

Why Successful Data Transformation Demands a

ZERO TRUST

Security Model

DIGITAL TRANSFORMATION REQUIRES ENTERPRISE SECURITY AND NETWORK EVOLUTION.

USERS AND DEVICES, AS WELL AS APPLICATIONS AND DATA, ARE MOVING OUTSIDE THE TRADITIONAL ENTERPRISE PERIMETER AND ZONE OF CONTROL.

40.8%

More than 40.8% of companies have 21 – 40% remote employees. 25.7% have more than 40% remote employees.¹



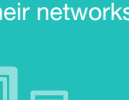
67%

More than 67% of workers use their own devices at work.²



80%

80% of all BYOD is completely unmanaged.³



50%

Enterprises are running cloud-based apps nearly 50% of the time.⁴



10%

Fewer than 10% of all organizations report they have complete awareness of what devices access their networks.⁵



NEW BUSINESS PROCESSES DRIVEN BY DIGITAL TRANSFORMATION INCREASE THE ATTACK SURFACE.

63%

of all data breaches are the result of third parties.⁶



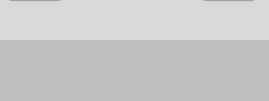
390,000

new malicious programs are registered every day.⁷



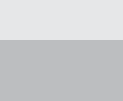
1/3

of mobile devices have a medium to high risk of data exposure.⁸



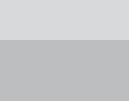
40,000,000

The number of malicious installation packages found striking mobile devices more than tripled in 2016, resulting in almost 40 million attacks.⁹



3.5x

Mobile ransomware volume rose 3.5x in the first few months of 2017.¹⁰



“TRUST BUT VERIFY” IS NO LONGER AN OPTION AS THREATS ARE MOVING INSIDE THE PERIMETER.

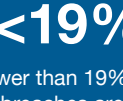
>40%

of breaches originate with authorized users accessing unauthorized systems.¹¹



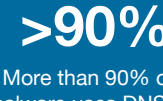
70%

of organizations have had a security incident that negatively impacted their business in the past year.¹²



3x

The number of ransomware attacks on businesses tripled last year, jumping from one attack every two minutes in Q1 to one every 40 seconds by Q3.¹³



4.3x

There were 4.3x more new ransomware variants in Q1 2017 than in Q1 2016.¹⁴



<19%

Fewer than 19% of breaches are self-detected.¹⁵

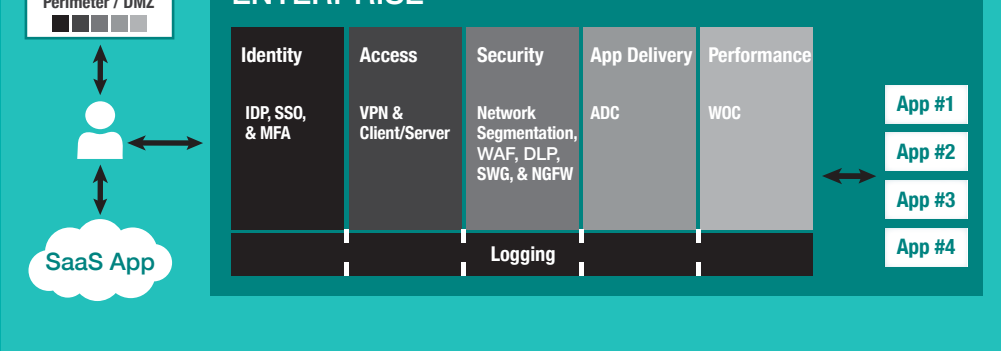


>90%

More than 90% of malware uses DNS to move within an enterprise.¹⁶



TRADITIONAL PERIMETERS ARE COMPLEX, INCREASE RISK, AND ARE NO LONGER CONDUCTIVE WITH TODAY'S BUSINESS MODELS.



75% of enterprises touch up to 14 network and app components.¹⁷

EXPECTATION

INSIDE = TRUSTED



- Users & apps inside
- Trust but verify
- Full-network access

REALITY

THERE IS NO INSIDE...



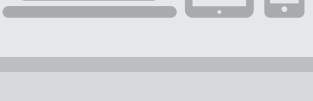
- Users & apps anywhere
- Verify & never trust
- Application-level access

41% of IT professionals rank complexity of architecture/integration issues as the largest concern.¹⁸

THE NUMBER AND TYPES OF DEVICES ON A CORPORATE NETWORK ARE PROLIFERATING AND THE DELINEATION BETWEEN ON- AND OFF-NETWORK IS NO LONGER HARD AND FAST.

20.4 BILLION

Gartner predicts 20.4 billion+ IoT devices will be installed by 2020.¹⁹



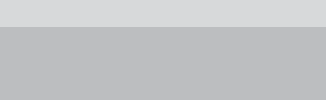
80%

of IoT & 71% of mobile apps are not tested for security vulnerabilities.²⁰

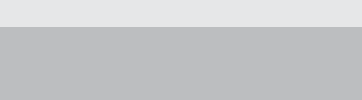


90%

of people have a mobile device within reach.²¹



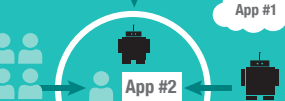
Should you trust this device on your network? Look where it can go in a week.



IT'S TIME TO ADOPT A CLOUD PERIMETER

Leverage a zero trust security and delivery model for successful digital transformation.

- Don't distinguish between external and internal
- Everything is external, just like on the Internet



- Verify everything, trust nothing
- Only deliver applications and data to authenticated and authorized users and devices



- Always verify with full logging and behavioral analytics
- Visibility is vital, need to understand what constitutes “normal”



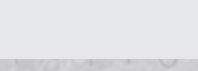
How Can IBM® Edge Delivery Services Help?

IBM Edge Delivery Services, powered by Akamai, has built the world's most secure, reliable, scalable, and high-performing platform to help you navigate today's untrustworthy and risk-laden ecosystem.

[Learn More](#)

SOURCES

1. IDC InfoBrief, Sponsored by Akamai, Remote Access and Security, September 2017
2. CBS Money <https://www.cbsnews.com/news/byod-alert-confidential-data-on-personal-devices>
3. <https://www.securedgenetworks.com/blog/topic/strategy>
4. <https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/louiscolombus/2017/05/14/enterprises-are-running-cloud-based-apps-nearly-50-of-the-time/&refURL>
5. <https://www.securedgenetworks.com/blog/topic/strategy>
6. IDC InfoBrief, Sponsored by Akamai, Remote Access and Security, September 2017
7. <https://www.av-test.org/en/statistics/malware>
8. Arxan: 2017 Study on Mobile and Internet of Things Application Security <https://track.akamai.com/Pew%20Research%20Center>
9. Kaspersky Lab's Mobile Malware Evolution 2016 report
10. Kaspersky Lab's Malware Report for Q1, 2017
11. IDC InfoBrief, Sponsored by Akamai, Remote Access and Security, September 2017
12. RSA Cybersecurity Poverty Index 2016 <https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016>
13. <https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757>
14. <https://blog.barkly.com/ransomware-statistics-2017>
15. Infocyte: The Breach Detection Gap and Strategies to Close It <https://www.infocyte.com/breach-detection-gap-conf>
16. Cisco 2016 Annual Security Report
17. IDC InfoBrief, Sponsored by Akamai, Remote Access and Security, September 2017
18. IDC InfoBrief, Sponsored by Akamai, Remote Access and Security, September 2017
19. <http://www.gartner.com/newsroom/id/3598917>
20. Arxan: 2017 Study on Mobile and Internet of Things Application Security <https://track.akamai.com/Pew%20Research%20Center>
21. Pew Research Center via Huffington Post <https://www.arxan.com/2017-Ponemon-Mobile-IoT-Study>



Edge Delivery Services

powered by Akamai