Main Menu

Prepare

Prepare and train your organization to defend against sophisticated threat actors using real-life simulation exercises.

Tabletop Exercise

Red Team / Blue Team Exercise

Adversary Emulation Exercise

Penetration Testing

Respond

Available under a Services Retainer, giving you access to security consultants and expertise to respond to a breach.

Incident Response

Compromise Assessment

Endpoint Recovery

Network Detection

Experienced a breach?

Fortify

Enhance your cybercsecurity practices and controls with actionable recommendations to fortify your cybersecurity posture.

Maturity Assessment

Technical Risk Assessment

SOC Assessment

Active Directory Assessment

Managed Services

Managed Detection & Response

Included in Falcon Complete and backed by CrowdStrike's Breach Prevention Warranty.

Managed Threat Hunting

Falcon OverWatch, as an extension of your team, hunting relentlessly to stop hidden threats.

Managed LogScale

Managed service that combines centralized log management technology with CrowdStrike's industry leading service expertise.

Additional Services

Cloud Security Services

Identity Protection Services

Falcon LogScale Services

Partner Services

- Why CrowdStrike?

Main Menu

Why CrowdStrike?

Considering Microsoft?

Compare CrowdStrike
See how we stack up against our competitors
Industry recognition
CrowdStrike is the recognized leader in endpoint protection solutions.
Customer stories
Don't take our word for it, hear what our customers have to say.

Solutions by topic
Zero Trust
Real-time breach protection on any endpoint, cloud workload or identity, wherever they are.
Cloud security
Stop cloud breaches for multi-cloud and hybrid environments in a single platform.
Ransomware protection
Learn what you can do to stop ransomware threats in their tracks.
Log4Shell mitigation
Get the latest information on this evolving vulnerability.
Observability & log management
Fills in the gaps, logs everything, and realizes real-time observability for your entire system.
Find your solution
Identify the best CrowdStrike solution for your business.

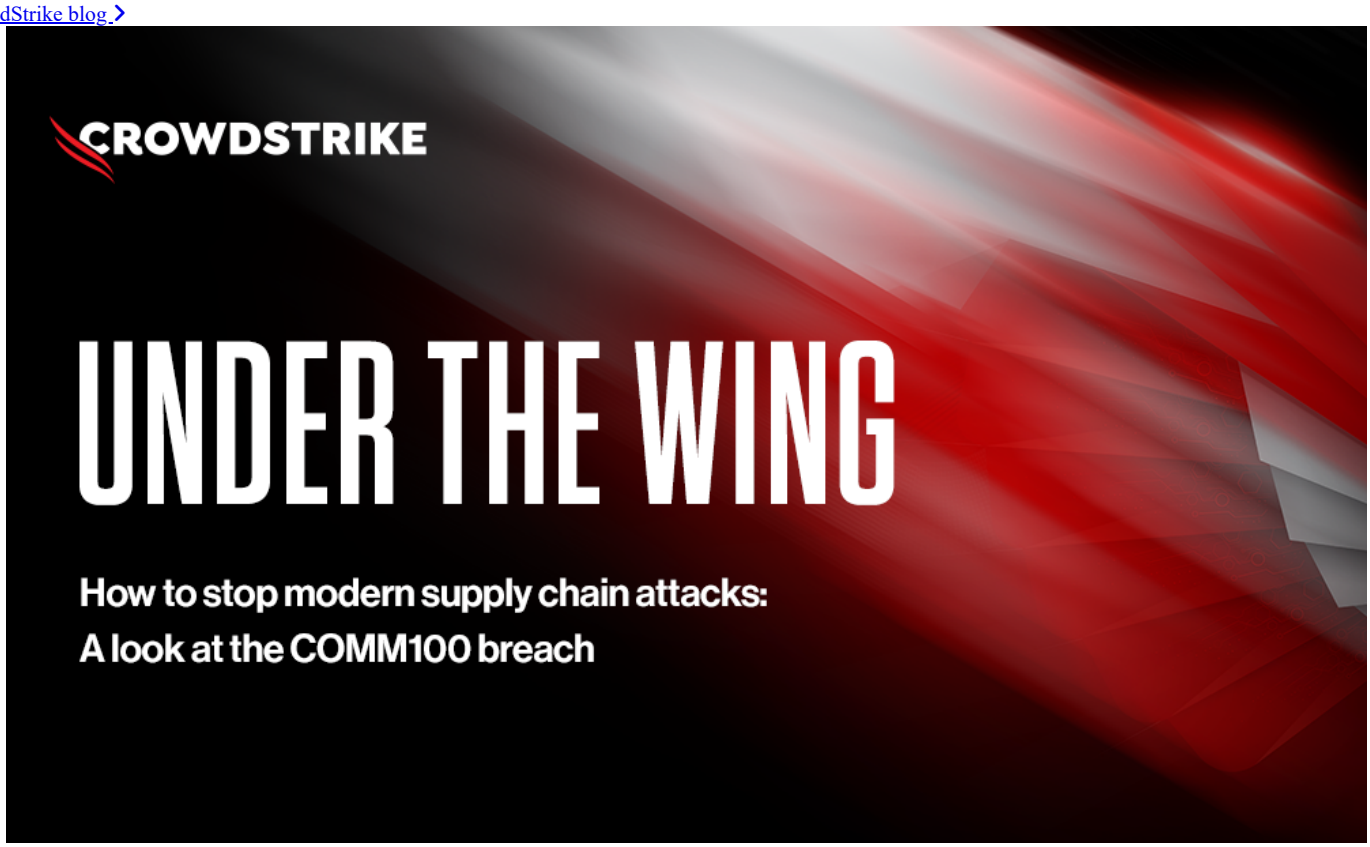
Solutions by industry
Small business
Election security
Public sector
Healthcare
Financial services
Retail

- Learn
  Main Menu

Featured resources
Considering Microsoft?
Cyber risk that starts with Microsoft ends with CrowdStrike

Cybersecurity 101 glossary
Explanations, examples and best practices on a variety of cybersecurity topics.
Get your threat landscape
Discover the adversaries targeting your industry.
2023 Global Threat Report
The highly anticipated annual threat report is here!
2022 Threat Hunting Report
CrowdStrike's threat hunting insights from July 1, 2021 to June 30, 2022.

CrowdStrike blog



Discover how CrowdStrike protects you against the most advanced attacks.
From the front lines
Executive viewpoint
Research & threat intelligence

Customer focused
Free trial guide
Customer support portal
CrowdStrike University
CrowdStrike Tech Center
Developer portal

Knowledge resources
Case studies
White papers
Webinars
Reports
Logging guides
All resources

- Company
Main Menu

Connect with us
Careers
Events
Fal.Con 2023
Falcon Encounter Hands-on Labs

Partner programs
Cloud providers
Technology partners

‹ Main Menu

Prepare ›

Prepare and train your organization to defend against sophisticated threat actors using real-life simulation exercises.

Tabletop Exercise ›
Red Team / Blue Team Exercise ›
Adversary Emulation Exercise ›
Penetration Testing ›

Respond ›

Available under a Services Retainer, giving you access to security consultants and expertise to respond to a breach.

Incident Response ›
Compromise Assessment ›
Endpoint Recovery ›
Network Detection ›

Experienced a breach?

Fortify ›

Enhance your cybercsecurity practices and controls with actionable recommendations to fortify your cybersecurity posture.

Maturity Assessment ›
Technical Risk Assessment ›
SOC Assessment ›
Active Directory Assessment ›

Managed Services

Managed Detection & Response ›

Included in Falcon Complete and backed by CrowdStrike's Breach Prevention Warranty.

Managed Threat Hunting ›

Falcon OverWatch, as an extension of your team, hunting relentlessly to stop hidden threats.

Managed LogScale ›

Managed service that combines centralized log management technology with CrowdStrike's industry leading service expertise.

Additional Services

Cloud Security Services ›
Identity Protection Services ›
Falcon LogScale Services ›
Partner Services ›

‹ Main Menu

Why CrowdStrike? ›

Considering Microsoft? ›

Compare CrowdStrike
See how we stack up against our competitors
Industry recognition
CrowdStrike is the recognized leader in endpoint protection solutions.
Customer stories
Don't take our word for it, hear what our customers have to say.

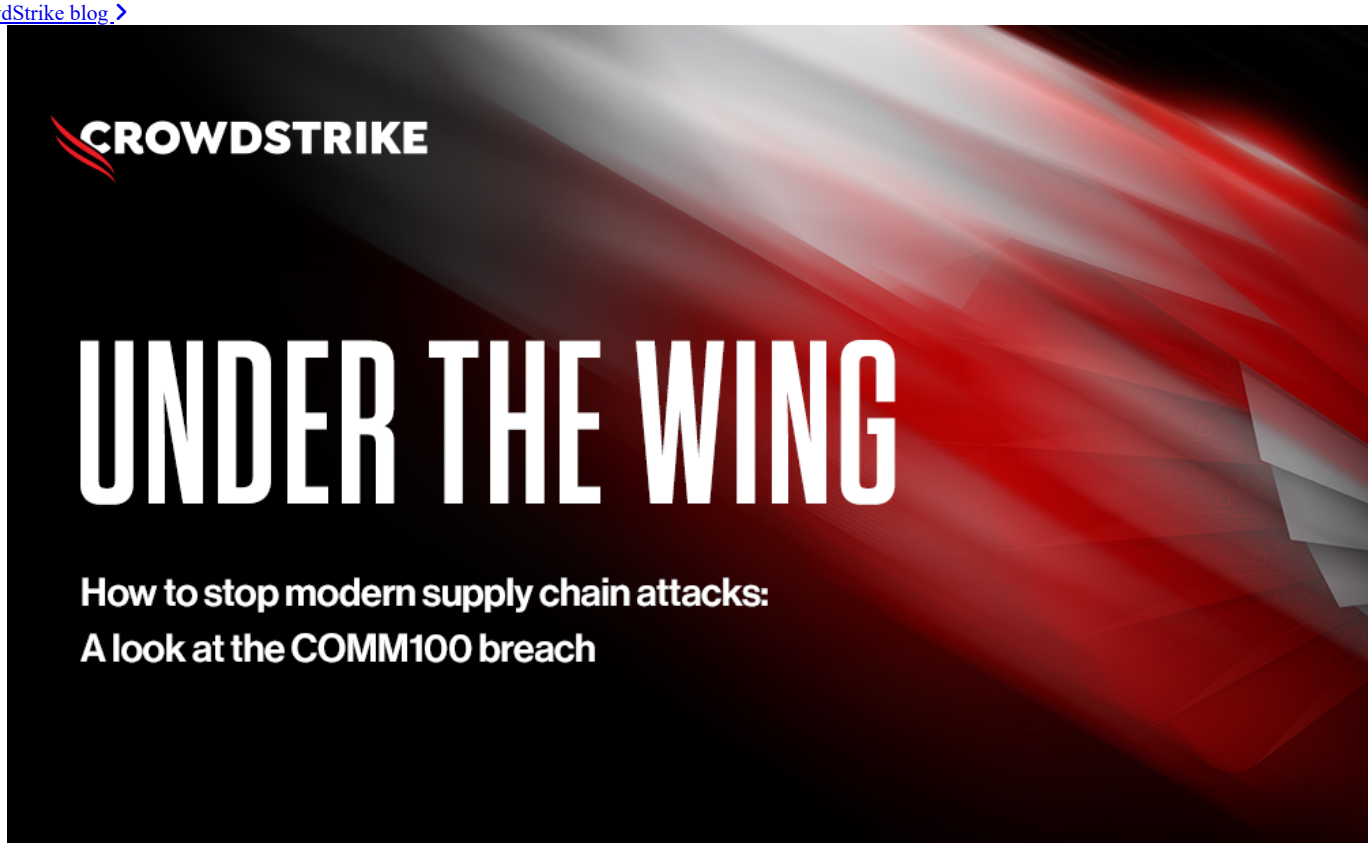
Solutions by topic
Zero Trust
Real-time breach protection on any endpoint, cloud workload or identity, wherever they are.
Cloud security
Stop cloud breaches for multi-cloud and hybrid environments in a single platform.
Ransomware protection
Learn what you can do to stop ransomware threats in their tracks.
Log4Shell mitigation
Get the latest information on this evolving vulnerability.
Observability & log management
Fills in the gaps, logs everything, and realizes real-time observability for your entire system.
Find your solution
Identify the best CrowdStrike solution for your business.

Solutions by industry
Small business
Election security
Public sector
Healthcare
Financial services
Retail
Main Menu

Featured resources
Considering Microsoft?
Cyber risk that starts with Microsoft ends with CrowdStrike
Cybersecurity 101 glossary

Explanations, examples and best practices
on a variety of cybersecurity topics.
Get your threat landscape
Discover the adversaries targeting
your industry.
2023 Global Threat Report
The highly anticipated annual
threat report is here!
2022 Threat Hunting Report
CrowdStrike's threat hunting insights
from July 1, 2021 to June 30, 2022.

CrowdStrike blog



Discover how CrowdStrike protects you against
the most advanced attacks.
From the front lines
Executive viewpoint
Research & threat intelligence

Customer focused
- Free trial guide
- Customer support portal
- CrowdStrike University
- CrowdStrike Tech Center
- Developer portal

Knowledge resources
- Case studies
- White papers
- Webinars
- Reports
- Logging guides
- All resources

Main Menu

Connect with us
- Careers
- Events
- Fal.Con 2023
- Falcon Encounter Hands-on Labs

Partner programs
- Cloud providers
- Technology partners
- Solution providers
- View all

SOFTWARE SECURITY: DEFINITIONS AND GUIDANCE

October 26, 2022

Today’s businesses rely on an increasing number of software programs to perform critical tasks. As companies continue to adopt digital solutions, software security threats are also growing in strength and frequency. Viruses, malware and other threats can put sensitive data at risk.

As a business, you want to ensure you have the strongest software security possible to protect your organization. Here's a quick breakdown of what software security means, why it's important, and how to implement, ensure and improve your protocols.

Software Security Definition

Software security refers to a set of practices that help protect software applications and digital solutions from attackers. Developers incorporate these techniques into the software development life cycle and testing processes. As a result, companies can ensure their digital solutions remain secure and are able to function in the event of a malicious attack.

Why Is Software Security Important?

Secure software development is incredibly important because there are always people out there who seek to exploit business data. As businesses become more reliant on software, these programs must remain safe and secure. With strong software security protocols in place, you can prevent attackers from stealing potentially sensitive information such as credit card numbers and trade secrets, and build trust among users.

The theft of critical data can be catastrophic for customers and businesses alike. Malicious actors can abuse sensitive information and even steal users' identities. Additionally, companies can face legal penalties in the event of a data breach and suffer reputational harm.

Businesses can work to protect critical data by implementing software security techniques into their development life cycles. Applying security techniques enables organizations to proactively identify system vulnerabilities and better protect their software.

What Is the Difference Between Software Security and Cybersecurity?

While the terms “software security” and “cybersecurity” may sound interchangeable, they actually refer to two different concepts. Software security protects or secures software programs from malicious threats, such as viruses or malware.

Cybersecurity is much broader. Also known as computer security or information security, cybersecurity protects networks, systems and programs. Cybersecurity threats may include trojan horse and ransomware attacks.

Software Security Issues

In today’s complex information technology (IT) landscape, software is an integral tool and more widespread than ever. However, security issues are just as prevalent, making it necessary to prioritize software security.

Why Security Is a Software Issue

Businesses constantly use software to manage finances, sell products, track customer data, collaborate on projects and communicate with teammates. With so much business activity happening via digital channels, it is critical to protect them.

System vulnerabilities are security flaws or weaknesses that appear in a software’s code. Hackers can exploit these vulnerabilities to access software programs, steal valuable data and destroy important systems.

To prevent a software threat, security must be a critical part of software development and testing. By integrating security best practices with these

processes, developers can identify and fix vulnerabilities before hackers have a chance to find them.

Major Concerns with Software Security

A security vulnerability can have major implications for healthcare organizations, financial institutions, homeland security agencies and more. It is important to identify these concerns quickly and proactively to avoid malicious attacks.

Below are some of the top software security issues businesses are facing:

- **Phishing**: Phishing happens when an attacker poses as someone else in an attempt to gain personal information, such as software credentials.
- **Distributed denial of service (DDoS) Attacks**: A DDoS attack happens when an attacker overloads servers with packets, causing the software to crash.
- **Cloud service attacks**: Companies are increasingly relying on cloud-based services to support remote workers. Some cloud infrastructure has vulnerabilities hackers can exploit.
- **Software supply chain attacks**: Some pieces of software are critical in the business supply chain, especially for e-commerce. A software supply chain attack happens when hackers exploit a third-party service to access data about a business.

Software Security Tools and Responsibilities

Building secure software is a group effort. All stakeholders in software development, from developers to executives, need to understand how software security practices benefit them. They must also understand the risks of not implementing them and allocate proper resources to security tasks.

There are several tools that an organization can leverage for software security:

- **Static application security testing**: This tool examines source code at rest and flags vulnerabilities for developers to fix.
- **Dynamic application security testing**: This tool examines an application's code while it is running and detects weaknesses in the software.
- **Software composition analysis**: This tool checks for vulnerabilities against a software's governance guidelines. Software composition analysis is especially valuable for open-source software.
- **Mobile application security testing**: This tool analyzes mobile code to identify specific vulnerabilities that could lead to unique security risks, such as improper platform usage and insecure data storage.

Software Security Best Practices

Malicious users often target vulnerable areas of software in order to access, use or destroy different programs. However, secure software development can help prevent these events from occurring. Here are a few key best practices for implementing, ensuring and improving software security.

Implementing Software Security

From the beginning of development, it is important to implement foundational security best practices. Here are a few examples:

- **Implement least privilege**: Least privilege refers to the practice of giving software users limited access to a program. A hacker will not be able to access features, rights and controls that a user does not have, helping minimize the impact of an attack.

- **Encrypt software data**: Data encryption transforms readable data into an unreadable, protected format. If a hacker is able to access this information, they would not be able to use it unless they have the encryption key. Make sure to encrypt all software data at rest and in transit.

- **Automate software security tasks**: It can be difficult to monitor your entire infrastructure for vulnerabilities. Consider investing in security software that performs these tasks for you. With automation, you can reduce human error and increase the scope of your security protocol.

- **Implement two-factor authentication**: This security protocol requires a user to provide two pieces of information in order to log into their account, such as sending a text to their phone. A hacker won't be able to access the system even if they have one set of credentials.

- **Perform employee training**: All employees need to be aware of the importance of software security and know how to protect themselves and their data. Software security teams can host regular training sessions to keep everyone up to date.

Ensuring and Improving Software Security

Secure software development is an ongoing process. All new features, tools and software should adhere to security protocol and be free of vulnerabilities. To ensure and improve software security, it is important to:

- Embed security improvements in the development life cycle.
- Implement security best practices into the design and development of new features.
- Perform regular application testing to identify potential weaknesses.
- Patch or fix a vulnerability as soon as someone detects it.
- Regularly update security protocol to stay ahead of evolving software security threats.

Learn More About Software Security

Software security is essential to make programs free of vulnerabilities and avoid attacks that could leak sensitive data. If your company is engaging in software development, it is critical to perform regular testing and follow application security best practices.

However, these processes can be time-consuming and complex. Investing in security software can help your business maintain strong protocols and reduce vulnerability.

The CrowdStrike Falcon® platform can help you secure the most critical areas of software risk. Using this unified cloud-native platform, you can protect your business against security threats while gaining complete visibility into your infrastructure, applications and more. Learn more about the Falcon platform and its powerful features here.

Most Common Types of Cyber Vulnerabilities

What Is Cybersecurity? Definition, Types, Tips, and More

What is a Cyberattack?

Start your

- Definition
- Issues
- Tools
- Best Practices
- Learn More

en easier. Take advantage of our free 15-day trial and explore the most popular solutions for your business:

e with next-gen antivirus.
with USB device control.
wall management.
ghts with automated threat intelligence.

New to CrowdStrike?

About the platform
Explore products
Services
Why choose CrowdStrike?

Company
- About CrowdStrike
- Careers
- Events
- Newsroom
- Partners

Learn with CrowdStrike
- 2023 Global Threat Report
- Cybersecurity 101
- Your Threat Landscape
- Tech Center
- View all resources

Contact us
- Experienced a breach?

Not sure where to start?
- Help me decide