The True Cost of SSO for SMBs

Electric Helpdesk

November 4th, 2019

Single Sign-On (SSO) is an essential part of any organization's security protocols. Businesses use it to relieve employees of password and credential fatigue, to save IT resources from doing countless password resets, and to mitigate damage in the event of a data breach.

What is Single Sign-On?

SSO is a centralized access control system in which a trusted third party verifies user credentials. In such a system, users can move from application to application without needing to log in each time. Well-known SSO vendors include Okta, OAuth, and OneLogin. SSO vendors usually provide additional functionality like two-factor (2FA) or multi-factor authentication (MFA) .

In the consumer space, platforms like Facebook and LinkedIn offer SSO access into multiple web applications. Social platform SSO allows companies to attract new customers without forcing them to create new usernames and passwords every time they want to use a new app.

The benefits of SSO include:

Reduced risk of data exposure since passwords are stored with a third-party

Ease of use for employees and increased likelihood that they will follow security procedures

Streamlined IT monitoring and management (e.g., universal user access or disabling)

The Importance of SSO for SMBs

SSO is an essential security requirement for any company that uses multiple SaaS applications and platforms. This means that SMBs—even those with just a handful of employees—need a centralized identity and authentication management system.

While news stories about data breaches often focus on large companies, the reality is that SMBs are increasingly becoming the victims. On average, a **cyberattack costs a small business $200,000** and 60 percent of victims **go out of business within six months** following a data breach.

Most vulnerability exploits, password exposures, and phishing scams happen to small businesses that don't have the security protocols in place to prevent these events or mitigate their damage. It's much easier for hackers to take advantage of security gaps at startups and small businesses than at established enterprises.

While SSO is certainly not the silver bullet to prevent cyberattacks, at the very least it should be a part of a company's security strategy. The cost of not implementing SSO is just too high to risk.

How Much will SSO Cost My Business?

There is no single answer to how much SSO will cost. How much you spend will depend on some the following SSO business requirements:

Training: How much training will your employees need to understand the SSO solution? How will the vendor conduct the training? How often will they

update you after the initial training?

Administration: Do you have an IT team in place to manage SSO after the vendor's initial training? Will you need ongoing consulting services for administrative support? How does the vendor structure its support services? (e.g., unlimited, charge per-request)

Infrastructure: What devices and hardware will you need for the SSO solution? How will you configure and maintain them? Can you modify what you already have?

Applications: Does the SSO vendor support most or all of the applications that your company currently uses? Is there a limit to how many applications it will support? Is there an individual fee for each one?

What Is the SSO Tax?

When calculating the cost of SSO, you will not only need to factor in the SSO requirements of the vendor, but also the requirements of each individual application your company uses. Despite the growing awareness around data security and the known benefits of SSO, many SaaS vendors **charge a premium** to clients who want to manage access through a third-party authenticator.

For some SaaS vendors, the price increase from base to SSO-enabled pricing can be more than 5x. While most SaaS vendors offer enterprise volume discounts, they require companies to have hundreds, if not thousands of users, meaning that many startups will not have access to them.

It's not as if these SaaS vendors are completely indifferent to security. Most have their own security and authentication mechanisms, so you might contemplate if having an SSO add-on is completely necessary.

In addition to preventing password fatigue and the other benefits mentioned earlier, SSO gives administrators more power to enforce security protocols most appropriate to their organizations. This includes requiring employees to use 2FA or MFA. Some SaaS vendors simply do not have that functionality in their products.

Electric's Stance on SSO

Small businesses should not have to compromise security in order to use a product affordably. If you are considering a product that charges a "tax" for SSO, do your research on the actual costs you'll incur.

At Electric, our business is providing IT management and **support for startups** and fast-growing SMBs. This also includes enforcing **cybersecurity best practices**.

Through our clients, we have come to understand the delicate balance that SMBs tend to juggle between cost and security. Security comes first at Electric and we work with our clients to provide the most appropriate solutions for them.

Related Blog Posts

Blog Post

SMB Cyber Security Best Practices

Blog Post

Best Cyber Security Practices for Password Management

🏷 PROACTIVE IT SUPPORT 🏷

Blog Post

Best Cybersecurity Practices for Your Small to Mid-Size Business

View All Blog Posts

Ready to modernize your IT?

Our Approach to Security

Product

Slack + Electric

Careers

Customers

Blog

Company

Customer

Login

Legal

Electric

New York

hello@electric.ai

What is Electric?

Electric is reinventing how businesses manage their IT security, support, and devices. Through its user-friendly interface, Electric streamlines time-consuming and business-critical IT tasks by providing accessible, lightning-fast support, and increased visibility into your IT infrastructure.

Contact Us