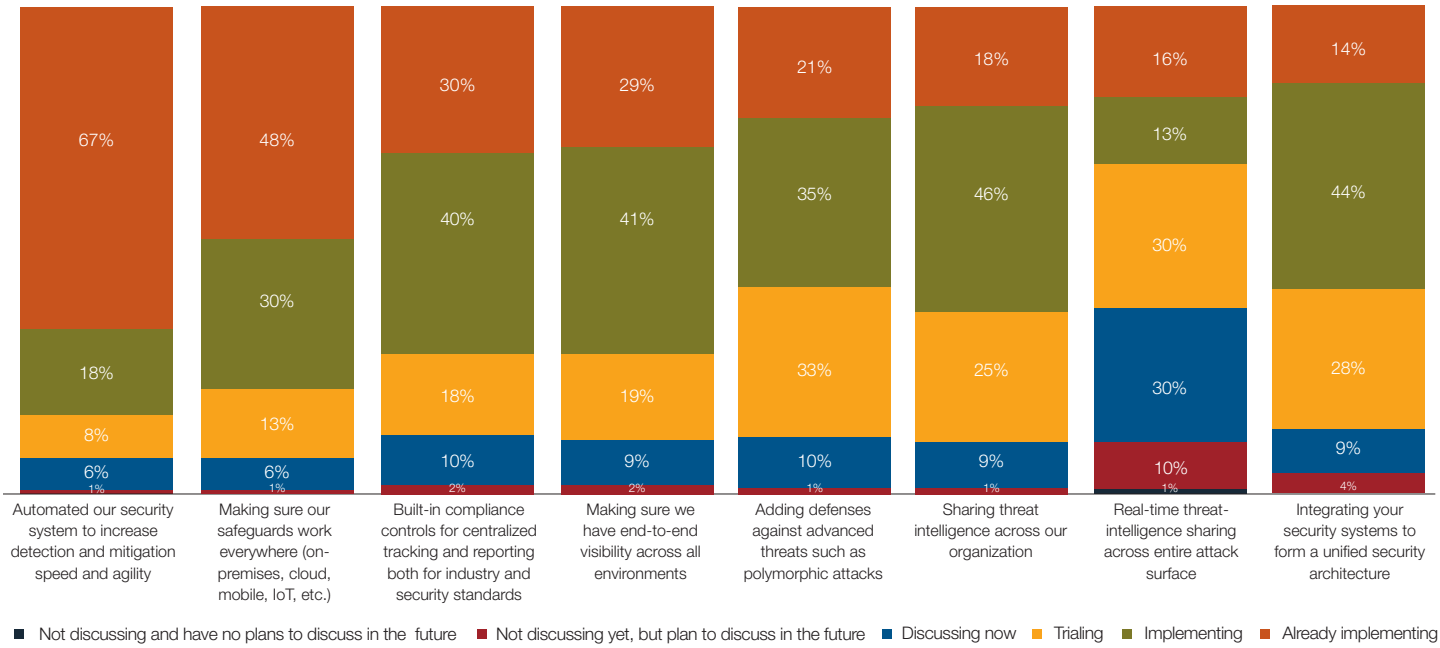
TYPICAL NUMBER OF BREACHES OVER 24 MONTHS

While this result is unsettling, there is also reason for optimism in the result. **One-third** of organizations surveyed had no attacks that caused downtime, data loss, or compliance events in the past two years. We will analyze what these organizations are doing differently in the next section.

TREND: ORGANIZATIONS HAVE AUTOMATED ONLY A PORTION OF THEIR SECURITY PRACTICES AND ARE FURTHER BEHIND ON OTHER SECURITY BEST PRACTICES

Automation means different things to different organizations, and the survey did not define automation to the respondents. While many (two-thirds) indicate they have automated some security practices, **more than half of these processes remain manual at the typical organization**. And that number is likely low, as true automation isn't possible without integration across the entire attack surface and every security element. For example, recent ESG research indicates that while 58% of organizations had deployed some security automation, only 19% had done so extensively.[8]

Nearly half of participants indicate that their safeguards now work across all attack surfaces (on-premises, cloud, mobile, IoT, etc.), and another 30% are deploying solutions that will get them to that point. But in many cases, these solutions likely remain siloed and lack integration.



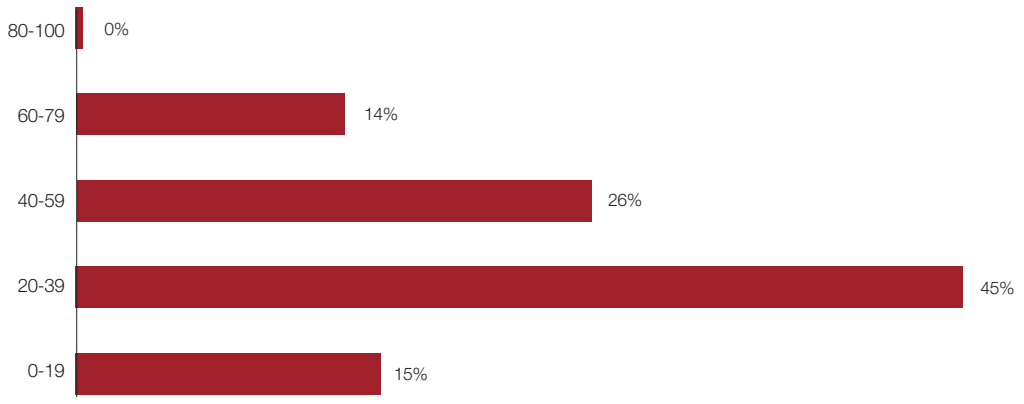
LEVEL OF ENGAGEMENT WITH DX SECURITY PRACTICES

Organizations are less far along in implementing several other security practices referenced in the survey. Projects to integrate security solutions, provide end-to-end visibility, and automate compliance controls are still in progress at **30% to 40% of organizations**, and complete at **fewer than one-third.** The fact that so many are in deployment indicates that organizations are moving quickly in an attempt to stay a step ahead of evolving threats.

TREND: BIG CHUNKS OF INFRASTRUCTURE REMAIN VULNERABLE

The median respondent estimates that **25% of infrastructure** is not protected against today's security threats. As the attack surface expands, legacy security architectures are often unable to scale to meet the new demand. Even if point solutions are deployed to provide some protection, the resulting proliferation of silos means that the organization's overall security profile may not be much improved.

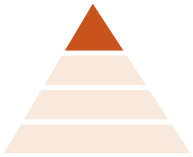
Vulnerabilities that can be resolved with software updates and patching remain a potential issue with some organizations. While almost all the organizations in our survey report that patches are "somewhat up to date," **only one-third** indicate that they are "extremely up to date."



PERCENTAGE OF INFRASTRUCTURE NOT FULLY PROTECTED AGAINST TODAY'S SECURITY THREATS

BEST PRACTICES OF TOP-TIER ENTERPRISES

Delving more deeply into how the respondents are faring with regard to security, we noted a wide range of results with operational metrics. Based on these results, we grouped the results into top and bottom tiers—each of which comprised approximately one-third of respondents. The differences in results between the top and bottom tiers is remarkable:



TOP-TIER ORGANIZATIONS	BOTTOM-TIER ORGANIZATIONS
20%-39% of infrastructure NOT fully protected	**40%-59%** of infrastructure NOT fully protected
11 breaches in 2 years, NO outage, data loss, or compliance event	**56** breaches in 2 years, **16** resulting in outage, data loss, or compliance event
ZERO ransomware attacks	**5** ransomware attacks, **3** resulting in outage, data loss, or compliance event
2 DDoS attacks, NO outage, data loss, or compliance event	**9.5** DDoS attacks, **3** resulting in downtime
56% of CISOs feel secure at their organizations	**33%** of CISOs feel secure at their organizations

Perhaps not surprisingly, top-tier organizations tended to take a more holistic and strategic approach to security. Among our findings:

01

Top-tier organizations are 76% more likely to integrate their security systems to form a unified security architecture.

Taking a strategic approach means breaking down silos and deploying consistent technology and processes across all parts of the network, from IoT endpoints to multi-cloud infrastructures. Top-tier organizations are much further along with this strategy than their counterparts in the bottom tier.

02

Top-tier organizations are 38% more likely to share threat intelligence across their organization.

One result of technology and process silos is that the full breadth of threat intelligence accessible to an organization is not utilized across the infrastructure. The best performers are much more likely to have addressed this issue.

03

Top-tier organizations are 34% more likely to make sure their safeguards work everywhere (on-premises, cloud, IoT, mobile, etc.).

As an organization's attack surface increases along with the proliferation of different kinds of endpoints and cloud-based systems, legacy security tools sometimes do not keep up. Addressing this issue, and ensuring that tools are integrated across the infrastructure, greatly improves an organization's security posture.

04

Top-tier organizations are 24% more likely to build-in compliance controls for centralized tracking and reporting, both for industry and security standards.

Highly regulated industries led the way in adopting automated compliance controls a number of years ago. More recently, other industries have played catch-up in the wake of a flood of new regulations and standards, huge changes to IT infrastructure, and the evolving threat landscape.

05

Top-tier organizations are 20% more likely to have end-to-end visibility across all environments.

End-to-end visibility is virtually impossible with siloed security tools. Without this transparency, organizations simply cannot keep pace with the advanced threat landscape. While the definition of "end-to-end" is rapidly expanding, organizations that are further along in this process are getting the best results.

06

Top-tier organizations are 24% more likely to have automated more than half of their security practices.

The volume of threats seen at most organizations today means that manual monitoring and remediation has moved from being a waste of staff time to being impossible to do. But setting up automation of workflows requires time and testing. The most secure organizations are further along in the automation journey than their less successful counterparts.

CONCLUSION

The core findings from our survey are fairly straightforward. Just to recap:

- DX is the overriding IT trend in the marketplace.
- Security is the biggest barrier to accomplishing it.
- Both internal and external security threats exist, most notably:
  - Polymorphic threats
  - Vulnerabilities introduced via DevOps
- The typical organization is seeing damaging attacks.
- Most companies are scrambling to assemble an adequate security framework that addresses the new computing realities presented by DX.

While these findings certainly give one pause, there are positives when it comes to DX. Despite challenges such as an expanded attack surface, increased complexity in managing all of the moving parts, and an evolving advanced threat landscape, some organizations have been successful in preventing damaging attacks. The key is a **proactive risk management approach** that protects from malicious attacks and breaches. In particular, **organizations that adhere to a few guiding principles are vastly more secure than other organizations**—and have experienced no outages, data loss, or compliance events. These best practices include:

- A security architecture that provides **transparent visibility and centralized controls**.
- A strategy that **uses integration to unlock automation of workflows** and threat-intelligence sharing.
- **Built-in compliance controls** for centralized tracking and reporting—and reduced risk.

[1] "Digital Transformation: Online Guide to Digital Business Transformation," iSCOOP, accessed July 7, 2018, https://www.i-scoop.eu/digital-transformation/.

[2] Greg Verdino, "What Is Digital Transformation, Really?" March 5, 2015, http://www.gregverdino.com/digital-transformation-definition/.

[3] "What is digital transformation?" The Enterprisers Project, accessed July 7, 2018, https://enterprisersproject.com/what-is-digital-transformation.

[4] Galen Gruman, "What digital transformation really means," InfoWorld, June 14, 2016, https://www.infoworld.com/article/3080644/it-management/what-digital-transformation-really-means.html.

[5] Benson Chan "Digital transformation reimagines everything," Strategy of Things, September 7, 2017, https://strategyofthings.io/digital-transformation.

[6] Maarten van Montifoort, "3 Key Barriers to Digital Transformation," COMPAREX, August 12, 2017, https://www.comparex-group.com/web/com/about/press/2017/3-key-barriers-to-digital-transformation.htm#; Jeremy Deaner, "How to Overcome Barriers to Digital Transformation (& Reach Your Customer Engagement Potential)," EngageHub, accessed July 7, 2018, https://engagehub.com/blog/how-to-overcome-barriers-to-digital-transformation.

[7] Cameron McKenzie, "Avoiding the most common DevOps security vulnerabilities in the cloud," TheServerSide, accessed July 7, 2018, https://www.theserverside.com/feature/Avoiding-the-most-common-DevOps-security-vulnerabilities-in-the-cloud.

[8] Jon Oltsik, "Enterprise plans for security automation and orchestration," CSO, January 30, 2018, https://www.csoonline.com/article/3252230/security/enterprise-plans-for-security-automation-and-orchestration.html.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

July 20, 2018 9:20 AM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:Report-CISO-Digital-Transformation-Survey:report-ciso-digital-transformation-survey