InfoSmart Technologies Inc.
SOFTWARE SOLUTIONS PROVIDER

STRENGTHENING SOFTWARE SECURITY:

EMBRACING DEVSECOPS AS THE ULTIMATE SOLUTION

Digital transformation has significantly changed how IT businesses operate, but it has also created new security challenges. Organizations often prioritize fast-paced service delivery and customer satisfaction over security, which makes their software development vulnerable to cyber-attacks. However, with the rise of DevSecOps principles, security integration has become integral to the software development life cycle (SDLC).

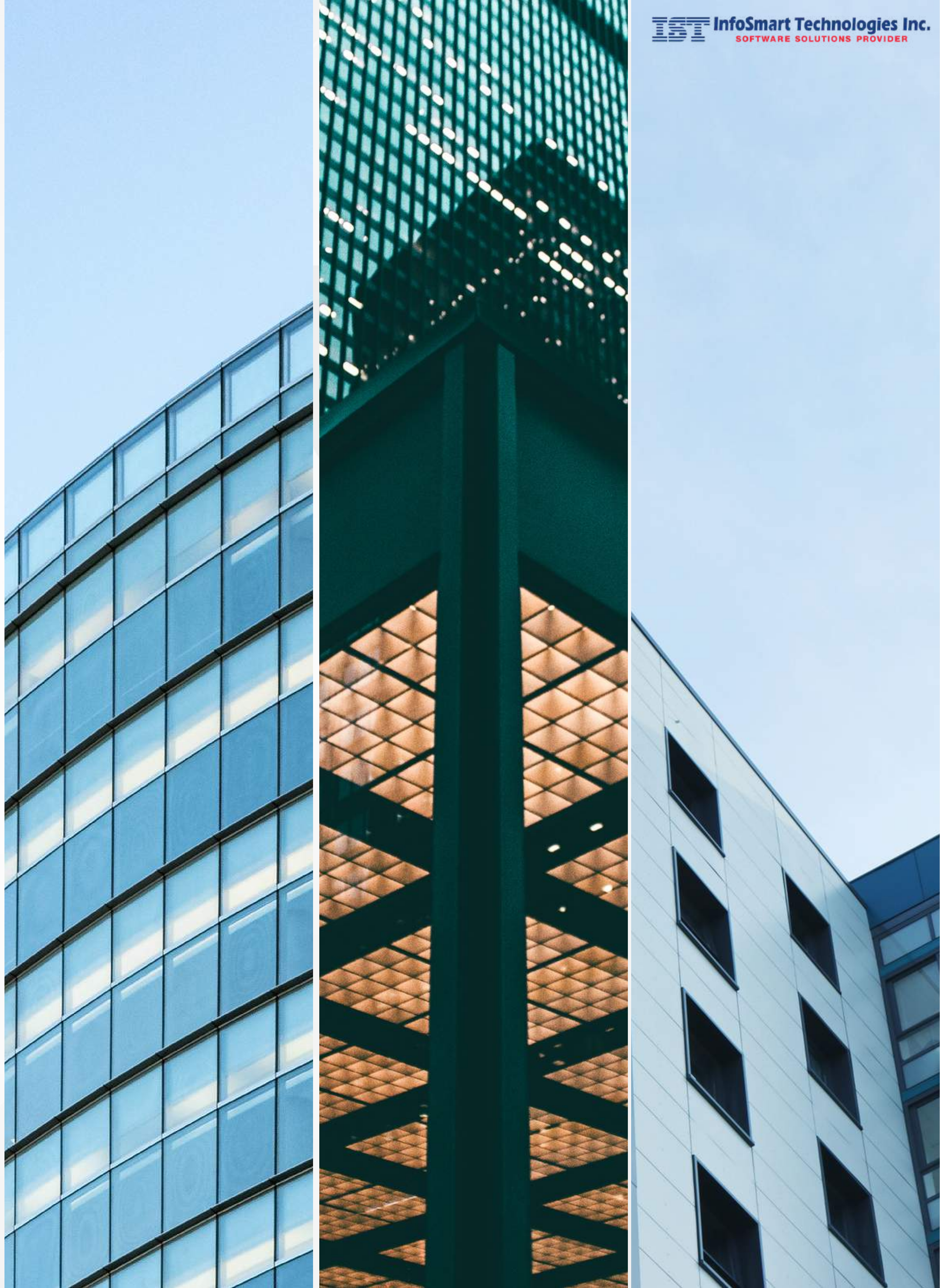
THE NEED FOR DEVSECOPS

In today's world, security breaches are costing organizations millions of dollars, making security an essential component of the business strategy. Cybersecurity threats are expected to cost the world over USD 6 trillion per year by 2021, highlighting the need for companies to rethink their security measures

Capital One (2019): In 2019, Capital One, a leading financial institution in the US, experienced a massive data breach that exposed the personal information of over 100 million customers. The breach was caused by a misconfigured firewall in their cloud infrastructure, which allowed a hacker to access sensitive data. This incident highlights the importance of implementing proper security measures, such as DevSecOps, to prevent such breaches

Equifax (2017): In 2017, Equifax, one of the largest credit reporting agencies in the US, experienced a data breach that exposed the personal information of over 140 million customers. The breach was caused by a vulnerability in their web application framework, which had not been patched for several months. This incident highlights the importance of prioritizing security updates and patching vulnerabilities as soon as they are discovered.

These case studies illustrate the importance of DevSecOps for businesses and the need to incorporate security into their overall business strategy. By implementing a DevSecOps approach, businesses can ensure that security is built into their software development process from the start, rather than being an afterthought. This can help prevent security breaches and protect customer data, leading to increased customer trust and improved business outcomes.



DEVSECOPS

VALUE ADDITION TO BUSINESS

01 COST REDUCTION

By automating application performance analysis in the design and development stages, DevSecOps nullifies the chances of security breaches and resultant losses.

02 INCREASED SECURITY

DevSecOps uses rigid infrastructure to reduce vulnerabilities, & insecure defaults, increase code coverage, and enhance automation. The immutable infrastructure allows companies to rebuild infrastructure with new credentials in the event of an attack.

03 INNOVATION

Regular security audits and monitoring help organizations stay ahead of hacking attempts, allowing for room to innovate in terms of security enhancements

04 SPEEDY RECOVERY

Security personnel employ templates or pet/cattle methodology to deal with a security incident, allowing for a faster recovery process.

05 EVERYONE RESPONSIBLE

DevSecOps promotes a culture of openness, presenting room for enhanced security right from the early stages of development. The collaborative approach of all stakeholders can enhance the security firewall against breaches.

06 SECURE DESIGN

DevSecOps enhances security by using automated security review of code, application security testing, and encouraging developers to use secure design patterns.

DEVSECOPS
TOOLS & IMPLEMENTATION

DevSecOps principles require integrating security tools and processes in the development cycle. Some popular DevSecOps tools include:

1. SonarQube: An open-source platform for continuous code quality inspection.
2. OWASP ZAP: An open-source web application security scanner that can detect vulnerabilities and prevent attacks.
3. Aqua Security: A container security platform that offers vulnerability scanning, runtime protection, and compliance management.
4. Checkmarx: A static application security testing tool that can scan code for security vulnerabilities.
5. GitLab: A source code management tool that can automate the deployment of code and monitor its performance.
6. JFrog Xray: An open-source software for analyzing and managing binary artifacts.

DEVSECOPS
INDUSTRY BENEFITS

DevSecOps principles apply to any industry that deals with software development. Some of the industries that have benefited from DevSecOps implementation include:

Financial Services: The finance industry has implemented DevSecOps to secure applications and meet regulatory compliance.

Healthcare: The healthcare industry has used DevSecOps to secure electronic health records and patient data.

Retail: Retailers have implemented DevSecOps to secure their e-commerce platforms and payment gateways.

Gaming: The gaming industry has used DevSecOps to secure their games and prevent cheating.

DEVSECOPS GLOBAL TRENDS & FORECAST

The DevSecOps market is expected to continue its strong growth in the coming years, driven by the increasing adoption of cloud computing, the rise of digital transformation, and the growing need for enhanced application security. According to a report by MarketsandMarkets, the global DevSecOps market size is expected to grow from USD 1.5 billion in 2020 to USD 13.9 billion by 2025, at a CAGR of 56.2% during the forecast period.

The report also identifies some key trends in the DevSecOps market, including.
:

1. Adoption of Artificial Intelligence (AI) and Machine Learning (ML): AI and ML are expected to become increasingly important in the DevSecOps market as organizations seek to automate security testing, improve threat detection, and enhance incident response.
2. The growing importance of containerization and microservices: As more applications are developed using containerization and microservices, there is a need for DevSecOps tools and processes that can support these technologies.
3. Integration with DevOps tools and processes: Integrating security into the DevOps process is becoming increasingly important as organizations look to streamline their software development lifecycle and improve their overall security posture.
4. Increased focus on compliance and regulatory requirements: With the growing number of data protection and privacy regulations, such as GDPR and CCPA, organizations are emphasising more on ensuring that their DevSecOps processes comply with these requirements.

GLOBAL DEVSECOPS MARKET RECENT DEVELOPMENTS

The DevSecOps market has rapidly evolved, with many new developments and trends emerging. Some of the recent developments in the global DevSecOps market are:

CLOUD-BASED DEVSECOPS SOLUTIONS

These are gaining popularity as they offer scalability, flexibility, and cost-effectiveness. Cloud-based DevSecOps solutions also allow organizations to implement DevSecOps practices seamlessly across their development and operations teams, enabling faster time-to-market and better software quality.

DEVSECOPS TOOLS & PLATFORMS

Many new DevSecOps tools and platforms are being introduced in the market, offering advanced security testing, analysis, and reporting capabilities. These tools and platforms are helping organizations to integrate security into their development and operations workflows seamlessly

GROWING ADOPTION OF DEVSECOPS IN SMES

DevSecOps is no longer limited to large enterprises. SMEs are increasingly adopting DevSecOps practices to enhance their software security and improve their competitiveness.

AI & MACHINE LEARNING IN DEVSECOPS

These are gaining popularity as they offer scalability, flexibility, and cost-effectiveness. Cloud-based DevSecOps solutions also allow organizations to implement DevSecOps practices seamlessly across their development and operations teams, enabling faster time-to-market and better software quality.

DEVSECOPS TRAINING & CERTIFICATION

DevSecOps training and certification programs are becoming more popular as organizations realize the importance of upskilling their development and operations teams in security. These programs offer comprehensive training in DevSecOps practices, tools, and techniques, enabling professionals to implement DevSecOps practices effectively.

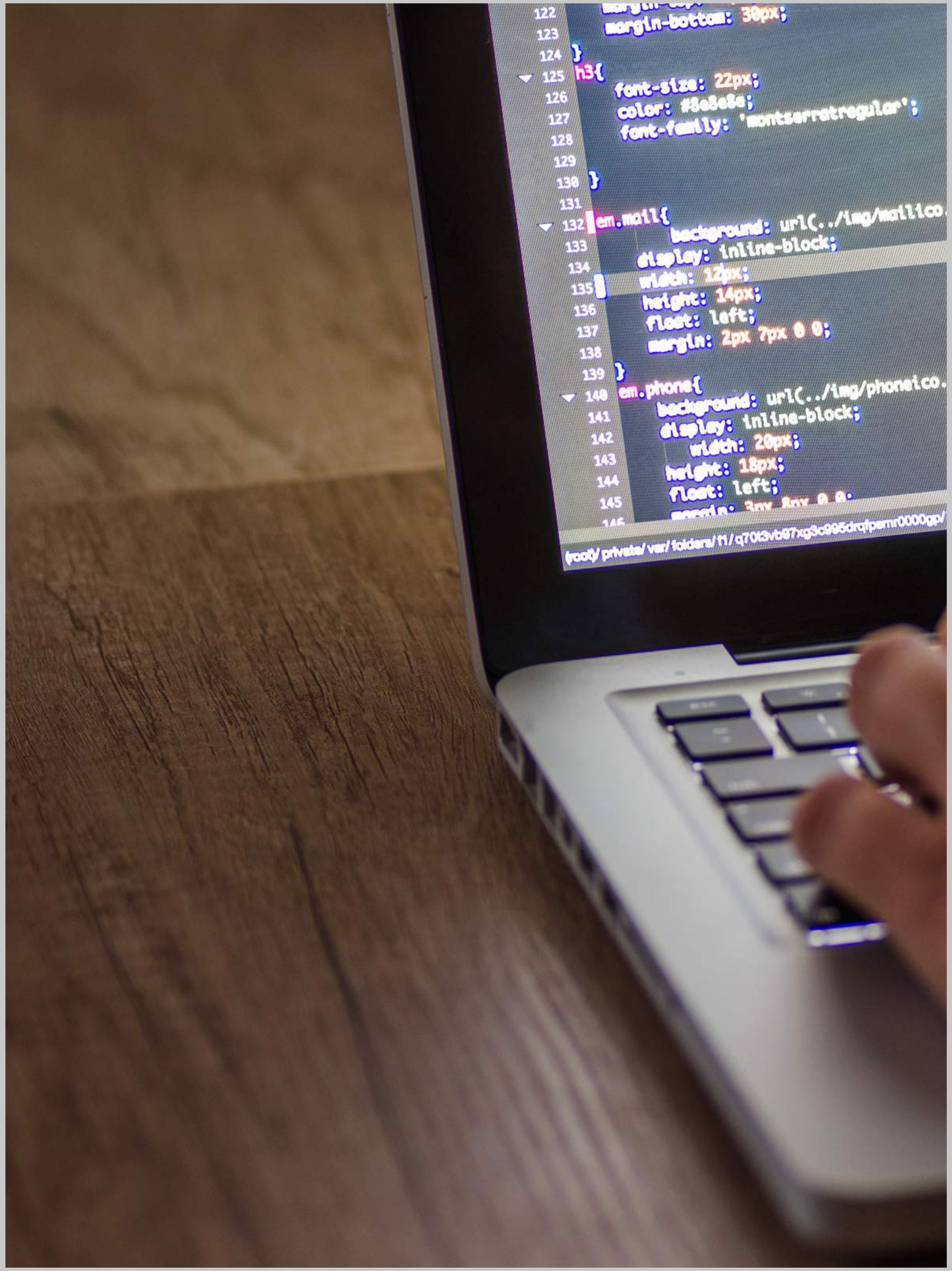
InfoSmart Technologies Inc.
SOFTWARE SOLUTIONS PROVIDER

DEVSECOPS SOLUTIONS PROVIDER

In today's digital world, security threats are constantly evolving and increasing in complexity, making it more important than ever for businesses to prioritize their security needs. By implementing DevSecOps practices, companies can ensure that security is integrated into every stage of the software development lifecycle, from planning and development to deployment and maintenance.

At InfoSmart Technologies, we specialize in providing DevSecOps solutions that enable businesses to stay ahead of security threats and protect their valuable assets. Our team of experienced professionals can help you assess your security needs, design and implement customized DevSecOps solutions, and provide ongoing support to ensure that your systems remain secure.

Contact us today to learn more about how we can help you achieve your security goals and keep your business safe from cyber threats.



```
margin-bottom: 30px;
}
h3{
    font-size: 22px;
    color: #8e8e8e;
    font-family: 'montserratregular';


}

em.mail{
        background: url(../img/mailico.
    display: inline-block;
    width: 12px;
    height: 14px;
    float: left;
    margin: 2px 7px 0 0;
}
em.phone{
        background: url(../img/phoneico.
    display: inline-block;
        width: 20px;
    height: 18px;
    float: left;
    margin: 3px 8px 0 0;
```

```
(root)/ private/ var/ folders/ f1/ q70t3vb97xg3c995drqfpsmr0000gp/
```

ISO

9001-2015
20000-1:2018
27001:2013

SBA
U.S. Small Business Administration
8(a) CERTIFIED

GSA IT Schedule 70 Contract Holder

NMSDC
National Minority Supplier Development Council

DISADVANTAGED BUSINESS ENTERPRISE
DBE
CERTIFIED

CONTACT US

☎ +1-833-782-7165

✉ mail@infosmarttech.com

🌐 infosmarttech.com

📍 Suwanee, Georgia 30024