NOVEMBER 2015

UBM

THE STATE OF Segmentation in Security Architectures

Fixing the Data Breach Blind Spot

Executive Summary

Recent data breaches have seen cybercriminals siphon off millions of records containing personally identifiable information and credit as well as debit card data, which is taking a major toll on company profits and customer loyalty. To identify the gaps in IT security that allow hackers to steal so much data, a joint UBM Tech and Certes Networks survey asked security experts how they protect their sensitive data, and specifically how they employ segmentation technologies to shrink their attack surfaces and reduce the damage caused by a data breach.

Segmentation is commonly understood as the practice of dividing or separating IT resources into their own logical or physical domains, often for the purpose of simplifying traffic management or providing security. The survey and this analysis paper focus primarily on segmentation of networks and enterprise applications that are shared on networks.

When it comes to dealing with enterprise data breaches, IT security is broadly divided into three main areas: threat prevention, threat detection and response, and threat containment.

Threat containment focuses on limiting the scope and extent of data theft from the inevitable breaches. Segmentation plays a role in preventing unauthorized people from accessing IT resources that they should not. It acts as threat-containment technology by narrowing the attack surface that can be targeted by an intruder and restricting access to sensitive applications.

Many security experts urge enterprises to develop security strategies based on the assumption that their network has already been compromised. Despite this suggestion, the survey data shows that respondents ranked breach containment technologies like segmentation as least likely to be deployed when compared to the other two forms of breach security. Respondents' replies indicated many reasons that segmentation was not more widely deployed such as difficulty with management; fragmentation of segmentation technologies across groups, applications, and network siloes; and performance issues when attempting to use network devices for segmentation.

In this report, we examine the role of segmentation in containing breaches and how it can be done more effectively. We explore the possible shortcomings of segmentation that is tied to network infrastructure. Finally, we discuss a "software-defined" approach to segmenting applications that decouples security enforcement from the underlying network or infrastructure and enables an enterprise to contain breaches and minimize damage should an attack occur.

A majority of the survey respondents cited segmentation as a highly effective security tool. However, the survey results also show that many IT shops have difficulty implementing segmentation, largely due to overlapping responsibilities, siloed operations management across different network and technology domains, and concerns over degrading the performance of networks or applications.

Among the findings:

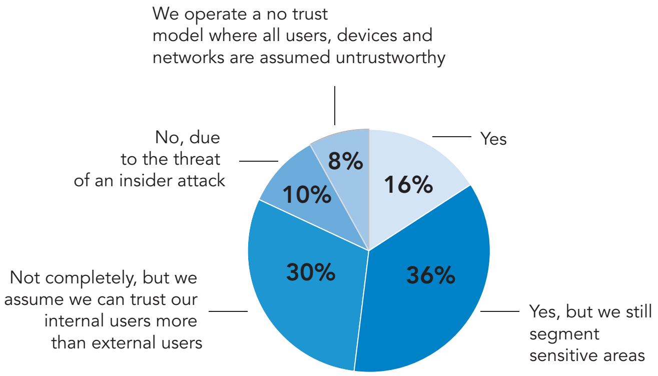
- Despite recent breaches, 82% of respondents still largely trust internal networks and users, proving time and again the overreliance on prevention and detection strategies at the perimeter.
- Though 64% said segmentation is quite or very effective as a security control, only 42% reported that they deploy any form of robust network segmentation as part of a data breach prevention program.
- Almost half (48%) said they need to change how their environments are segmented but are concerned about breaking key processes and services or have other tasks drawing them away from this objective.
- More than two-thirds (69%) reported that overlapping responsibilities among different groups and employees can create security gaps.
- Respondents cited impacts on the performance of the infrastructure as a top reason not to segment internal networks.

The most common form of segmentation is the use of infrastructure-centric technologies such as firewalls to segment along the line of "public" (untrusted) and "private" (trusted) networks and IT environments. In these architectures, the tendency is to trust users, networks, and devices on the internal, private network, and to not trust external users, networks, and devices.

- Firewalls and virtual local area networks (VLANs) are by far the most popular segmentation technologies, followed by routers and virtual private networks (VPNs).
- Nearly a third of respondents assume they can trust internal users more than external users.
- Encryption of application traffic is spotty, with 16% encrypting traffic only on external networks and 29% saying they encrypt all traffic everywhere.

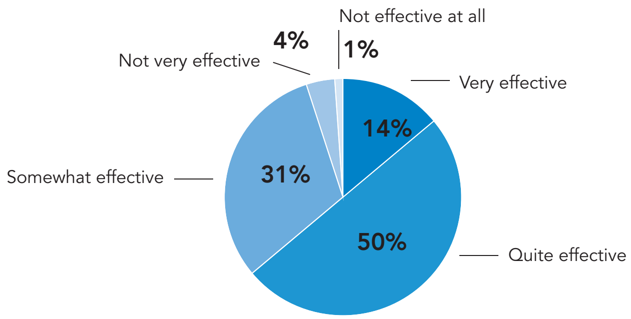
The survey data paints a stark picture of enterprise security architects facing a difficult dilemma. While

Figure 1: Do you fully trust your internal network?



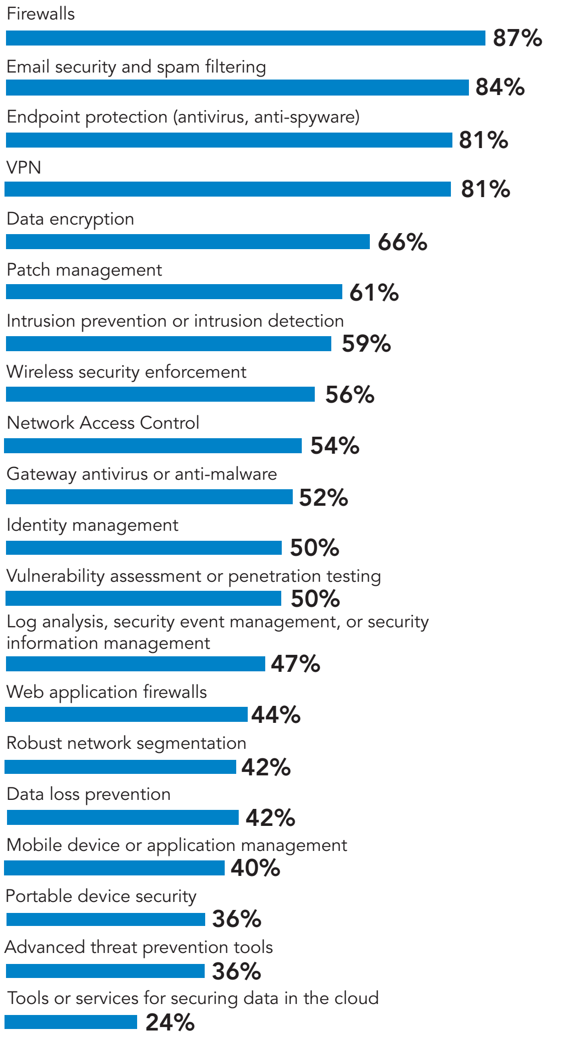
Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

Figure 2: How do you rate the effectiveness of network segmentation as a security control?



Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

Figure 3: Which of these security products are currently in use to protect sensitive data from breaches?



Note: Multiple responses allowed
Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

the value and importance of using segmentation technologies to protect sensitive applications is well understood, the limitations of the infrastructure as well as the fragmented and siloed nature of the available tools and security responsibility make effective segmentation hard to achieve.

Unfortunately, there is mounting evidence that incomplete or inadequate segmentation may enable an attacker to penetrate a single system and then move laterally across other systems in the enterprise – a favorite tactic for many hackers and cyber criminals.

The Data Breach Blind Spot

The most common example of network-based segmentation is in the establishment of a firewalled enterprise perimeter. In the survey results, 40% of respondents reported using perimeter-based segmentation to separate internal networks — local area networks (LANs) — from external networks such as wide area networks (WANs) or the Internet.

Traditional network segmentation using firewalls assumes that attackers are an external entity or malware trying to breach the fortified perimeter defenses to break directly into application servers on the internal network. This basic security architecture is outmoded. In modern attacks, the enterprise perimeter is simply bypassed. Hackers are able to compromise a single authorized user by stealing that person's credentials.

The predicament that enterprises are as vulnerable to a breach as the least secure of their internal or external users is known as the data breach blind spot. This vulnerability is caused by modern enterprise applications, user behaviors, the proliferation of new smart devices, and business relationships that no longer recognize or respect the traditional enterprise perimeter. Applications are routinely shared with external users and partners. Users regularly bring personal devices and applications into the enterprise environment, outside the control or awareness of the traditional IT department — that is, shadow IT. Additionally, supply chain members, contractors, and professional services firms often have access to applications within the firewalled perimeter as a way to streamline interactions, collaboration, and routine business processes.

The blind spot in the defense against data breaches is a single user who can be lured into visiting a malicious website, can be tricked into opening an infected Word document or viewing a booby-trapped PDF, or, most commonly, falls prey to a phishing attack that compromises access credentials. Once attackers have exploited this weak link to install malware or obtain a user's network credentials, they can launch their attacks as if they are insiders, moving laterally to access applications inside the "fortified" perimeter.

The documented analysis of the attacks that led to the data breaches at TalkTalk, Target, Home Depot, Anthem, Sony, the U.S. Office of Personnel Management, and many others points to hackers using compromised individual users or single systems as stepping stones that permit unfettered access to internal systems. Yet, the survey found that enterprises continue to treat those with credentials as trusted users, and almost none, a mere 7%, design segmentation based on the sensitivity of applications. Only 12% employ segmentation that isolates particular servers and users from other resources, and only 5% create segments designed to permit access to applications based on user roles.

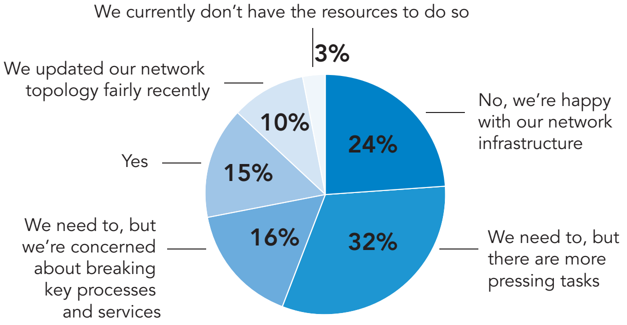
The 'No Trust' Strategy

Nevertheless, survey results indicate that attitudes are changing. While a majority of respondents continue to trust internal networks and users, only 16% completely trust them without any reservation. Specifically:

- 36% said they trust the internal networks but use segmentation to secure the most sensitive areas anyway.
- 18% indicated that they do not trust internal networks because of the threat of insider attacks, or because they operate a "No Trust" model of security architecture.

Industry observers and IT security experts have advocated the "No Trust" architecture for years. "No Trust" simply assumes there is no such thing as an untrusted or trusted network or IT environment. Instead, every user, device, network, and application is treated as untrusted, and all enterprise systems are considered already compromised by unauthorized users or malware. Traffic over the LAN is regarded and protected in the same fashion as traffic over the Internet. User access controls are applied consistently across all users and applications, regardless of the network or device the user might be on.

Figure 4: Do you plan to change how network resources are segregated to better control communications between resources within the next twelve months?

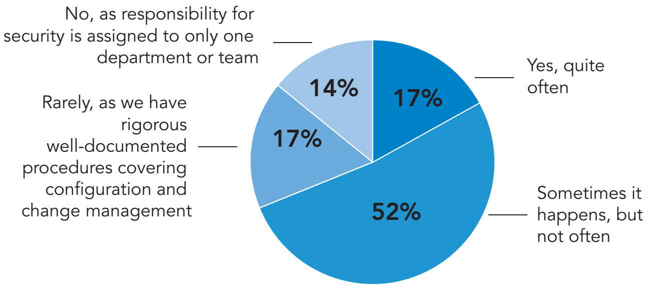


Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

Following the assumption that systems are already compromised, a major feature of "No Trust" design is threat containment. The security architects typically continue to use threat prevention technologies like firewalls or VPNs and threat-detection technologies such as intrusion-detection systems. The design also emphasizes segmenting networks, isolating applications with strong encryption, shrinking the attack surface that is exposed to hackers, and tightly controlling user access to only the applications they need to do their jobs.

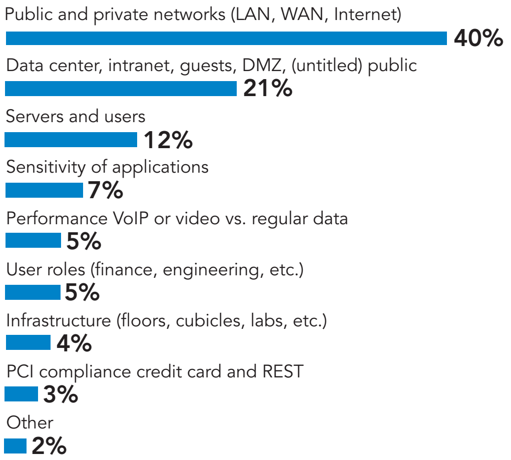
The "No Trust" design aims to address a major gap in the time it takes for breaches to occur and

Figure 5: Do overlaps in responsibility between departments or teams create gaps in your security?



Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

Figure 6: What is the dimension along which you segment?



Base: 154 respondents who do not run a flat network
Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

the time it takes to detect them.

According to data from [Verizon's 2015 Data Breach Investigation Report], breaches from initial attack to compromise can occur in the span of a few minutes. But breach detection continues to take months if not years. This defender-detection response gap gives attackers the time to install extensive attack tools, analyze the layout, map the defenses of the network, and discover key machines and applications containing the most sensitive data. Pivoting from a single compromised system to fully controlling the most sensitive servers on a network is the final step before extracting and exfiltrating the targeted data.

Containment is the only way to stop attackers from reaching their end goal and extracting the most valuable data they came for. If segmentation has been employed effectively, damage from a breach will be immediately contained within the segment, even if the breach hasn't been detected.

Internal network segmentation has been likened to the internal bulkheads and compartmentalization that are common in ship and submarine design. If a breach of the hull occurs, one compartment may be flooded, but watertight bulkheads prevent water from inundating the other compartments and the vessel remains afloat.

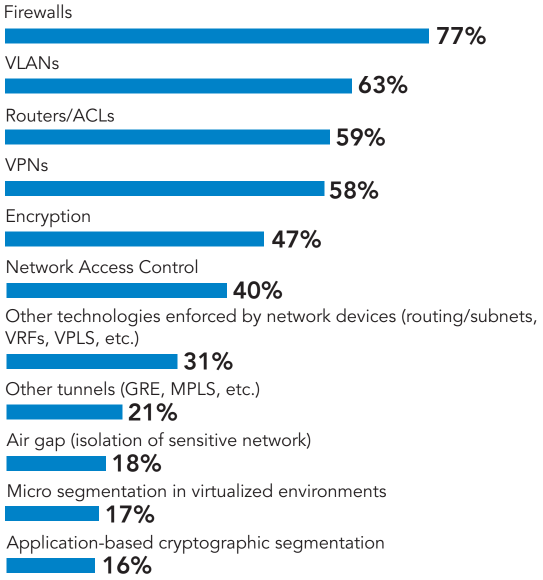
Segmentation Fragmentation

What stands in the way of more enterprises adopting the "No Trust" model and deploying segmentation in their networks?

The survey yields several important data points that describe the challenges:

- Survey respondents indicated 11 different technologies and techniques are used for segmentation, with the majority indicating that they deploy firewalls, VLANs, routers with access control lists, and VPNs for the purposes of segmentation.
- Access control is equally fragmented, with users citing seven forms or methods of user identification, authentication, and access policy enforcement.
- There is little consistency in which types of IT professionals or departments have control over the segmentation technology. More than half indicated that security managers

Figure 7: Which types of resource segmentation technologies do you use?

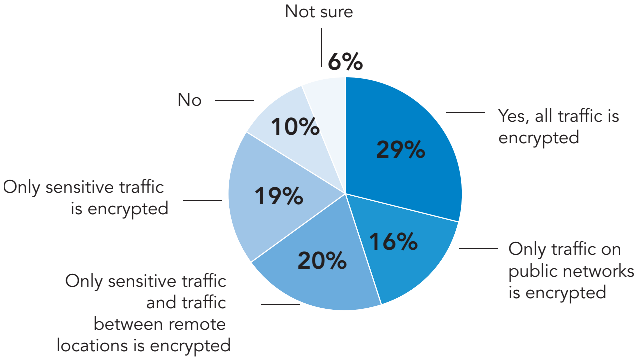


Note: Multiple responses allowed
Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

have the ability to manipulate the segments, but half said network engineers can configure segments independently.

- Configuration of these technologies was cited as a chief challenge. Only 4% described the configuration of segmentation technologies as "easy," while 80% said it was "difficult," "very difficult," or required an experienced staff to complete the job.
- Respondents indicated that the segmentation itself is often quite static, with 42% saying that they change or update segmentation only when infrastructure is added or upgraded. Almost one in 10 indicated that segments had not been updated for years.

Figure 8: Do you use encryption on your internal networks?



Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

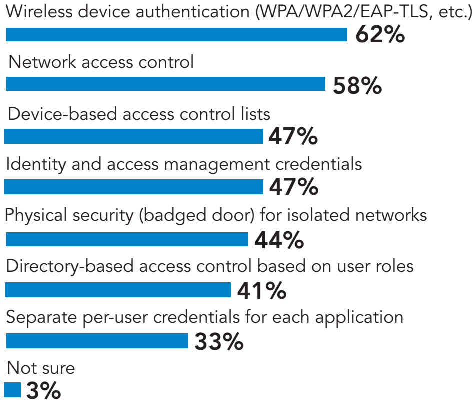
The net result of these responses is consistent with many of the findings of industry researchers and observers in recent years, especially in light of the ongoing wave of hacking attacks and data breaches.

It is clear that tying segmentation to the network, devices, or other components of the infrastructure is extremely limiting. The network is full of siloes, including LAN, WAN, Internet, mobile, Wi-Fi, cloud, data center, and firewalled perimeter. Each of these siloes has its own method of application protection and access controls and is often managed by separate teams in the enterprise. Enforcing consistent policies and protection from end to end across all these zones is enormously difficult given the fragmented nature of the technologies and teams. Changing segmentation to encompass new users, applications, or use cases becomes a painful exercise in infrastructure architecting and reconfiguration. It renders the segments largely static and inflexible when compared to the fluidity of modern applications and the mobility of users.

Most importantly, the fragmented nature of segmentation controls and responsibilities creates the likelihood of gaps in the security architecture. For example, when an internal user shares an application with an external supplier, that application may be protected with VPN-based access controls and encryption if used across the Internet. But the portion of the application flow that is routed through the enterprise data center and LAN is transported without protection and is not isolated in its own segment. This oversight creates a security gap. It means that an attacker who compromises that external user will have access beyond the firewall and then free rein to move laterally to any internal system or resource that is available.

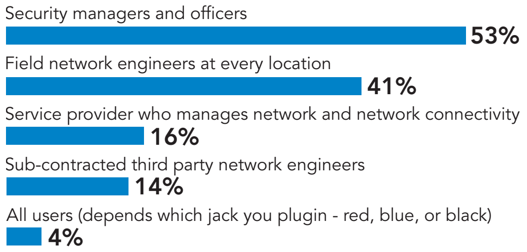
As one survey respondent said, "The major problem is that all the defense-in-depth [tools] they are

Figure 9: How do you control access to the segments?



Note: Multiple responses allowed
Base: 154 respondents who do not run a flat network
Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

Figure 10: Who has the ability to manipulate, define, or modify the network segments?



Note: Multiple responses allowed
Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

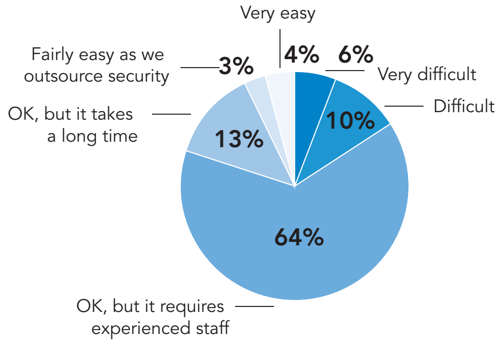
using to try to secure their environments don't work well together, and hackers regularly figure out how to get around them. It's like Swiss cheese — lots of holes that constantly change."

These challenges are a chief reason the concept of virtualized segmentation or "software-defined security" has taken hold recently. This trend focuses on decoupling segmentation from the infrastructure and instead aligns segmentation to applications, managing the segments from end to end over all intervening networks and creating a single point of control across all applications for all users.

Software-Defined Segmentation

The software-defined approach reorients segmentations from the infrastructure to focus on business applications.

Figure 11: How easy or difficult do you find it to configure segmentation technologies?



Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

Since applications are no longer restricted to enterprise perimeters, the segmentation strategy must also be decoupled from the network and infrastructure components such as firewalls, routers, or switches.

The application flows of today's virtualized environments need policies to be updated dynamically when applications routinely cross enterprise perimeters, move around with mobile users, or are offloaded into the cloud.

Certes' CryptoFlow software-defined security solution looks to solve these problems and make business-centric application segmentation a lot more straightforward with a unified, central point of control.

Certes' CryptoFlow products create secure virtual overlays that are simply cryptographically protected traffic flows between applications and authorized users, removing the need to reconfigure firewalls, routers, switches, or applications.

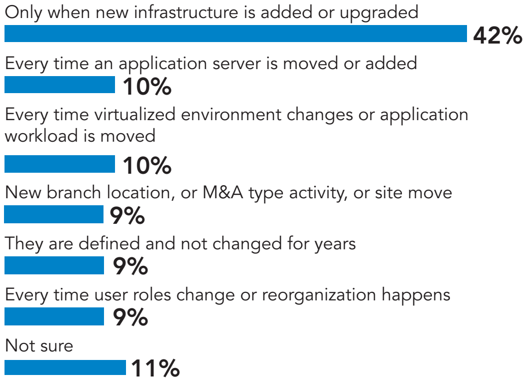
Instead of connecting a trusted device to a trusted network like a traditional VPN, CryptoFlows connect users based on roles to the cryptographically isolated applications they're authorized to use — an approach to segmentation that Certes calls crypto-segmentation. CryptoFlows encrypt the application traffic to fully isolate each application into its own segment, with protection profiles, cryptographic keying, and access control policies applied on a per-application basis. CryptoFlows cross all networks, including the Internet, and extend to cloud environments out of enterprise control, and yet apply the same protection for all the enterprise's applications.

Most importantly, CryptoFlows enable security managers to grant access to application segments based on authorized users' roles, which directly aligns the process of segmentation to the company's business objectives. A physician can get automatic access to a patient records application, the pharmacy ordering application, and the like, but can also be automatically blocked from access to the hospital's credit card processing application or financial records.

A security administrator using CryptoFlows defines a security profile for each application based on business rules, where user roles and business policies determine access rights. Each application has its own encryption key, which isolates the application regardless of whether it's located in a physical or virtual data center, is in a private or public cloud, or has components in all of them. This approach enables administrators to dynamically control security without being reliant on the network or other infrastructure.

Further, this capability significantly simplifies and accelerates the security configuration tasks that must occur for a new application to be introduced in the enterprise. Instead of 11 segmentation technologies and methods to configure, the security manager has to manage only one.

Figure 12: How often do you think you need to update your network segments?



Data: UBM Tech survey of 165 security technology professionals at companies with 500 or more employees, September 2015

Access to applications is cryptographically protected end to end from users' endpoint devices to application servers, no matter their location. This solves many of the problems administrators have maintaining and updating fragmented segmentation across siloes. There no longer is a need for the complex segmentation configuration tasks at each hop or network silo.

Attackers who breach the network's perimeter defenses will not be able to access a CryptoFlow segmented application as they're not an authorized user of that CryptoFlow. If they manage to compromise the credentials of someone who is authorized, they will only obtain access to the CryptoFlow or application that the user is authorized for. The result is a crypto-segmented application network that shrinks the attack surface and automatically contains the breach by preventing the lateral movement of an attacker. This blocks the main attack vector that was the hallmark of the Target, OPM, Home Depot, Anthem, and other significant breaches over last few years.

Conclusion

Prevention and detection of threats alone are proving insufficient, and organizations can no longer base their security strategies solely around these technologies. Threat containment as a layer of defense has to play a bigger role, and segmentation can be very effective at halting an attack in its tracks. It greatly limits the exposure of valuable business assets by reducing the enterprise attack surface. It limits the impact of a security breach by preventing an attacker's lateral movement from one application segment to another application segment.

Segmentation is most effective when implemented along business needs and not around the outdated notion of trusted versus untrusted networks or devices. The survey results show that segmentation using common infrastructure-centric techniques is very difficult because of the fragmented and siloed nature of the network devices and supporting teams.

By leveraging cryptography to raise segmentation from the infrastructure to the business layer and granting access to crypto-segments based on user roles, Certes Networks has created an effective, business-driven approach to segment and compartmentalize enterprise applications. Simplifying security to align with business objectives is the key to good security. The CryptoFlow approach can accelerate the rollout of new enterprise applications as the enterprise security architecture is software-defined and decoupled from the fragmented infrastructure-based segmentation.

A software-defined, or virtualized, segmentation strategy aligned to business applications and business objectives can overcome the siloes and fragmentation and provide end-to-end protection of applications. This in turn can contain the inevitable breach when it occurs and can block attackers from gaining access to the most sensitive applications and valuable data.

As one respondent put it: "Everyone gets attacked. The issue is how successful were the attackers and did they, in truth, compromise IP, financial data, or other pertinent business operations data?"

About Certes Networks: Certes Networks protects data in motion with market-leading software-defined security solutions. The company's award-winning CryptoFlow® Solutions safeguard application traffic in physical, virtual, and cloud environments, enabling secure connectivity over any infrastructure without compromising network device or application performance. Companies around the world rely on security solutions from Certes Networks to protect access, accelerate application deployment, simplify network projects, reduce compliance costs, and improve the return on investment in IT infrastructure. For more information, visit certesnetworks.com.