Build Your Zero Trust Security Strategy With Microsegmentation

Why Digital Businesses Need A Granular Network Segmentation Approach
Overview

The idea of a secure network perimeter is dead. As companies rapidly scale their digital capabilities to deliver better customer experiences and operational efficiencies, they also become substantially more vulnerable to cyberattacks. Digital transformation necessitates an evolution of their security approaches to one that can manage threats in a complex and expanding technology landscape.

In May 2018, Unisys commissioned Forrester Consulting to conduct a custom survey of 164 IT professionals in North America to explore the security challenges they face as they seek to digitally transform, the progress they've made toward adopting a Zero Trust security architecture, and the benefits they expect from network microsegmentation.

Country
» 71% - United States
» 29% - Canada

Number of employees
» 54% - 1,000 to 4,999
» 31% - 5,000 to 19,999
» 15% - 20,000 or more

Seniority
» 29% - C-level or VP
» 41% - Director
» 30% - Manager
Organizations Are Embracing Digital Transformation

The need to satisfy customers' heightened expectations has propelled companies to digitally transform their internal processes and customer interactions. To support this effort, they are investing aggressively in new technologies that drive innovation and efficiency. They have adopted: analytics to turn data into insight for improved decision making; cloud services to augment connectivity, speed, and scalability; internet of things (IoT) to digitize physical products and optimize operations through improved monitoring; mobile applications and devices to delight customers in their moments of need and connect an untethered workforce; and artificial intelligence (AI) to better anticipate and deliver personalized customer interactions. While these initiatives are essential, they also raise the requirements for security and privacy — their No. 1 digital transformation technology investment area.

Digital businesses continuously create and exploit digital assets to deliver new sources of customer value and increase operational agility.
Digital Transformation Raises The Security Bar

As they implement new cloud services, devices, partners, bring-your-own-device policies, and customer engagement models, digital businesses find themselves in a new technology landscape. Their ecosystem is now more diverse, interconnected, and vulnerable. Eighty percent agree that digital transformation has expanded the cyberattack surface — so much so that the security perimeter is difficult to define.

To protect their data and information assets, companies must now find ways to consistently apply end-to-end security policies in a diverse landscape and safeguard sensitive information throughout the digital supply chain. The need to scale security practices to the fast rate of digital transformation change complicates this endeavor.

As companies digitize their businesses, they face new threats across a wide and diverse technology landscape.

---

**“How much do you agree or disagree with the following statements about digital transformation?”**

<table>
<thead>
<tr>
<th>Statement</th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>It contributes to a more heterogenous operating environment</td>
<td>32%</td>
<td>53%</td>
<td>85%</td>
</tr>
<tr>
<td>It expands the cyberattack surface</td>
<td>24%</td>
<td>56%</td>
<td>80%</td>
</tr>
<tr>
<td>It exposes us to new/novel forms of attack</td>
<td>30%</td>
<td>47%</td>
<td>77%</td>
</tr>
<tr>
<td>It introduces risks related to shadow IT/BYOD</td>
<td>25%</td>
<td>52%</td>
<td>77%</td>
</tr>
<tr>
<td>It increases reliance on third parties/partners</td>
<td>24%</td>
<td>53%</td>
<td>77%</td>
</tr>
<tr>
<td>It makes the security perimeter more difficult to define</td>
<td>27%</td>
<td>41%</td>
<td>68%</td>
</tr>
<tr>
<td>It makes protecting customer privacy/ regulatory compliance more difficult</td>
<td>30%</td>
<td>37%</td>
<td>67%</td>
</tr>
</tbody>
</table>

Base: 164 IT security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Unisys, July 2018
The Network Perimeter Is No Longer Defensible

Organizations have historically focused on securing the network perimeter. In this model, traffic inside the perimeter is classified as safe, and traffic outside of it is deemed unsafe. However, today’s digital ecosystem has rendered this approach obsolete. Attacks that originate within companies — where controls are weaker — are often the culprits of myriad security failures. The network perimeter offers little protection. Once inside the company, threats can spread unabated. Given that most respondents say the perimeter is difficult to define, it’s no surprise that 58% also believe it is indefensible. Put simply, there is no perimeter; companies must update their thinking and defensive strategies accordingly.

Thankfully, decision makers recognize the need for change: 84% agree that they must adjust traditional perimeter-based security strategies.

“To what degree do you agree or disagree with the following statements?”

- 28% Strongly agree, 30% Agree: “The network perimeter is indefensible in today’s technology ecosystem of distributed cloud workloads and mobile/remote users.”
- 51% Strongly agree, 33% Agree: “Digital transformation necessitates adjustments to traditional (perimeter-based) security strategies.”

Digital businesses need an inside-out security approach.

Base: 164 IT security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Unisys, July 2018
Zero Trust Affords Digital Businesses Operational Agility While Containing Risk

Companies cannot afford to trust internal network traffic as legitimate, nor can they trust employees and partners to always be well-meaning and careful with systems and data. To manage the complexities of their environment without constraining their digital transformation ambitions, many companies are moving toward a Zero Trust (ZT) security model — a more identity- and data-centric approach based on network segmentation, data obfuscation, security analytics, and automation that never assumes trust. ZT allows security and privacy protections to travel with the data itself — across hosting models, locations, devices, and third parties. It also applies the appropriate access rights based on the user’s identity. This allows companies to adapt to an evolving threat landscape quickly and effectively. While just 7% of those surveyed have applied all aspects of ZT, 84% have already adopted, plan to adopt, or have interest in adopting one or more pieces of the model.

“Which of the following best describes your organization’s adoption of Zero Trust?”

- Unfamiliar with this approach and not interested in adopting: 9%
- Unfamiliar with this approach but interested in adopting: 12%
- Does not describe our approach, and we have no interest in adopting: 7%
- Does not describe our approach — we have interest but no immediate plans to adopt: 10%
- Does not describe our approach, but we are planning to adopt one or more aspects within the next 12 months: 10%
- We practice some aspects of this approach: 29%
- We practice most aspects of this approach: 16%
- We practice all aspects of this approach: 7%

Base: 164 IT security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Unisys, July 2018
Microsegmentation Is A Key Piece Of Any Zero Trust Network

To successfully promote a ZT architectural model, security teams will need improved isolation of environments and infrastructures in the form of microsegmentation. Microsegmentation divides a network at a granular level, allowing organizations to tailor security settings to different types of traffic and create policies that limit network and application flows to those that are explicitly permitted. It allows security teams the flexibility to apply the right level of protection to a given workload based on sensitivity and value to the business. Over 75% of respondents agree that various aspects of their digital transformation technology programs necessitate microsegmentation. AI, IoT, and network-enabled device technologies top the list of technologies in need of microsegmentation, as they introduce a massive area of potential compromise through device and data proliferation.

Over 75% agree that their digital transformation technology programs necessitate microsegment-level protection.
Network Microsegmentation Is Gaining Momentum

In today’s technology environment, security teams must be able to isolate, secure, and control traffic on the network at all times — and do so at the micro level. Unfortunately, this is not the standard. While decision makers recognize the value of microsegmentation, only 26% already have it in place today. However, our research suggests that its popularity will soon spread: 22% have plans to implement microsegmentation in the next 12 months, and another 32% express interest.

While microsegmentation is not a new concept, traditional approaches have relied on building microperimeters by installing more firewalls. In fact, among the 26% who have adopted microsegmentation in our study, most say (64%) they use firewalls for all or part of their strategy. New microsegmentation approaches — including ones that are software-defined and offer embedded encryption capabilities — can ease infrastructure complexity.

Eighty-two percent describe access to a security solution that can encrypt data-in-motion as important to improving their security posture.
Microsegmentation Delivers On Strategic Benefits

Respondents whose companies have already adopted microsegmentation cite a long list of benefits — benefits that are consistent with Forrester’s ZT research. Most of all, they view it as valuable to improving their security posture (65%). Microsegmentation improves visibility and control at a granular level, allowing companies to better contain threats while minimizing disruption (i.e., locate and quarantine the affected person or group without shutting down an entire site). Operational benefits — including improved performance, easier segmentation of the network, and improved agility — also top the list. Finally, many consider microsegmentation helpful for protecting critical information assets and meeting compliance standards. The ability to shield intellectual property and sensitive customer data from falling into the wrong hands is a critical requirement for companies that compete on their ability to deliver personalized experiences without violating customer privacy and trust.

"What benefits do you associate with adopting a microsegmentation approach?"

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved security/reduced frequency of breaches</td>
<td>65%</td>
</tr>
<tr>
<td>Improved performance</td>
<td>45%</td>
</tr>
<tr>
<td>Ability to limit lateral spread of threats by better containing network problems</td>
<td>43%</td>
</tr>
<tr>
<td>Easier segmentation of network</td>
<td>43%</td>
</tr>
<tr>
<td>Improved ability to protect critical data/information assets</td>
<td>41%</td>
</tr>
<tr>
<td>Ability to more easily meet compliance standards</td>
<td>36%</td>
</tr>
<tr>
<td>Improved agility</td>
<td>34%</td>
</tr>
</tbody>
</table>

Even those companies that have not yet adopted microsegmentation find value: 98% associate one or more benefits with the approach.
Zero Trust Requires A Comprehensive Suite Of Tools Combined With Strategy

Digital businesses need security technology partners that offer a range of capabilities that: 1) are easy to use and integrate; 2) improve their network visibility; and 3) support the ZT model. They place especially high value on partner solutions that can apply security controls across environments uniformly and quickly, with features that allow them to modify settings as circumstances change. Eighty-eight percent also say that it’s important for them to be able to base security on user identity — a key tenet of ZT.

Support for controlling industrial control systems (ICS) and operational technology (OT) is also vital. Because these machines often run on proprietary software and are geographically dispersed, they can be difficult to update and secure. Disruptions to these technologies — which are critical to controlling any number of core functions, like factory automation, patient machines, and production processes — can result in significant profit loss, security threats, and even physical damage or harm. For this reason, 82% say their ability to secure these technologies is “important” or “very important” to improving their security posture.
Conclusion

While the digitization of products, services, and operations will be necessary to deliver on the experience expectations of demanding customers, it also increases organizations’ security risk. Perimeter-based security approaches are no longer sufficient. Companies need sophisticated capabilities that support a ZT security architecture — a more data- and identity-centric security approach built on focused network segmentation. Solutions that help firms secure their network at the microsegment level can help companies promote ZT principles and realize key benefits, including an improved ability to protect critical data assets in an evolving landscape; greater network visibility and control; and operational agility.

Endnotes
2 Ibid.
3 Ibid.