3 STRATEGIES TO MANAGE COMPLIANCE MANDATES

Meeting security-related compliance requirements is an increasingly complex job. Focus on these three strategies to easily manage compliance.

"Most companies have between three and five different types of data classifications, ranging from public to top secret."

— STAN BLACK
CHIEF SECURITY OFFICER, CITRIX

Here's good news for security leaders: If you've established sound policies, enforce them rigorously, and thoroughly monitor and report security effectiveness, you're well on your way to protecting your company from today's growing swarm of increasingly potent threats. Now here's the bad news: More and more auditors, regulators, partners, and customers are demanding defensible proof of that fact.

"Globally, there are over 300 security and privacy-related standards, regulations, and laws with over 3,500 specific controls, with more coming all the time," says Stan Black, chief security officer at Citrix. "The people responsible for those rules want evidence that you're in compliance."

The consequences for disappointing auditors and regulators can be severe. Failure to comply with today's ever-expanding thicket of security-related compliance requirements can result in fines and penalties, outraged customers, loss of sensitive data, increased scrutiny from regulators, and costly damage to your organization's brand and reputation.

Not surprisingly, then, compliance has become a topic of intense interest to senior executives and board members. To bolster their confidence that your company meets all of its requirements—and can defensively prove it—follow these best practices:

1. Enable access while protecting information

Adopting a comprehensive approach to identify and access management, combined with an intense focus on sensitive data and relevant reporting and metrics is an important balance. Policies should specify granular data access privileges based on where employees are located, what network they're on, and which device they're using, with additional controls commensurate with risk. For example, access should be further scrutinized when utilizing a personally owned smartphone over a public network, than when using a company-owned laptop at the office.

Job role is another important variable. "You should grant access only to people who have a need to know for their role and function," advises Kurt Roemer, chief security strategist at Citrix. Role-specific training and automated role-based access control will ensure employees understand your policies and follow them.

You should also diligently enforce your policies with the

help of a robust security architecture. For example, data-focused security measures help protect data "in transit" across public and private networks, "at rest" in cloud-based or on-site storage, and "in use" on end-user devices. It also manages device security and other assets employees use to access information, builds tighter security controls into the company's applications and networks, and manages those controls both centrally and when management responsibilities are distributed.

2. Control sensitive data

Most security mandates apply chiefly to personally identifiable information, healthcare records, payment transactions, and other classified data. To comply with mandates, you must first identify sensitive data by creating a classification model for the various kinds of information your company creates, transmits, and stores.

"Most companies have between three and five different types of data classifications, ranging from public to top secret," Black says.

Next, make data classification assignments and prioritizations. To ensure the right data ends up in the right categories, involve a wide cross-section of stakeholders in this process, including representatives from your business groups, legal department, and operational functions.

Now you're ready to implement policies and enforcement mechanisms for securing data based on how sensitive it is, where it's stored, and where it's being accessed. For example, you might choose to control public data minimally regardless of user, network, and device, but limit access to confidential information on "bring your own" and consumer hardware. Always apply your strictest controls to your most sensitive data. "It makes sense to deny access to sensitive data altogether on devices and networks that can't be verified as appropriately secured," Roemer says.

Once again, security solutions can help you enforce classification-based policies automatically.

3. Audit, measure, and demonstrate compliance

Comprehensive security reporting is always important, but especially critical when it comes to compliance. "Auditors and others want to see clear evidence that you did what you said you would," Black says.

Satisfying those demands takes systematic logging, reporting, and auditing processes thorough enough to track when specific users access specific apps and data, and flexible enough to address new regulations and standards as they emerge. Create a reporting dashboard as well where authorized managers can see the latest compliance goals and results. "Otherwise you'll be pushing around spreadsheets that are out of date before anyone even gets them," Black notes.

Should an audit uncover gaps in your compliance measures, take a cradle-to-grave approach to resolving them by centrally tracking issues from detection to closure. Treat the people who found those issues as colleagues rather than adversaries. Internal auditors can help you eliminate risks and justify additional security investments. External auditors can provide valuable, unbiased feedback on your compliance regime.

Consulting with peers is often similarly helpful. Executives in your field may be reluctant to speak freely, but security leaders in other industries are often willing to exchange useful insights if everyone commits to nondisclosure agreements in advance.

Opportunities like this make clear that, for all its difficulties, compliance can pay real dividends. "Quite honestly, the reason most of these laws and standards exist is because businesses have struggled to understand and deliver a 'best practice,'" Black says.

Meeting today's constantly shifting compliance requirements is an excellent way to test your defenses regularly and keep them aligned with the business need for security. ■

MAKE COMPLIANCE SIMPLE AND SECURE WITH CITRIX

Beginning on May 25, 2018, the General Data Protection Regulation (GDPR) will implement a new legal framework in the European Union (EU) for the protection and distribution of personal data. Organizations around the world that serve customers and individuals in the EU will be required to put in place security policies to address different risks and effectively enforce these policies with technical controls—or potentially face fines of up to 4% of their global turnover.

While GDPR readiness can pose a significant challenge, many of its technical requirements align closely with security & compliance best practices already supported by Citrix solutions. These include centralizing apps & data in the data center or cloud so that data is not stored on devices; ensuring that data is protected in a secured enclave when it must be distributed; controlling access to resources with context-aware policies; and providing visibility & management capabilities that unite your entire IT infrastructure.

As organizations prepare for GDPR, Citrix can enable a simple approach to achieve compliance without impeding productivity.