

Intellyx White Paper

Securing the Frictionless Enterprise

Jason Bloomberg

August 13, 2015

The Dark Side of the Frictionless Enterprise

During the seventy-year history of enterprise information technology, generation after generation of IT have transformed the nature of business. No process, no customer, no aspect of day-to-day work has been left unchanged, as the exponential pace of technology advancement continues unabated.

Today it seems we've reached an inflection point in this inexorable march of progress, as so many facets of technology are impacting organizations, from cloud computing to mobile technologies to big data.

Furthermore, these technology advancements are removing impediments to business, as customers demand increasingly real-time, always-on service from the companies they do business with.

Welcome to the *frictionless enterprise*.

Applications and data networks have changed. Applications can be shared anywhere, on a range of new and diverse devices. External partners, customers and employees need to access mission-critical data rapidly and efficiently.

In addition, companies no longer stand alone. Instead, ecosystems become the central organizational principle, as enterprises offload responsibilities to partners, customers, and other participants in the value chain.

Yet with all these advances come greater risks. The insular, proprietary network and application technologies of the last century may have been inflexible and expensive to maintain, but at least they provided a measure of protection from criminals and other bad actors. Every step we take toward the frictionless enterprise opens up holes for hackers to exploit.

Sharing applications across borders also means exposing them to hackers. Every time an organization places an application on the network, its attack surface grows wider and harder to defend.

As recent high-profile cybersecurity breaches have shown, the old way of securing systems and the precious data on them is not enough. Hackers are compromising global business, turning corporate IT environments into targets ripe for attack – stealing valuable data at will.

As these global IT attacks become increasingly commonplace, executives must ask themselves: are they adequately protecting corporate data, from credit cards to patient records to bank accounts to social security numbers – as well as other sensitive information flowing freely across the enterprise?

There are security tools aplenty, and cybersecurity is a booming business to be sure. But the attacks continue unabated. Something has got to give. Bottom line: we all need a better, simpler way to protect the information lifeblood of our organizations.

Limitations of Threat Prevention and Response

Today the world has changed. There are no more “safe zones.” The internal network is untrusted, and everything outside is downright hostile.

Controlled border security breaks down as organizations become increasingly frictionless, as activities like provisioning virtual machines in the cloud or new endpoints like mobile devices take place outside the perimeter.

A prime example: the [Target breach!](#) that hit the news at the end of 2013. A phishing attack compromised the login credentials of a heating and cooling contractor servicing Target stores. Once inside, the hackers installed malware and took their time breaking into other systems, eventually stealing millions of credit card numbers.

Did Target have firewalls? Absolutely. Did they stop – or even mitigate – this attack? *Not at all.*

Simply *detecting* the breach took over six months.

In fact, firewalls *by design* can never stop all attacks, because they must provide access to authorized personnel. And if there's access for working, that means there's access for hacking. Furthermore, there is always the risk of essentially undetectable, previously unknown zero day attacks.

Because breaches are inevitable, and furthermore, hackers have already penetrated most enterprises, the security industry is now focusing on narrowing the lag between the occurrence and detection of each breach.

¹ <https://corporate.target.com/about/shopping-experience/payment-card-issue-faq>

Six months is simply too long. As a result, many of the new security products in the marketplace focus on reducing the detection gap from months to weeks or days. But even a matter of a few days can leave plenty of time for hackers to find and exfiltrate sensitive enterprise data.

Containment of such breaches, therefore, is often the best a security organization can hope to achieve in order to minimize the damage from such attacks. One such approach is segmentation of networks and applications.

Network Segmentation – Part of the Solution

As organizations extend their applications to virtually everyone, they become easier to hack. Data that are easier to share are also easier to steal. Furthermore, any company's security is only as strong as its weakest link, which could be any technology component or more likely, any person – a partner, an employee, or a contractor.


Enterprises obviously need better security, but no security is perfect – which is just another way of saying that perfect security is infinitely expensive. Every executive responsible for cybersecurity must weigh existing risks against the budget for mitigating those risks. The sad reality, therefore, is that there will always be vulnerabilities.

Security personnel can't prevent every attack, but perhaps they can contain the damage. The typical approach to dealing with this reality is *network segmentation*. Splitting up the network into discrete segments compartmentalizes the potential damage a hacker might be able to cause.

Controlled border security – using firewalls to establish a perimeter around the organization – is the most common form of network segmentation. This approach is network-centric, with strong protections at the perimeter. It treats the internal network as a safe zone and everything outside the internal network as untrusted.

In addition to its firewalls, we can only assume that Target must have had a fragmented patchwork of virtual private networks, SSL and TLS security, IPsec tunneling, VLANs, ACLs, FW DMZs, Internet WAN DMZs, routing policies and application-layer encryption controls. However, this alphabet soup of traditional network segmentation approaches are all tied to network infrastructure, rather than business rules and policies. They are *infrastructure-centric* rather than *business-centric*.

There are simply too many tools, too many moving parts, resulting in a management nightmare – both in terms of management software as well as the variety of people in different roles who must all work together to manage IT security. After all, complexity is the enemy of security.



SPLITTING UP THE NETWORK INTO DISCRETE SEGMENTS COMPARTMENTALIZES THE POTENTIAL DAMAGE A HACKER MIGHT BE ABLE TO CAUSE.

Borderless Security for a Post-Trust World

The security challenge for the 21st century is to realize that borders are porous. Applications can be anywhere. Endpoints can be any number of different types of devices, including phones, televisions, sensors, etc. This borderless world requires enterprises to implement *borderless security*.

With borderless security, applications are decoupled from their underlying infrastructure, raising threat mitigation to the application-centric business level. The *business* must establish security policies, where software-based controls enforce those policies across borders.

Such borderless security is especially important for organizations implementing hybrid clouds or mobile applications, as these technologies are inherently borderless. This approach is also necessary whenever an organization is dealing with sensitive data or regulated environments – which in essence includes all enterprises, some more so than others.

Such borderless security is very different from traditional network segmentation-based approaches, as it recognizes that we now live in a *post-trust* world.

By *post-trust* we mean that companies recognize that they can't fully trust *any* internal network or *any* user. Perimeter security-based architectures – as well as other approaches to threat prevention – are woefully obsolete. And furthermore, *breaches have already occurred*. It's not a question of *if*. It's not even a question of *when*. It's a question of *what do you do now to contain the damage immediately – even before you are able to detect and repair it*.

Segmentation is still the answer – only not the chaos of infrastructure-centric network segmentation. Enterprises require a business-centric segmentation approach that rises above the hodgepodge of infrastructure in order to contain breaches and contain the damage in the time between breach and remediation.

ENTERPRISES REQUIRE A BUSINESS-CENTRIC SEGMENTATION APPROACH THAT RISES ABOVE THE HODGEPODGE OF INFRASTRUCTURE IN ORDER TO CONTAIN BREACHES AND CONTAIN THE DAMAGE IN THE TIME BETWEEN BREACH AND REMEDIATION.

Crypto-Segmentation: Security for the Frictionless Enterprise

The secret to effective, business-centric network segmentation is to protect application traffic with strong cryptography and grant access to each application based upon user roles, an approach we call *crypto-segmentation*.

Encryption alone, however, is not the answer. Encryption is the first line of defense for protecting sensitive information to be sure, but most security teams tie it to infrastructure rather than business rules. Furthermore, encryption can adversely impact performance, and in many cases, people apply it inconsistently. Additionally, encryption requires private key management, which is a headache in itself.

The end result: security gaps hackers are only too happy to exploit.

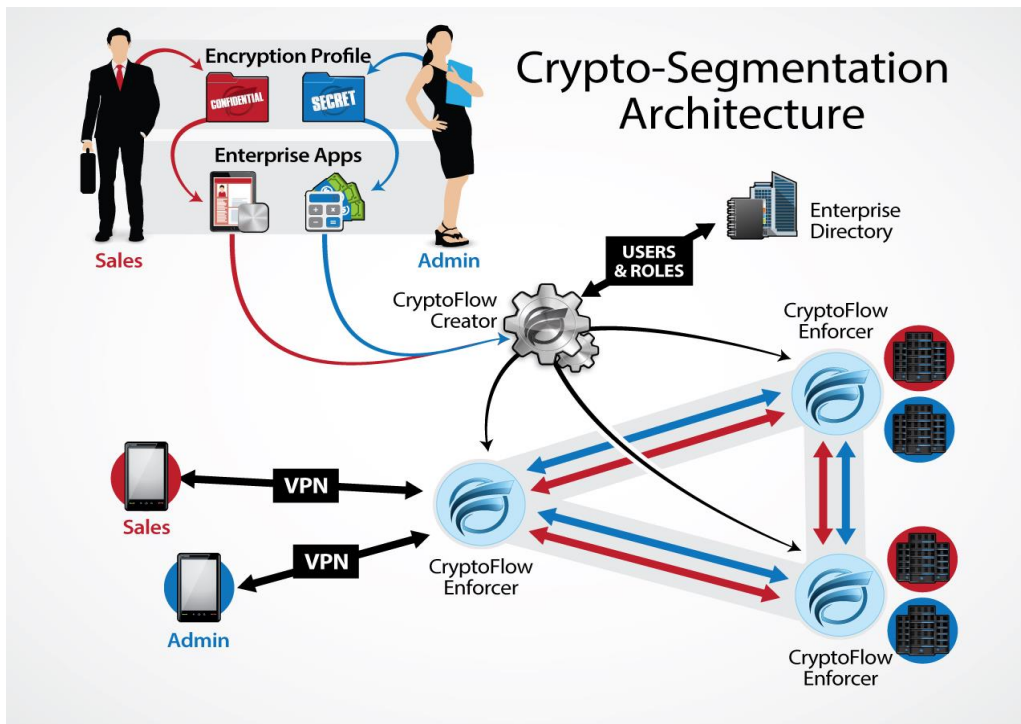
Crypto-segmentation addresses these limitations of encryption by establishing role-based access to *cryptographically isolated*, networked applications. Instead of the physical network segments that constitute the infrastructure-centric approach to segmentation, crypto-segmentation establishes *logical, policy-driven* network segmentation that abstracts the physical elements of the infrastructure.

In essence, the organization encrypts each virtual segment separately with a unique key. Security admins base the definition of each crypto-segment upon business rules for each application, where user roles and business policies determine access rights that depend on verified identity.

The robustness of crypto-segmentation, therefore, centers on key management rather than a hodgepodge of separate tools and network infrastructure components. Security admins maintain complete control of the keys and the key lifecycle. And because organizations can't fully trust their admins, crypto-segmentation also requires centralized audit logging for all access to the policies.

The result: when breaches occur (and they will), the compromise of networks, applications, or even users does not compromise other crypto-segments on the network.

Crypto-segmentation, therefore, compartmentalizes the network, preventing the lateral movement that was the hallmark of the Target, OPM, Home Depot, Anthem, and other significant breaches over last two years. The diagram below illustrates crypto-segmentation in action.



Crypto-Segmentation in Action (Source: Certes Networks)

Fundamentally, crypto-segmentation is an important part of software-defined security (SDS), where software controls drive all security infrastructure. The security team is fully in control, leveraging strong user identity management and role enforcement across the environment. In fact, crypto-segmentation technology orchestrates keys, policies, and the ability to audit the security controls across all applications, users, and networks.

Certes Networks CryptoFlows

Leading the innovation in crypto-segmentation is Certes Networks (www.certesnetworks.com). Certes' software-defined security approach enables customers to dynamically control data traffic security without dependence on applications or the network infrastructure.

Certes Networks' core offering is the *CryptoFlow Solution*, which uses crypto-segmentation to safeguard enterprise applications over any network for any user, on any device.

A *CryptoFlow* is a secure virtual overlay for each application, protecting each application with strong encryption, with its own security profile and keys. It extends to wherever the application resides in either physical or virtual data centers or private or public clouds – wherever users want access, across any network, to any of their chosen devices.

CryptoFlows also provide a single point of control for end-to-end protection of sensitive applications. Via this crypto-segmentation, CryptoFlows isolate and protect sensitive applications from the application server to users' end-point devices, regardless of their location. Furthermore, CryptoFlows auto-generate session keys and protect them from any user, even one with administrative privileges.

As a result, IT security managers have a single point of control where they can automatically crypto-segment application flows across networks, clouds, and data centers inside or outside the enterprise, granting access to CryptoFlows based upon a user's role.

Even if hackers breach the firewall, they cannot access sensitive applications, because they are not an authorized user of that CryptoFlow. Furthermore, even if hackers compromise a contractor or member of the supply chain, the attacker can only get access to the CryptoFlow that the contractor was authorized for, like a billing or inventory management application. All other applications are safe on their own CryptoFlows, blocking lateral movement or hopping from application to application.

CryptoFlow cybersecurity solutions accelerate the rollout of new enterprise applications by cutting months of security architecture design and review. Now organizations can deploy secure applications faster, with more users, at lower risk.

CRYPTOFLAWS PROVIDE A
SINGLE POINT OF CONTROL
FOR END-TO-END
PROTECTION OF SENSITIVE
APPLICATIONS.

Conclusion

Threat prevention, detection and mitigation alone do not adequately address cybersecurity in the frictionless enterprise. Infrastructure-centric approaches to segmentation lack sufficient business controls and don't take into account the borderless nature of today's enterprises.

Correspondingly, cryptography-based approaches by themselves are insufficient to address the myriad types of attacks that today's hackers are likely to mount. Modern attack surfaces are simply too broad and diverse, and infrastructure-based encryption is too inflexible to support the fluid nature of modern applications and their users.

Breaches may still occur, as no security is perfect, but Certes' CryptoFlows effectively compartmentalize today's complex enterprise environments. As a result, crypto-segmentation dramatically reduces any organization's attack surfaces, making the attacker's job substantially more difficult. In most instances, this increased difficulty is sufficient to convince hackers to move onto easier targets at other organizations.

By leveraging encryption to raise segmentation from the infrastructure to the business layer and granting access to crypto-segments based on user roles, Certes Networks has implemented an effective, business-driven approach to securing the borderless, frictionless enterprise.

Certes Networks is an Intellyx client. Intellyx retains full editorial control over the content of this paper.