FORRESTER®

A Custom Technology Adoption Profile Commissioned By Certes Networks

Zero Trust Requires Effective Business-Centric Application Segmentation

GET STARTED ▶

A Custom Technology Adoption Profile Commissioned By Certes Networks

Zero Trust Requires Effective Business-Centric Application Segmentation

Zero Trust Requires Effective Business-Centric Application Segmentation

To protect the network from today's sophisticated attacks, IT security decision-makers must adopt a Zero Trust approach to network security. Hackers use multiple attack methods to find a network's weakness, even targeting business partners and suppliers to get inside. Many enterprises today rely on outdated network defenses that protect the perimeter but will not protect them from bad actors already inside their network or risks posed by compromised users. To properly protect their enterprises, security architects need to adopt a policy of Zero Trust in their networks and look to meet the security challenges of the 21st century by focusing on effective application segmentation aligned with business objectives.

In August 2015, Certes Networks commissioned Forrester Consulting to evaluate current application and network segmentation strategies in the wake of increasingly sophisticated attack methods.

58%

I am often the final decision-maker for network security.

42%

I provide significant input to the final decision-maker around network security.

Demographics

50 US IT security decision-makers with responsibility for network security in organizations with 500+ employees.

Job Title

- C-level executive: 32%
- Vice president: 14%
- Director: 34%
- Manager: 20%

A Custom Technology Adoption Profile Commissioned By Certes Networks

Zero Trust Requires Effective Business-Centric Application Segmentation

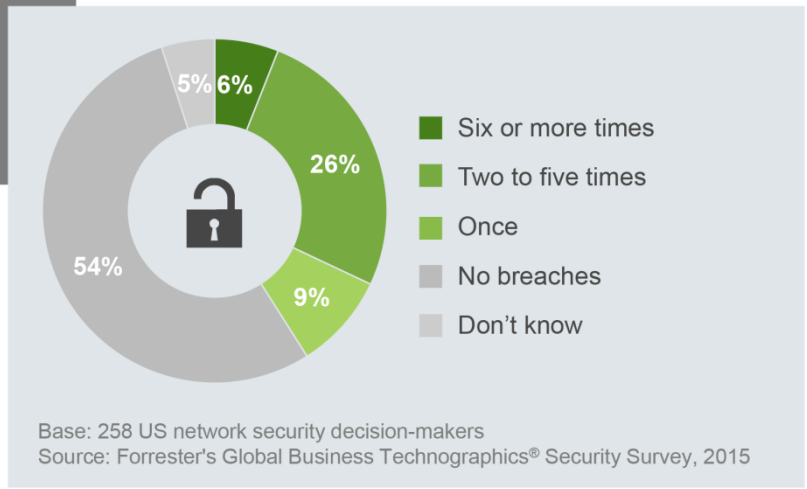
1 2 3

Data Breaches Plague Organizations Today

It seems like every day a new data breach is making headlines. According to Forrester's Global Business Technographics Security Survey, 2015, 41% of US security pros estimate that their firm's sensitive data was potentially compromised or breached in the past 12 months. Hackers are targeting companies they perceive as vulnerable; 36% of organizations have been breached more than once in the past year! Data breaches can seriously damage a company's revenues, reputation, and brand image.

36% of US organizations in our Global Security Survey have been breached more than once in the past year!

"How many times do you estimate that your firm's sensitive data was potentially compromised or breached in the past 12 months?"



Base: 258 US network security decision-makers
Source: Forrester's Global Business Technographics® Security Survey, 2015

A Custom Technology Adoption Profile Commissioned By Certes Networks

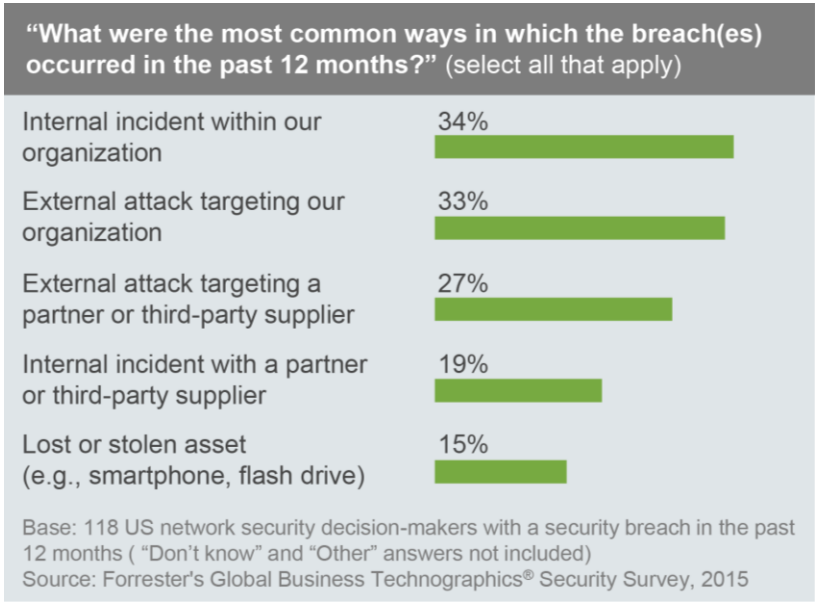
Zero Trust Requires Effective Business-Centric Application Segmentation

1 2 3

Hackers Expand Their Sights To Breach Targets

There is much more sophistication in the way hackers attack their targets today. They launch organized, sustained attacks with a variety of methods in order to get to their main target. Attacks are not just external and targeting the organization; internal incidents account for a large number of breaches today. In many cases, partners or third-party suppliers are being compromised and used as a gateway to access the target enterprises' sensitive data. For instance, law firms are targeted to gain access to their client's sensitive financial information. Organizations can no longer assume that their networks provide adequate security so long as they have a strong defense against external threats. This is the basis of the Zero Trust security model. We have found that:

- 34% of organizations that have experienced a breach were victims of an internal incident.
- 46% were targeted through a partner or third-party supplier



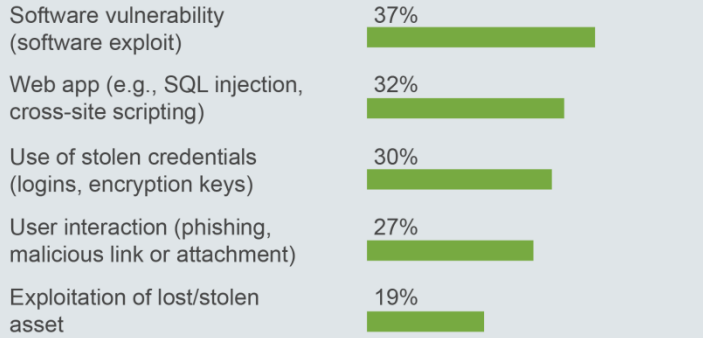
A Custom Technology Adoption Profile Commissioned By Certes Networks

Zero Trust Requires Effective Business-Centric Application Segmentation

Effective Attack Vectors Expose Vulnerabilities

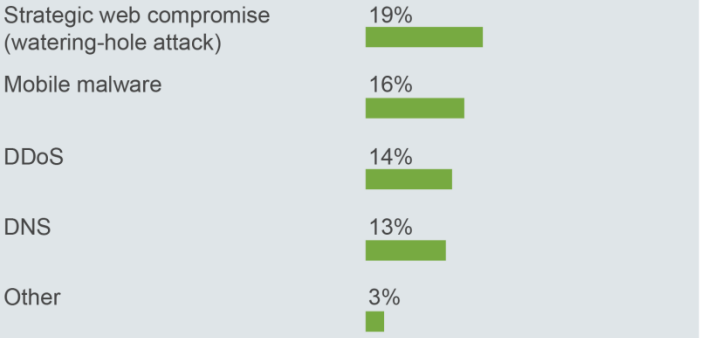
External attacks are carried out through a variety of methods and involve multiple steps, targeting not only vulnerable applications and networks, but also vulnerable employees and partners. Forrester's Business Technographics Security Survey, 2015 shows that 30% of external attacks were carried out through the use of stolen credentials, and 27% through user interaction. Attacks today are also increasingly happening without malware, with hackers running scripts and moving throughout the network once they have access with valid but compromised user credentials, which makes them difficult to detect.

"How was the external attack carried out?" (select all that apply)
(Responses 1 to 5)



Base: 63 US network security decision-makers with an external security breach in the past 12 months
Source: Forrester's Global Business Technographics® Security Survey, 2015

"How was the external attack carried out?" (select all that apply)
(Responses 6 to 10)



Base: 63 US network security decision-makers with an external security breach in the past 12 months
Source: Forrester's Global Business Technographics® Security Survey, 2015

1 2

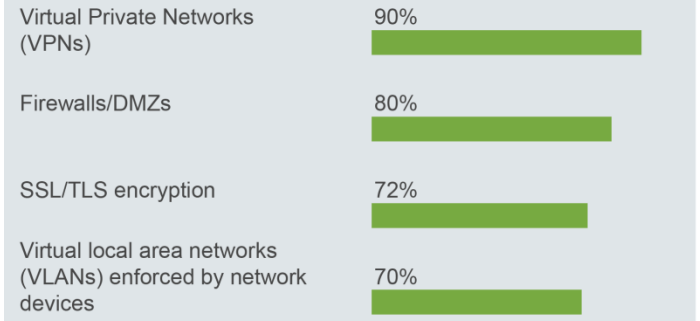
Segmentation Technologies Are Fragmented And Ineffective

Most firms rely on fragmented, outdated technology to segment applications and networks that were implemented before today's sophisticated attack methods were created. These networks rely on defenses, such as VPNs and perimeter firewalls, that many methods can bypass.

Network and application segmentation is fragmented. Most firms use multiple technologies to segment their networks, creating silos that leave some areas of the network less secure than others because of gaps or inconsistencies in these silos.

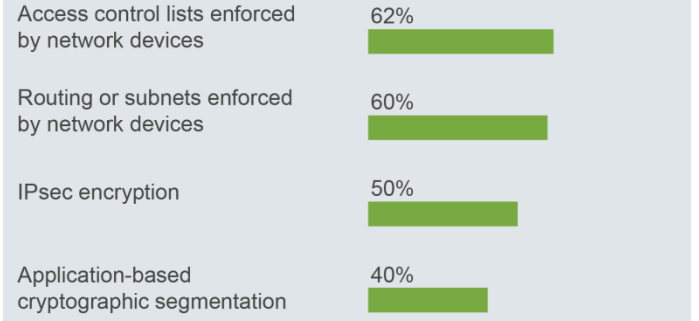
70% of respondents use VLANs to segment internal networks, but VLANs are part of network infrastructure and are designed to improve traffic flow. They do not provide strong security controls for role-based access to applications and fail to limit attackers' ability to move throughout the network.

"Which of the following network segmentation technologies does your organization use today for segmenting networks and isolating applications or networks?" (select all that apply)



Base: 50 US IT security decision-makers responsible for network security
Source: A commissioned study conducted by Forrester Consulting on behalf of Certes Networks, September 2015

"Which of the following network segmentation technologies does your organization use today for segmenting networks and isolating applications or networks?" (select all that apply)



Base: 50 US IT security decision-makers responsible for network security
Source: A commissioned study conducted by Forrester Consulting on behalf of Certes Networks, September 2015

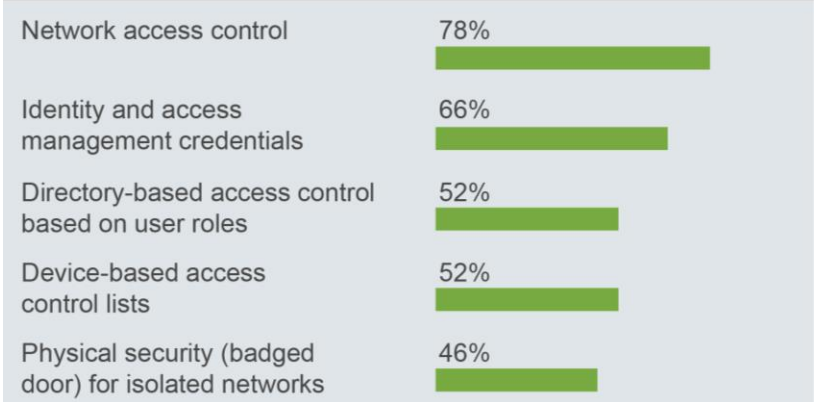
Zero Trust Requires Effective Business-Centric Application Segmentation

1 2

Segmentation Controls Are Outdated

Most organizations use network segment access controls that are designed almost exclusively to protect infrastructure and are tied to infrastructure components. Such controls are outdated in the face of borderless applications, public cloud migration, increasingly mobile users, and sophisticated new attacks. The most popular methods — network access control (78%), identity and access management credentials (66%), and directory-based access controls (52%), are usually used at the network perimeter. Once a hacker is in the network, they are free to move laterally though the network undetected, effectively hopping from app to app. Even when enterprises enforce user role-based access, this is usually only one of several methods and there are alternate ways to gain access and circumvent such controls.

"If you segment your networks or isolate applications, how do you control access to the segments?"
(select all that apply) (top five responses shown)



Base: 50 US IT security decision-makers responsible for network security
Source: A commissioned study conducted by Forrester Consulting on behalf of Certes Networks, September 2015

Zero Trust Requires Effective Business-Centric Application Segmentation

1 2

Zero Trust Architectures Rely On Effective Business-Centric Application Segmentation

In order to embrace the tenets of Zero Trust of the network, security architects must redesign their segmentation around business needs to effectively protect against today's attacks. If firms do not effectively segment business applications and place too much trust in networks, hackers can easily move laterally within a network once they gain access. This makes application segmentation an essential practice of proper security hygiene. However, organizations must be sure to use the right tools for the job.

Almost all firms use some form of segmentation and the majority use segmentation as a best practice for security (63%) and for regulation and compliance (59%).

"Why does your organization use network segmentation technologies?"

63%
It's a best practice for security

59%
Regulation or compliance purposes

45%
Network or traffic shaping

41%
To contain malware

Base: 49 US IT security decision-makers responsible for network security (top four responses shown)
Source: A commissioned study conducted by Forrester Consulting on behalf of Certes Networks, September 2015

1 2

Prevent Breaches With Application-Based Segmentation

Organizations must make sure they are using segmentation technologies like application-based cryptographic segmentation with role-based access control. The technology must translate directly to business security needs and protect business applications within the network and outside of the network, even when perimeter is breached and the network is compromised.

Current network segmentation practices are infrastructure-centric and perimeter-based. Only a minority, 40%, are doing application-specific segmentation and only 22% use microsegmentation.

Unfortunately, because of the infrastructure-centric approach to security, only 54% of firms can say that they were not breached in the past 12 months. The right business-centric approach with application-based cryptographic segmentation and role-based access control needs to be adopted more widely to stop this alarming avalanche of breaches.

Only 40% of respondents report that they are doing application-specific segmentation; only 22% use microsegmentation.

A Custom Technology Adoption Profile Commissioned By Certes Networks

Zero Trust Requires Effective Business-Centric Application Segmentation

Conclusion

To embrace Zero Trust, companies must adopt business-centric application segmentation. Attackers are becoming more sophisticated every day and will prey on companies that still implicitly trust their networks and are not sufficiently protected with effective segmentation technologies. Many enterprises today rely on outdated segmentation technologies that emphasize infrastructure over business applications and secure the perimeter but offer no protection once attackers are in the network. Security architects need to be sure they are using the right segmentation technologies to secure their applications.

METHODOLOGY

- This Technology Adoption Profile was commissioned by Certes Networks.
- To create this profile, we leveraged Forrester's Global Business Technographics® Security Survey, 2015. Forrester Consulting supplemented this data with custom survey questions asked of US IT security decision-makers responsible for their organization's network security.
- The auxiliary custom survey was completed in September 2015. For more information on Forrester's data panel and Tech Industry Consulting services, visit forrester.com