SECURITY LEADERSHIP SERIES:

Security Strategies for Success

Are you protecting the information that matters most?
TABLE OF CONTENTS

5 STEPS TO CONTROL APPS AND DATA
PAGE 4

5 BEST PRACTICES TO MAKE SECURITY EVERYONE’S BUSINESS
PAGE 6

3 STRATEGIES TO MANAGE COMPLIANCE MANDATES
PAGE 8
SECURITY HAS NEVER BEEN SO CHALLENGING. Trends such as mobility, bring-your-own device and cloud computing mean that more people are accessing sensitive business information from more places and in more ways than ever before.

For IT, the challenge is to protect this information from loss, theft, and increasingly sophisticated threats while addressing privacy, compliance, and risk management mandates. Solid security strategies must include smart policies, rigorous enforcement, and deep monitoring/reporting, as well as provide people with the level of access to business resources that they need to be productive and get their work done.

Citrix, a recognized leader for its contributions to the advancement of information security, can help you proactively protect information, manage risk, and achieve compliance. You can rely on Citrix for the security of your business with an integrated and comprehensive secure digital workspace that unifies and enriches the end user experience; secures all types of enterprise applications and data; and simplifies IT’s ability to manage increasingly complex, hybrid, and multi-cloud environments.

Complemented by industry-leading security partners, Citrix offers holistic security solutions to help you address the growing cybersecurity threats of today while preparing for future requirements.

In this exclusive Security Leadership Series eBook, Citrix chief security officer Stan Black and chief security strategist Kurt Roemer share best practices for:

- Securing a business environment transformed by new technologies
- Engaging end users to protect business information
- Meeting security-related compliance requirements

For IT and security leaders, these security strategies for success are essential reading. Get started today.
The digital revolution has transformed business operations and models in many positive ways, and is delivering benefits that range from enhanced customer service to greater productivity to new revenue streams. But digital business transformation has also presented new opportunities for hackers, cyber criminals, and other bad actors. Never before have applications and data been more critical to business operations, or more at risk for theft, exposure, and corruption.

Even as organizations collectively spend billions of dollars to counter cyber threats, the diversity, volume, and sophistication of those threats continue to expand. Complicating matters further are shifting models of computing and networking.

In the past, corporations routinely kept their most sensitive systems and data secured in their central datacenters and enterprise-managed laptops. Nowadays, however, data and applications often reside on mobile devices within department-based solutions, or in cloud-based servers. All of these platforms and locations—plus the networks that interconnect them—require strong security controls that must enable an all-encompassing software-defined security perimeter.

Traditional tools and methods for securing apps and data have proven insufficient to adequately address the complexities inherent in today’s diverse business and threat landscape. Organizations—particularly those in highly regulated sectors—need to manage and mitigate cyber risks in ways that protect data at rest, in use, and in transit. Plus they must accomplish these goals even when their “user” community includes on-premises, remote, and mobile employees; third-party consultants; outsourcing vendors; and other business partners.

“Businesses need to take smarter steps to protect their most sensitive information—especially while threats are on the rise and more employees are going around security practices and policies because they’re too complex,” says Stan Black, chief security officer at Citrix. “The demand for devices and anytime, anywhere access often trumps security fears these days. No one can afford to assume that a device or network is inherently safe.”
To better secure their applications and data, organizations should integrate these best practices:

1. **Focus on balancing security and user-experience needs**
   When sensitive apps and data are threatened, security must take precedence over ease of access and ease of use. That said, successful organizations take a holistic view of security that strives to implement unobtrusive security controls and practices that won’t needlessly frustrate users or hinder productivity. Fortunately, some of the most effective security defenses are seamless and transparent to end users.

2. **Enable flexible options for data storage, access, and management**
   Businesses can benefit greatly from having a workforce that is mobile or widely dispersed. Inevitably, however, dispersed and internetworked users, devices, and systems provide cyber attackers with more targets. Companies need to devise and implement data management strategies commensurate with the value and sensitivity of the data at risk. For their most sensitive and critical data, for example, companies may decide to allow storage only on their most secure central servers, preventing distribution outside of company walls and imposing strict requirements and access procedures.

3. **Deploy a rich policy engine for contextual controls**
   Rather than giving users all-access passes to your data, apps, and networks, you should implement controls that can consider the context of each access request. With these controls, IT managers can set policies that factor in people’s titles and departments, their locations, the security of the networks they’re using, the capabilities of their endpoints, and even variables such as the time of day when they attempt to access data.

4. **Enable efficient compliance management and reporting**
   Globally, organizations must navigate more than 300 security and privacy-related standards, regulations, and laws which encompass more than 3,500 specific controls at present. To ensure compliance and meet auditing demands, security solutions need to provide complete and automated monitoring, logging, and reporting of data access, data movement, and network-level activities. It’s important that the solutions are flexible enough to easily accommodate new regulations and standards as they emerge.

5. **Reduce the attack surface while lowering IT costs**
   By controlling the distribution of data and providing contextual access, organizations can significantly reduce their attack surfaces. Those protections must include the routine use of encryption for apps and data at rest, in use, or in transit. In turn, with fewer exposed targets to protect, companies can lower their operational costs by avoiding purchases of individual device-centric security technologies.

**Citrix as a trusted security partner**
For nearly three decades, Citrix has served as a trusted IT partner for thousands of companies around the world. Customers rely on Citrix for the security of their business through an integrated and comprehensive secure digital workspace that unifies and enriches end user experience; secures all types of enterprise applications and data; and simplifies IT’s ability to manage increasingly complex, hybrid, and multi-cloud environments. The core security capabilities delivered by the Citrix portfolio include:

- **CONTEXTUAL ACCESS** — Gain the controls needed to ensure appropriate levels of access based on the user, endpoint, network, and security profile of every individual inside and outside your organization.
- **NETWORK SECURITY** — Provide encrypted delivery of applications and desktops to employees and third parties, enforce network access control and microsegment networks for compliance and security, while delivering the highest level of service uptime and performance.
- **APP SECURITY** — Centralize application and operating system patch management and configuration management, provide secure access to organizational resources—even from employee-owned devices—while mitigating advanced threats and denial-of-service attacks.
- **DATA SECURITY** — Prevent sensitive and highly valuable data from residing on endpoints by keeping it in the data center whenever possible. When data must be mobilized, address insecure mobile data storage with containerization, data encryption, and secure file sharing.
- **ANALYTICS AND INSIGHTS** — Gain the ability to triage user performance degradation to quickly identify the source, rapidly detect misconfigurations and attacks, and comply with regulations to reduce the scope of audits.

“Customers rely on Citrix as a security provider in the most demanding environments, including healthcare, government, education, manufacturing, and financial services,” says Kurt Roemer, chief security strategist at Citrix. “Combined with the strength of our Citrix Ready partnerships, Citrix empowers security across enterprise, cloud, and mobile, while streamlining the user experience.”

Customers from every industry, including the most highly regulated and targeted sectors, rely on Citrix to provide a secure digital workspace with a software defined perimeter that combines secure access to apps and data with contextual control, visibility, and behavior analytics across devices, networks, and clouds. This holistic security and analytics approach helps organizations address the growing cybersecurity threats of today while preparing for future requirements.
BEST PRACTICES TO MAKE SECURITY EVERYONE’S BUSINESS

Employees are one of your greatest risks to information security. Use these five proven techniques to strengthen your security strategy and protect your business.

Menaced by an ever-expanding array of increasingly potent threats, today’s highly mobile employees are frontline participants in the struggle to secure the enterprise. So while solid security strategies must include smart policies, rigorous enforcement, and deep monitoring/reporting, they must also reflect the needs and habits of the company’s users.

“End users are ultimately where security succeeds or fails,” says Kurt Roemer, chief security strategist at Citrix.

Unfortunately, keeping employees both safe and satisfied isn’t easy. Employees want anywhere, anytime access to information from any device without cumbersome security protections slowing them down. Business managers want to safeguard important information without inhibiting growth, innovation, and competitiveness. IT departments want to keep everyone productive while recognizing that employees and their devices are often the weak links in the security chain.

To balance those competing interests, security leaders should follow these best practices:

1. Educate users
An informed, security-conscious workforce is every company’s first line of defense against security threats, so teaching people how to work safely from any location on any device must be a top priority.

Simply preaching best practices is a recipe for failure. Take the time to understand who your users are, what they do, and what they need. Then explain your company’s security policies to them in terms that are easily understood and relevant to their role.

“Relevance is key,” Roemer says. “Everything you present should be specific to a person’s function rather than one-size-fits-all.”

It should also be personal, Stan Black, chief security officer at Citrix adds. For example, in addition to work-related security training, Citrix gives its employees advice on topics like securing a home wireless network and helping their kids use the Internet safely.

“We try to tie all our education efforts to the full lifecycle of...
security, not just what people do at the office," Black says. That makes security training more valuable for employees while also protecting sensitive data from poorly secured personal hardware.

2. Engage with line-of-business organizations
Close working relationships between IT executives and line-of-business managers are an essential ingredient for effective security. Meeting regularly with business decision makers empowers security leaders to build appropriate safeguards into new business initiatives right from the beginning. It also gives them an indispensable, up-close perspective on a business group’s unique risks and requirements.

“You’ll learn more about operational processes and potential dangers that you’d never know about otherwise," Black says. “You can then incorporate those insights into your security plans and make them even richer.”

3. Take a modern and mobile look at security policies
As critical as it is, training alone doesn’t ensure strong security. Many of the devices, networks, and storage systems employees rely on these days are outside of IT control.

"IT needs to update traditional security policies for the new mobile and cloud services reality," Roemer observes.

Start by thinking through how strictly you want to limit access to your company’s data based on where an employee is located and what kind of device they’re using. Most companies adopt graduated policies that protect sensitive information more carefully than public information and provide less access from consumer-grade and "bring your own devices" (BYOD) than from more thoroughly "locked down" enterprise-grade devices.

Then revise your security policies to reflect risks like storing business data on personally owned devices, posting passwords on a computer monitor, or using a USB storage device you found on the floor.

4. Enforce policies fairly and consistently
Security policies can lose value over time if users don’t believe violating them has consequences—or worse yet, if they believe bypassing them improves productivity. Policies must be maintained and kept current with the business. Security leaders must therefore enforce policies fairly and consistently.

“When policies are developed collaboratively across the company, and security awareness is woven into the culture, violations are infrequent," Black says.

5. Automate security seamlessly
To further reduce policy violations, use security software to automate policy enforcement. For example, many security solutions can implement desired behaviors—like encrypting business data on mobile devices—by default. They can also build tighter security into core elements of the user experience by automatically preventing employees from running unauthorized apps over the company network or limiting which apps people can open email attachments with, for example. Other solutions provide logging and reporting functionality that can help you prove to auditors that you’ve applied appropriate policies scrupulously.

Even so, software is ultimately just one piece of the security puzzle.

“To really protect the company you have to get to know your line-of-business groups and your end users," Roemer says.

Ultimately, the best security strategies are as much about people as technology.

MANAGE MOBILITY SECURELY WITHOUT COMPROMISING PRODUCTIVITY

Mobility has given people the freedom to work anywhere, at any time—but it has also brought endless complications. People want access to information from any device without cumbersome security protections slowing them down. Business managers want to safeguard important information without inhibiting growth, innovation, and competitiveness. IT and security departments want to keep users productive while recognizing that mobile devices accessing sensitive information are often the weak links in the security chain.

Citrix helps companies maintain the security of their apps and data even if an endpoint is lost, stolen, destroyed, or compromised. Our unique security solution creates a software-defined perimeter that combines secure access to apps and data with contextual control, visibility, and behavior analytics across devices, networks, and clouds. By extending control beyond the traditional datacenter to mediate user interactions with apps and data, IT can proactively secure, detect, and mitigate risk with intelligence applied to each unique scenario.

With Citrix, people can securely access the apps and data they need from any device—managed or unmanaged—they choose.

To find out more, please visit www.citrix.com/secure
Meeting security-related compliance requirements is an increasingly complex job. Focus on these three strategies to easily manage compliance.

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 defensibly 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 hardware. Always apply your strictest controls to your most confidential information on ‘bring your own’ and consumer devices,” 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.