illumio

PAYING THE “INACTION TAX”:

THE INEVITABLE COSTS OF STATUS QUO SECURITY

WP201903

Every organization invests in its perimeter to prevent breaches. Yet an equal threat to the network is security behind the firewall. Once inside the perimeter, hackers often have little preventing their movement between applications, and sufficient time to do so undetected. In fact, global median "dwell time" – or the period of time between a breach and when it is discovered – reached 101 days in 2017[1]. This means attackers may have up to an entire business quarter to surveil your network, prioritize its most high-value targets, and successfully infiltrate them. The question, then, is not "if" you are going to be breached, but instead: how prepared are you?

The goal is to protect crown jewel applications and high-value assets. Ringfencing crown jewel applications can reduce your data center and cloud attack surface by 90 percent, preventing successful exfiltration of your most valuable data.

Most organizations cannot easily put a price on losing their most sensitive assets or information, but avoiding a reputational and competitive disaster is priceless. Often a major breach can force the end of operations in entire markets (think: GDPR) or the end of the business itself. However, there are other real-world costs of the fallout from breaches, both reputational and financial, as well as costs of inadequate security measures.

[1] https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

This paper quantifies:

1 The average global cost of a breach

2 The costs associated with regulatory non-compliance

3 The costs of status quo security to your organization

The Historical Cost of Breach

Factoring in both hard and soft costs, the Ponemon Institute lists the global average cost of a breach at $3,860,000. In the U.S., that average more than doubles to $7,910,000. If your company has no high-value assets or sensitive data to protect, this may be an acceptable loss—a tax you are willing to pay when it comes due periodically.

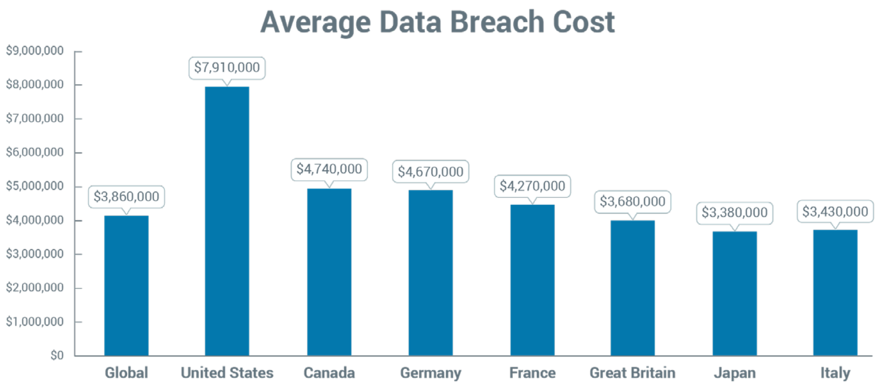


Figure 1: Average data breach cost, pre-GDPR, 2018
Source: https://www.ibm.com/security/data-breach

New regulations such as SWIFT and GDPR mandate compliance with standards for protecting a company's or country's most critical data, including that of its customers and partners, and preparing for breaches. Figure 2 below lists additional regulations aimed at consumer privacy, national security, and protection of industry. Their penalties include the risk of being excluded from industry-standard systems required to participate in banking in the case of SWIFT, or fines calculated by revenue for GDPR with a cap of 4 percent of total annual turnover. By mandating compliance, regulatory bodies have recognized the significance of business critical and sensitive information to the functioning of global business, requiring that corporations share the risk – and the pain– with joint responsibility.

Consumer Privacy	National Security / Infrastructure	Industry and Commerce
▪ General Data Protection Regulation (GDPR) ▪ California Consumer Privacy Act	▪ Continuous Diagnostics and Mitigation (CDM) – US Federal Government ▪ European Network and Information Security Directive (NIS) ▪ Military Programming Law of France (LPM)	▪ North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) ▪ Payment Card Industry Data Security Standard (PCI DSS) ▪ Society for Worldwide Interbank Financial Telecommunication (SWIFT) Standards ▪ New York Department of Financial Services (NYDFS) Cybersecurity Regulation

Figure 2: Recent regulations governing data security

Regulators have also taken note of the broader industry and global fallout of breaches, and are now attaching a punitive financial sting in the form of fines.

Considering the evolving regulatory environment, the status quo of non-compliance is not an option. The new cost of breach is no longer the cost of a breach itself, but breach plus fines.

The New Cost of the Status Quo

Even ignoring consequences like jail time, market exclusion, competitive disadvantage, organizational and personal reputational damage, and bankruptcy, combining the average breach costs with GDPR fines provides a new lens to look at the cost of a breach. Figure 3 estimates a potential small or medium-sized enterprise (SME) and enterprise-sized cost by revenue.

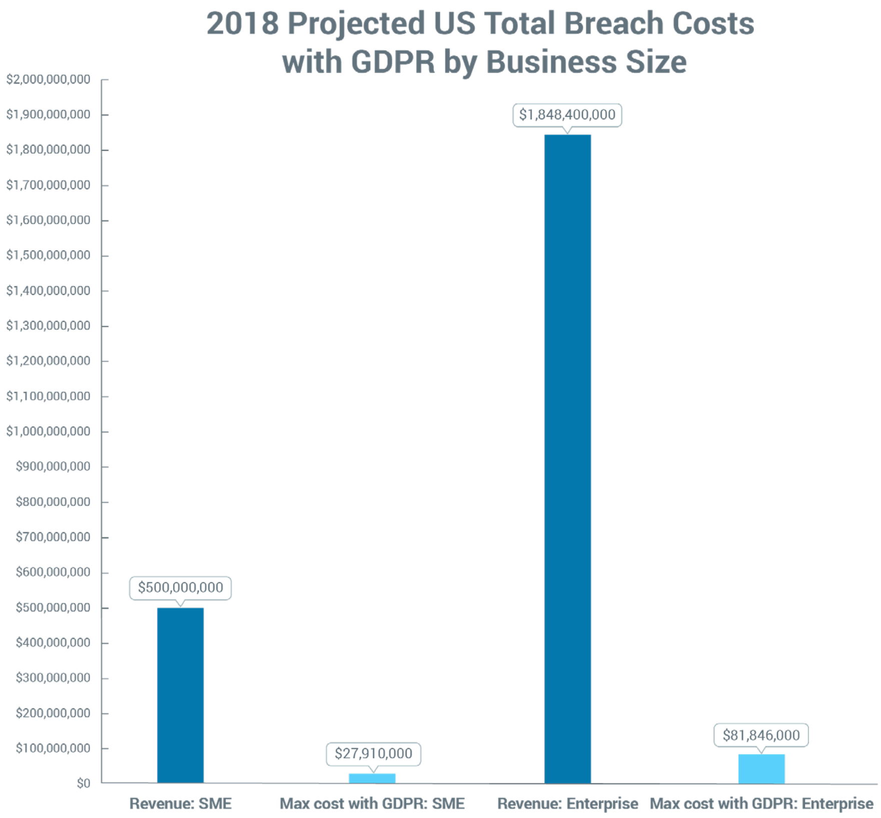
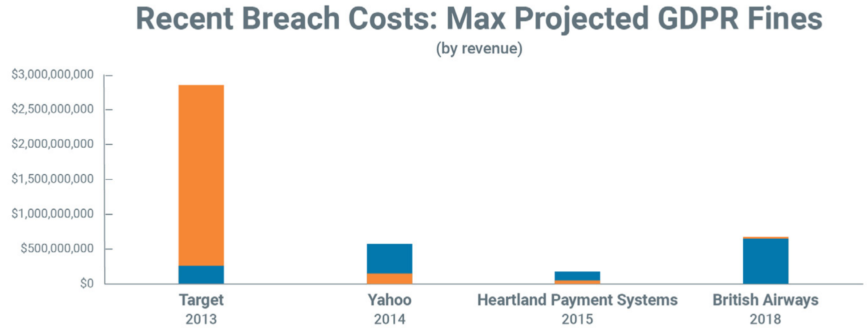


Figure 3: Estimated 2018 U.S. breach cost, including max GDPR fine (by revenue)

These numbers are conservative compared to some real-world examples. If we look at the largest data breaches in the last decade (figure 4 below), the costs are much more punitive than estimated averages—and with GDPR under enforcement since May 25, 2018, we can project how they would be compounded by fines equal to 4 percent annual revenue.



	Target 2013	Yahoo 2014	Heartland Payment Systems 2015	British Airways 2018
🟧 Projected GDPR fine	$2,851,200,000	$160,000,000	$32,920,000	$656,000,000
🟦 Cost	$202,000,000	$335,000,000	$140,000,000	$650,000,000

Figure 4: Historical breach costs with max projected GDPR fines

Traditionally, the percentage of overall operating costs dedicated to security has been approximately 3 percent (this may vary between organizations). The challenge that CISOs, CIOs, risk teams, and other technology leaders face is how to dramatically reduce the risk of the organization incurring a fine while not overspending on security.

What's more, using status quo technology to solve new world breach problems may more than double the spend on security (remember, technology refreshes only happen every five years). Now, instead of merely protecting the perimeter, organizations have to protect crown jewel applications and high-value assets as well.

No CFO wants to be presented with a bill that doubles the spend on security in a year. In fact, in both price and effectiveness, expecting status quo technology to adapt to modern security challenges may be like bringing a knife to a technical gunfight at a loss that no business can afford.

The Cost of Status Quo Security

Many organizations want to put a “micro-perimeter” around their most critical applications—commonly known as micro-segmentation. Micro-segmentation reduces risk by minimizing the attack surface that a bad actor can access by 90 percent or more. The challenges in creating micro-perimeters are:

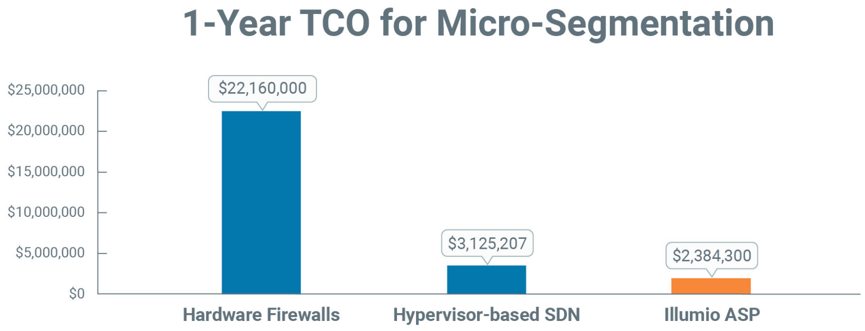
- Perimeters must not cause downtime for your crown jewel applications.
- Refactoring the network to change IP addresses, VLANs, and zones is a heavy lift.
    - Even if you can do this, there is a high probability you will have to purchase new infrastructure along the way, so it quickly becomes cost exorbitant.
- Even if you could make a point-in-time perimeter, it may not work in public cloud, and it may break if there are changes.

Implementing micro-segmentation using traditional infrastructure-based approaches with existing investments has trade-offs—not only in direct costs but, as stated above, in supporting the business and existing IT systems with the agility required to stay operational and competitive.

Can consistent policy management through micro-segmentation be deployed with traditional security infrastructure (firewalls, network switches, and hypervisors)? Yes—but at what cost?

Using traditional firewalls for micro-segmentation creates operational complexity[2] and unreasonable costs. Figure 5 compares the costs of different approaches to micro-segmentation, starting with host and infrastructure-based solutions.

[2] Complexity can also lead to misconfiguration, which is a leading action involved in breaches and security incidents per the Verizon breach report: https://enterprise.verizon.com/resources/reports/dbir/



Infrastructure Assumptions	Physical Servers	Workloads (VMs) per Server	Server NIC Bandwidth (Gbps)	Servers per Firewall Pair	Oversubscription Ration (20:1)	FW Price per Protected Mbps (1-year TCO)
	500	25	20	35	10	$9.07

Figure 5: 1-year total cost of ownership (TCO) for micro-segmentation solutions

The reasons for the cost differential are not only the face value cost and design limitations of infrastructure-based approaches, but their long-term limitations in supporting the speed of enterprise business efficiently from a deployment and operations perspective.

Some of these limitations include:

- Inconsistency – They are not flexible enough to be replicated across heterogeneous environments, including public cloud, with consistent, granular policy management.
- Opacity – They don't provide enough transparency to visualize your entire environment in real time.
- Speed – They are not built to be adaptive and keep up with the pace of business.
- Complexity – They are too complicated to scale to the operational needs of a limited security workforce with multiple functional commitments.

Benchmarking Your Organization’s Breach Preparedness

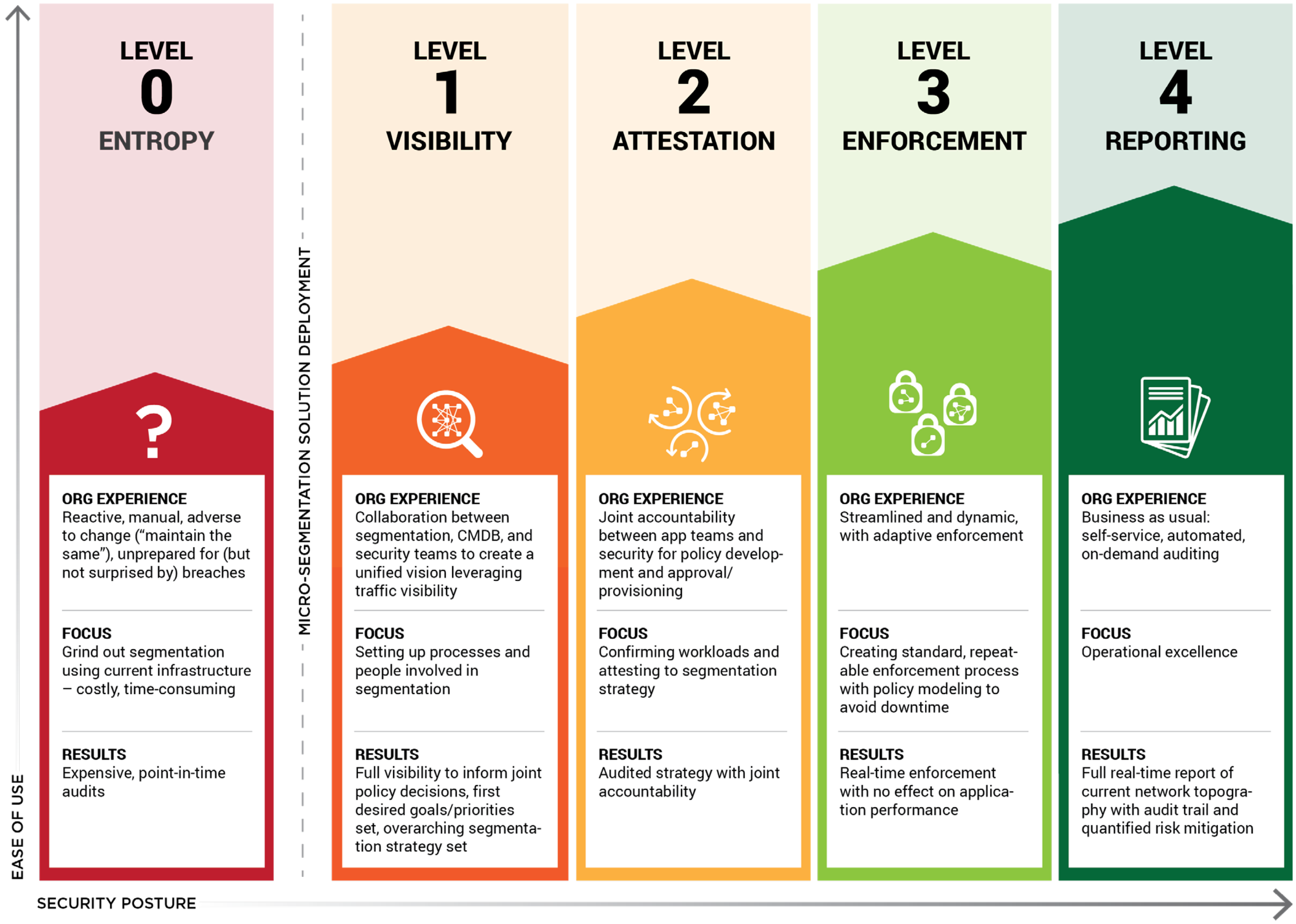
Most organizations struggle with how to compare themselves to others in their industry when it comes to breach preparedness. Establishing a common framework is an important first step to identifying and improving your security posture.

The following dimensions provide a framework to analyze your organization:

- Visibility – Do you have an accurate, real-time network topography for data in motion?
- Granularity – Can you enforce policies from entire environments down to processes running on individual hosts?
- Dynamic adaptation – Does your policy adapt to changes in your environment?
- Quantifiable risk mitigation – Can you measure your “before and after” risk mitigation?
- Reporting – Can you generate on-demand documentation of policy provisions?

How do you identify where you are, where you need to go, and how to get there?

The maturity model below maps out the common path in many organizations’ journey to compliance using micro-segmentation. It shows the value of attaining breach readiness for both the business and the IT organization, from initial mapping of application dependencies to providing real-time compliance documentation on demand.



	LEVEL 0 ENTROPY	LEVEL 1 VISIBILITY	LEVEL 2 ATTESTATION	LEVEL 3 ENFORCEMENT	LEVEL 4 REPORTING
ORG EXPERIENCE	Reactive, manual, adverse to change (“maintain the same”), unprepared for (but not surprised by) breaches	Collaboration between segmentation, CMDB, and security teams to create a unified vision leveraging traffic visibility	Joint accountability between app teams and security for policy development and approval/ provisioning	Streamlined and dynamic, with adaptive enforcement	Business as usual: self-service, automated, on-demand auditing
FOCUS	Grind out segmentation using current infrastructure – costly, time-consuming	Setting up processes and people involved in segmentation	Confirming workloads and attesting to segmentation strategy	Creating standard, repeatable enforcement process with policy modeling to avoid downtime	Operational excellence
RESULTS	Expensive, point-in-time audits	Full visibility to inform joint policy decisions, first desired goals/priorities set, overarching segmentation strategy set	Audited strategy with joint accountability	Real-time enforcement with no effect on application performance	Full real-time report of current network topography with audit trail and quantified risk mitigation

Figure 6: Maturity model for compliance using micro-segmentation

Conclusion

Protecting the perimeter is necessary but not sufficient. The worst consequences of a breach occur behind the perimeter in lateral attacks on crown jewel applications. Maintaining the status quo is no longer an option—especially because the cost of breach is now compounded by regulatory fines that can impact your business viability.

Using traditional security technologies to prepare your organization to be resilient in the event of a breach can double or triple the total security spend. Therefore, it is important to compare different solutions from a hard cost and soft cost perspective, while also evaluating the maturity of your organization compared to industry peers.

About Illumio

Follow Us

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information about Illumio, visit www.illumio.com/what-we-do or follow @Illumio.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com