
INTERACTIVE CYBERSECURITY SCENARIOS EBOOK

Real scenarios. Smarter decisions. Stronger defenses.

Dell's commitment to security is at the core of everything we do. By sharing insights, best practices, and innovative technologies, this eBook aims to empower you with the tools and knowledge needed to stay ahead of emerging cyber risks.



Choose an attack scenario

Cybersecurity threats are constantly evolving, and organizations need to respond effectively to protect their data. To best prepare your organization, immerse yourself in real-world simulation exercises to help navigate your cybersecurity strategies to combat cyberattacks.

Explore a wide range of attack types and industry-specific challenges across sectors like federal, state, and local government, financial services, and healthcare. Along the way, you'll discover how Dell's integrated security solutions—from laptops and desktops to enterprise systems—are built to safeguard against these threats.

[Backup Infiltration](#)[Ransomware](#)[Distributed Denial of Service \(DDoS\)](#)[Supply Chain Hardware](#)[Malicious Insider](#)[Supply Chain Software](#)[Man-in-the-Middle \(MITM\)](#)[Zero-Day](#)[Prompt / SQL Injection](#)

A man with a grey beard and glasses, wearing a light blue button-down shirt and a lanyard, is working in a server room. He is looking intently at a server rack. The room is dimly lit with blue ambient lighting. The background shows rows of server racks and a door.

Attack Type: Backup Infiltration

As the manager of a cloud backup service provider, one evening you get a phone call from a client who is trying to restore some data that they lost.

They have tried multiple times to recover from your cloud, and the recovery always fails.

You go to the office to find all the computer screens say all data has been encrypted and to regain access to the data you need to pay a ransom.

[Test Your Knowledge →](#)

Attack Type: Backup Infiltration



You're not sure which backup systems or customers have been impacted. What should be your first step?

Notify the authorities

Shut down all the systems

Try to contain and isolate the threat

Identify if you have a clean backup to restore from

[See The Correct Answer →](#)



Attack Type: Backup Infiltration



You're not sure which backup systems or customers have been impacted. What should be your first step?

- Notify the authorities
- Shut down all the systems
- Try to contain and isolate the threat
- Identify if you have a clean backup to restore from.

Immediately containing and isolating a threat prevents further spread or damage and allows time to assess the scope of the incident, potentially minimizing the impact for all types of cyberattacks, including those involving AI.

[Next Question →](#)



Attack Type: Backup Infiltration



Your priority is to get your customers' data available to them quickly. How would you accomplish this?

Pay the ransom

Identify the ransomware strain

Notify the authorities

Identify what data has been compromised

[See The Correct Answer →](#)



Attack Type: Backup Infiltration



Your priority is to get your customers' data available to them quickly. How would you accomplish this?

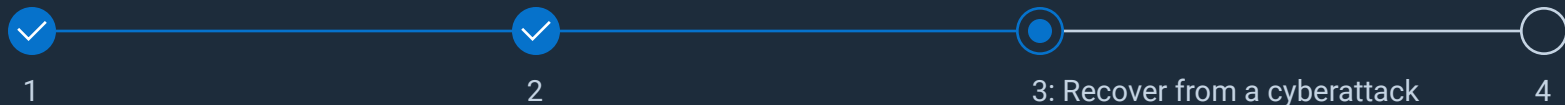
- Pay the ransom
- Identify the ransomware strain
- Notify the authorities
- Identify what data has been compromised

Identifying compromised data helps focus recovery efforts on restoring the most critical customer information, ensuring faster data availability, and avoiding unnecessary work on unaffected systems.

[Next Question →](#)



Attack Type: Backup Infiltration



You identify you have a backup to recover from. What should be the first step in your process?

Prioritize restoring critical systems first

Use forensic analysis to confirm the attack is fully contained

Change all passwords and revoke compromised credentials

Implement zero trust principles

[See The Correct Answer →](#)



Attack Type: Backup Infiltration



You identify you have a backup to recover from. What should be the first step in your process?

- Prioritize restoring critical systems first
- Use forensic analysis to confirm the attack is fully contained
- Change all passwords and revoke compromised credentials
- Implement zero trust principles

Before restoring systems, you need to ensure the attack is fully contained to help prevent accidental reinfection and further damage to avoid perpetuating or escalating threats in your environment.

[Next Question →](#)



Attack Type: Backup Infiltration



1



2



3



4: Overall best practices

What are potential ways to mitigate risk of this happening in the future?

Utilize zero trust principles

Enable Endpoint Detection and Response (EDR) capabilities

Implement immutable and air-gapped backups

All of the above

[See The Correct Answer →](#)



Attack Type: Backup Infiltration



What are potential ways to mitigate risk of this happening in the future?

- ✓ Utilize zero trust principles
- ✓ Enable Endpoint Detection and Response (EDR) capabilities
- ✓ Implement immutable and air-gapped backups
- ✓ All of the above

Using a multi-layered defense strategy can reduce risk, minimize damage, and enhance organizational resilience as no single measure is sufficient on its own.

[See Solutions →](#)



ATTACK TYPE: BACKUP INFILTRATION

Recap

Backup infiltration occurs when cybercriminals exploit vulnerabilities in backup systems to compromise, destroy, or encrypt critical recovery data. These sophisticated attacks may coincide with or follow other incidents, such as ransomware or malware deployment, amplifying the operational and financial fallout.

At Dell, we believe in empowering organizations to stay resilient in the face of evolving cyber threats. With our cutting-edge solutions, expert services, and trusted partnerships, we're here to help you protect what matters most.

Learn more about our solutions and how we're tackling today's toughest cyber challenges.

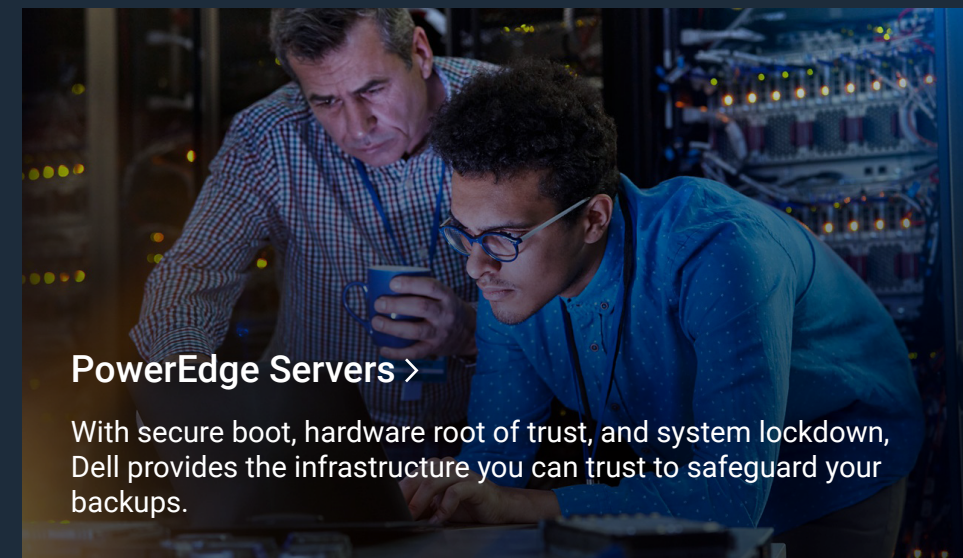
[Explore the Backup Infiltration Brief →](#)

[🏠 Back to Scenarios](#)



PowerProtect Portfolio >

Our immutable, air-gapped, and encrypted backup vaults, powered by AI-driven CyberSense analytics, ensure rapid detection and recovery so you can stay resilient.



PowerEdge Servers >

With secure boot, hardware root of trust, and system lockdown, Dell provides the infrastructure you can trust to safeguard your backups.



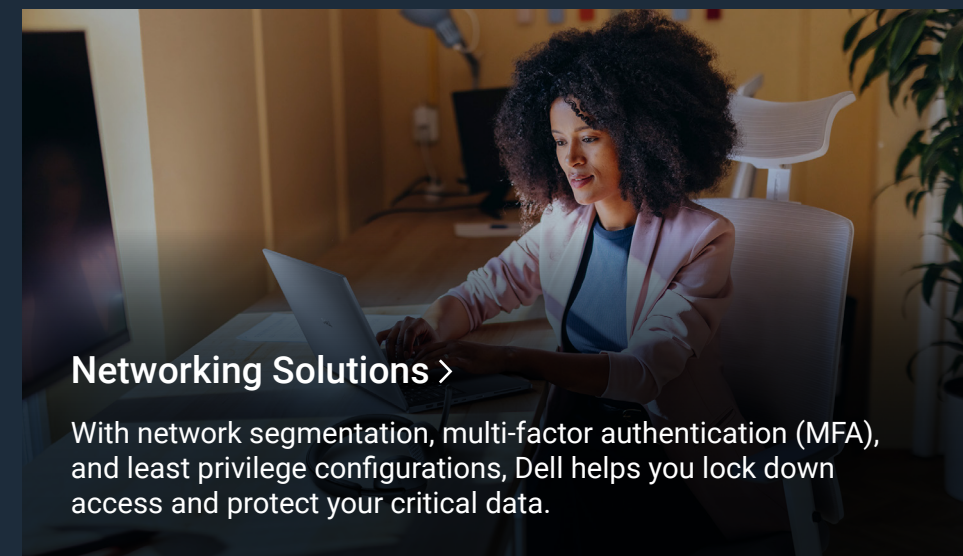
Trusted Workspace >

SafeBIOS and SafeData protections reduce risks, ensuring your backup systems remain untampered and ready when you need them.



Security and Resilience Services >

From secure deployment to proactive incident response, our experts and partners help you build resilience and recover faster.



Networking Solutions >

With network segmentation, multi-factor authentication (MFA), and least privilege configurations, Dell helps you lock down access and protect your critical data.

Attack Type: Distributed Denial of Service (DDoS)

It's Tuesday afternoon at a state government agency on a day of what is supposed to be a big snowstorm.

A flood of calls come into the IT team at the Department of Transportation from agents that can't get into any of their systems to:

- Renew driver's licenses
- Get road permits
- Pay taxes
- Check road conditions
- Engage emergency response systems, delaying road crews from clearing snowy/icy roads

all due to their systems timing out.

[Test Your Knowledge →](#)

Attack Type: Distributed Denial of Service (DDoS)



Where is the first place to look for what may be happening?

Check network devices for sudden, unexplained surges in inbound traffic

Check network devices for unusual traffic from a single or limited number of IP addresses

Check firewall or network visibility tools logs for excessive failed connections or traffic blocking events

All of the above

[See The Correct Answer →](#)



Attack Type: Distributed Denial of Service (DDoS)



Where is the first place to look for what may be happening?

- Check network devices for sudden, unexplained surges in inbound traffic
- Check network devices for unusual traffic from a single or limited number of IP addresses
- Check firewall or network visibility tools logs for excessive failed connections or traffic blocking events
- All of the above

To properly diagnose widespread system outages, you need to simultaneously review network device activity and firewall or visibility tool logs to quickly spot unusual patterns or blocking events. This allows for faster, more accurate incident response because you can distinguish between cyber incidents and infrastructure problems.

[Next Question →](#)



Attack Type: Distributed Denial of Service (DDoS)



You suspect this may be a DDoS attack. What is your first step?

- Redirect all network traffic through a DDoS mitigation service
- Activate Web Application Firewall (WAF) rules to filter out malicious patterns
- Check if the spike in traffic is due to legitimate sources
- Communicate internally and externally what is going on

[See The Correct Answer →](#)



Attack Type: Distributed Denial of Service (DDoS)



You suspect this may be a DDoS attack. What is your first step?

- Redirect all network traffic through a DDoS mitigation service
- Activate Web Application Firewall (WAF) rules to filter out malicious patterns
- Check if the spike in traffic is due to legitimate sources
- Communicate internally and externally what is going on

Before activating DDoS countermeasures, it is essential to verify the legitimacy of a traffic spike. This allows you to avoid accidentally blocking genuine users, prevent disruption to critical stakeholders and ensure that any further protective actions are appropriate and precisely targeted—minimizing negative impact on public operations and overall business continuity.

[Next Question →](#)



Attack Type: Distributed Denial of Service (DDoS)



What are some steps you can put in place to try to avoid a DDoS attack in the future?

Block the offending IP addresses

Perform regular penetration tests with DDoS simulations

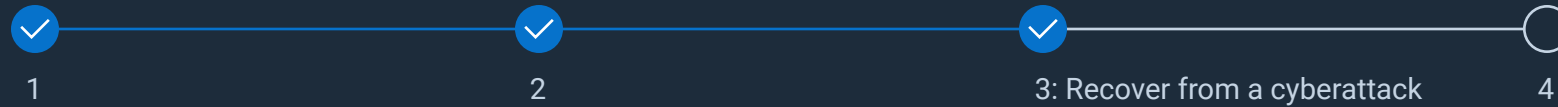
Move all applications to the cloud because cloud providers don't usually get DDoS attacks

Implement zero trust principles

[See The Correct Answer →](#)



Attack Type: Distributed Denial of Service (DDoS)



What are some steps you can put in place to try to avoid a DDoS attack in the future?

- Block the offending IP addresses
- Perform regular penetration tests with DDoS simulations
- Move all applications to the cloud because cloud providers don't usually get DDoS attacks
- Implement zero trust principles

Proactive penetration testing with DDoS simulations identifies and strengthens gaps in your defenses, while zero trust principles are focused on minimizing risk by enforcing least-privilege access at all times. This helps reduce the risk of disrupting essential systems, such as emergency response coordination or real-time traffic signal controls, that must remain functional even during an attack.

[Next Question →](#)



Attack Type: Distributed Denial of Service (DDoS)



As a part of your overall incident response and recovery plan (IRR), who should you notify?

Your legal team

Your cyber insurance vendor

CISA (Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC (Multi-State Information Sharing & Analysis Center)

All of the above

[See The Correct Answer →](#)



Attack Type: Distributed Denial of Service (DDoS)



As a part of your overall incident response and recovery plan (IRR), who should you notify?

- Your legal team
- Your cyber insurance vendor
- CISA (Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC (Multi-State Information Sharing & Analysis Center)
- All of the above

During a large-scale cyber incident, consider coordinating with legal, insurance, and government agencies regarding compliance, claims, and law enforcement. After you ensure all regulatory requirements are met, your organization can effectively contain, resolve, and recover from the incident.

[See Solutions →](#)



ATTACK TYPE: DISTRIBUTED DENIAL OF SERVICE (DDoS)

Recap

A DDoS attack seeks to disrupt the normal functioning of a network, service, or server by overwhelming it with a massive volume of traffic from multiple sources. These attacks are executed by exploiting botnets, which are networks of infected devices controlled remotely by attackers.

At Dell, we help organizations stay resilient against DDoS attacks by combining advanced detection and mitigation technologies with expert services and a zero trust approach, ensuring swift response, minimized disruptions, and strengthened defenses.

Learn more about advanced cyber resilience strategies and how Dell can help you safeguard your organization against DDoS.

[Explore the DDoS Brief →](#)

[🏠 Back to Scenarios](#)



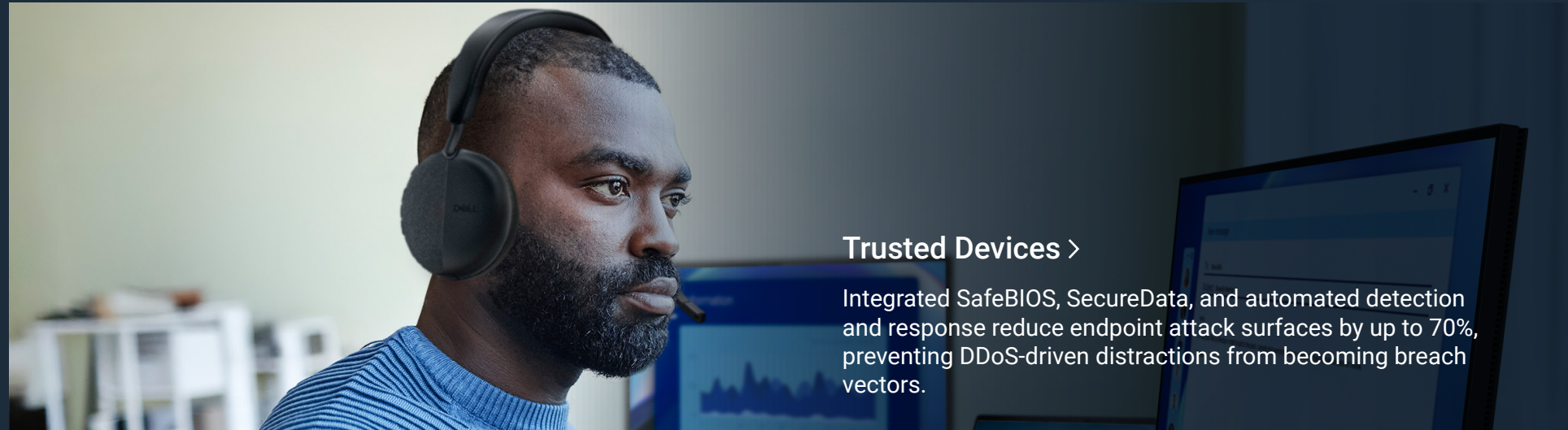
Networking Solutions >

Enable network segmentation, micro-segmentation, and least privilege enforcement to isolate critical assets, limit attack spread, and ensure rapid DDoS containment.



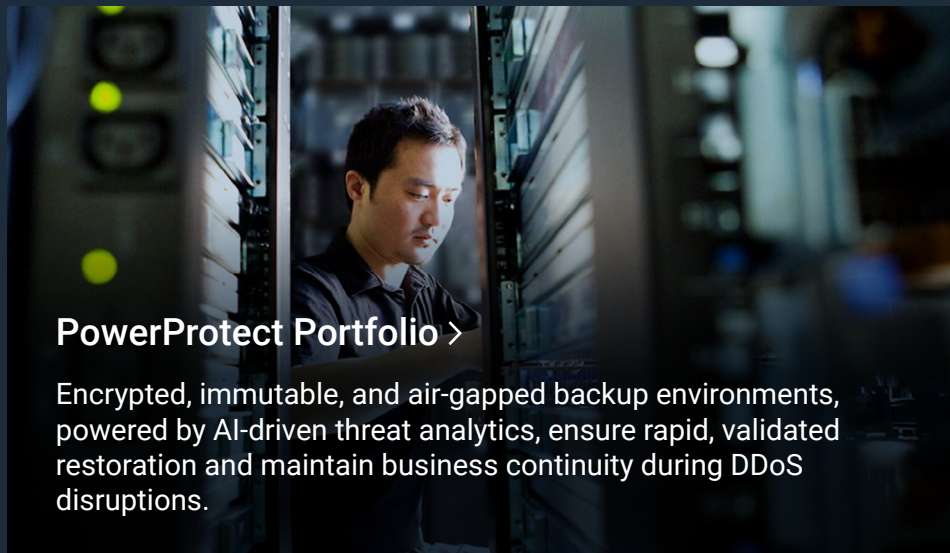
PowerEdge Servers >

With hardware root of trust, secure boot, system lockdown, and real-time tamper evidence, Dell delivers resilient, high-performance DDoS protection and accelerated recovery.



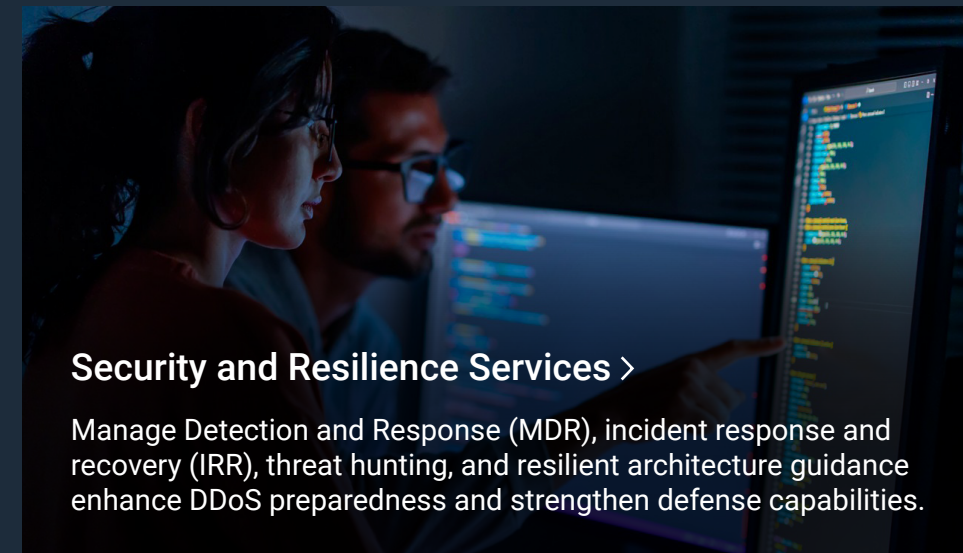
Trusted Devices >

Integrated SafeBIOS, SecureData, and automated detection and response reduce endpoint attack surfaces by up to 70%, preventing DDoS-driven distractions from becoming breach vectors.



PowerProtect Portfolio >

Encrypted, immutable, and air-gapped backup environments, powered by AI-driven threat analytics, ensure rapid, validated restoration and maintain business continuity during DDoS disruptions.



Security and Resilience Services >

Manage Detection and Response (MDR), incident response and recovery (IRR), threat hunting, and resilient architecture guidance enhance DDoS preparedness and strengthen defense capabilities.



Attack Type: Malicious Insider

It's 8:00AM on a Tuesday. The workday is just beginning for employees at a U.S. healthcare company.

A senior-level employee who works with highly-sensitive patient data logs in after a late night at the office.

She notices changes in a folder she was working in the night before. After running it by her team, she raises an inquiry with IT.

After investigating, they discover a junior IT employee with connections to a crime syndicate tricked a senior-level employee into inserting a USB Rubber Ducky into their device, which downgrades the Basic Input/Output System (BIOS) to a vulnerable version, compromising the system.

[Test Your Knowledge →](#)

Attack Type: Malicious Insider



The malicious insider initiated this attack using two methods tracked by the MITRE Adversarial Tactics, Techniques, and Common Knowledge, or MITRE ATT&CK, framework. What are they?

Trusted relationship + Replication through removable media

Social engineering + Replication through removable media

Social engineering + External remote services

Trusted relationship + Hardware additions

[See The Correct Answer →](#)



Attack Type: Malicious Insider



The malicious insider initiated this attack using two methods tracked by the MITRE Adversarial Tactics, Techniques, and Common Knowledge, or MITRE ATT&CK, framework. What are they?

- Trusted relationship + Replication through removable media
- Social engineering + Replication through removable media
- Social engineering + External remote services
- Trusted relationship + Hardware additions

By aligning with MITRE ATT&CK techniques for both human manipulation and replication through portable storage, the attacker leveraged social engineering to trick a senior employee into connecting a USB Rubber Ducky, delivering compromised data via removable media.

[Next Question →](#)



Attack Type: Malicious Insider



Why did the attacker need to use both methods?

Enter the network as a global admin to downgrade the Basic Input/Output System (BIOS)

Phish the admin to allow them to downgrade the BIOS

Change the device's domain name system (DNS) provider to obtain credentials needed for one-time network access

Install malware on a device to obtain credentials needed for continuous network access

[See The Correct Answer →](#)



Attack Type: Malicious Insider



Why did the attacker need to use both methods?

- Enter the network as a global admin to downgrade the Basic Input/Output System (BIOS)
- Phish the admin to allow them to downgrade the BIOS
- Change the device's domain name system (DNS) provider to obtain credentials needed for one-time network access
- Install malware on a device to obtain credentials needed for continuous network access

The attacker needed to use both methods—the malware installation via the USB Rubber Ducky to compromise the device and the credentials to enable ongoing continuous network access—to establish persistent, unauthorized control over the target environment.

[Next Question →](#)



Attack Type: Malicious Insider



What is one way of detecting irregular network activity?

Application control

Extended Detection and Response (XDR)

Next-gen antivirus (NGAV)

Endpoint geofencing

[See The Correct Answer →](#)



Attack Type: Malicious Insider



What is one way of detecting irregular network activity?

- Application control
- Extended Detection and Response (XDR)
- Next-gen antivirus (NGAV)
- Endpoint geofencing

When it comes to providing broad, correlated visibility for rapid detection of threats, XDR is best for detecting suspicious network activity because it continuously monitors and analyzes activity across endpoints, networks, and cloud environments.

[Next Question →](#)



Attack Type: Malicious Insider



What built-in PC security could detect suspicious activity early in the kill chain?

Security Information and Event Management (SIEM)

Extended Detection and Response (XDR)

Indicators of Attach (IOA)

Role-Based Access Control (RBAC)

[See The Correct Answer →](#)



Attack Type: Malicious Insider



What built-in PC security could detect suspicious activity early in the kill chain?

- Security Information and Event Management (SIEM)
- Extended Detection and Response (XDR)
- Indicators of Attach (IOA)
- Role-Based Access Control (RBAC)

IOA focuses on detecting attacker behaviors and suspicious activity patterns as they happen, allowing security teams to identify threats earlier than signature-based methods and intervene before significant damage occurs.

[Next Question →](#)



Attack Type: Malicious Insider



After pinpointing the initial access method, what measure could you take to recover from and prevent similar future breaches?

Update BIOS to the latest version

Disable BIOS downgrade option

Disable USB ports

Implement granular control to enable safe USB device use and prevent the spread of malware

All of the above

[See The Correct Answer →](#)



Attack Type: Malicious Insider



After pinpointing the initial access method, what measure could you take to recover from and prevent similar future breaches?

- ✓ Update BIOS to the latest version
- ✓ Disable BIOS downgrade option
- ✓ Disable USB ports
- ✓ Implement granular control to enable safe USB device use and prevent the spread of malware
- ✓ All of the above

By addressing distinct attack vectors to ensure hardware is secure and downgrades are blocked, USB-based threats can be contained and malware spread is stopped at multiple points to help create a comprehensive, layered defense that recovers impacted systems and protects against future breaches.

[See Solutions →](#)



ATTACK TYPE: MALICIOUS INSIDER

Recap

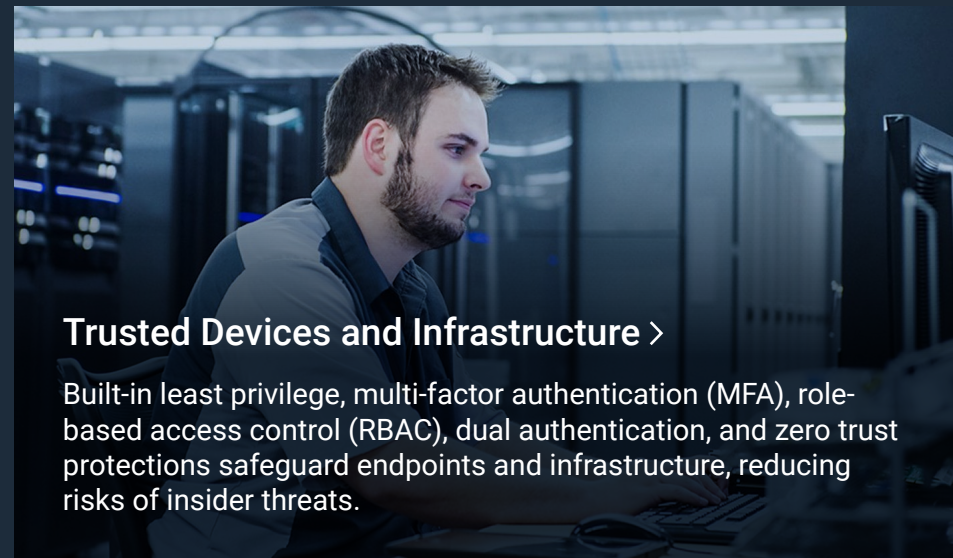
A Malicious Insider attack occurs when an individual within an organization misuses their access to compromise data, disrupt operations, or extract sensitive information for personal, financial, or competitive objectives. This individual could be an employee, contractor, partner, or anyone with legitimate access to the company's systems and networks.

Dell defends against malicious insider cyberattacks through a combination of advanced technologies and strict security protocols.

Learn more about advanced cyber resilience strategies and how Dell can help you safeguard your organization against Malicious Insider attacks.

[Explore the Malicious Insider Brief →](#)

[🏠 Back to Scenarios](#)



Trusted Devices and Infrastructure >

Built-in least privilege, multi-factor authentication (MFA), role-based access control (RBAC), dual authentication, and zero trust protections safeguard endpoints and infrastructure, reducing risks of insider threats.



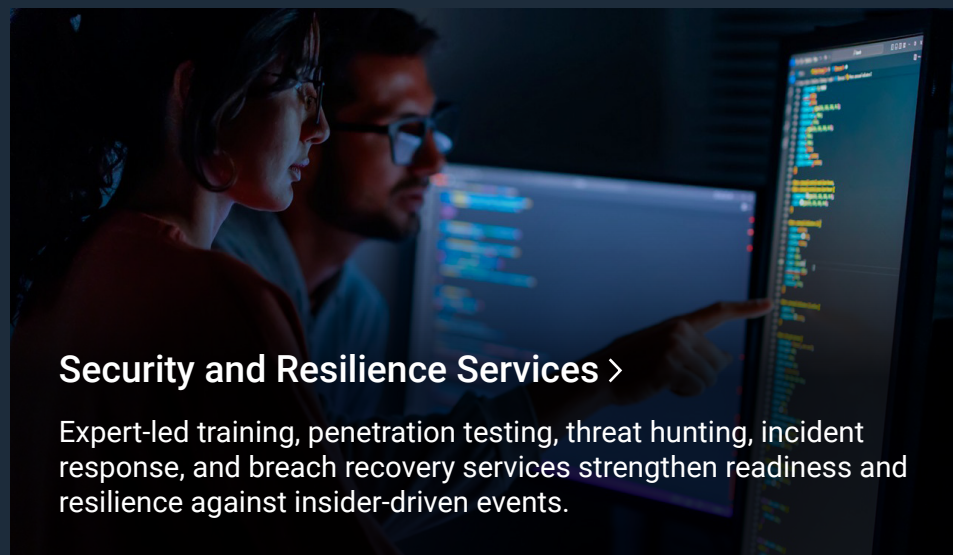
PowerEdge Servers >

Hardware root of trust, secure boot, dynamic USB port management, and system lockdown protect against tampering and halt physical or firmware-based insider attacks.



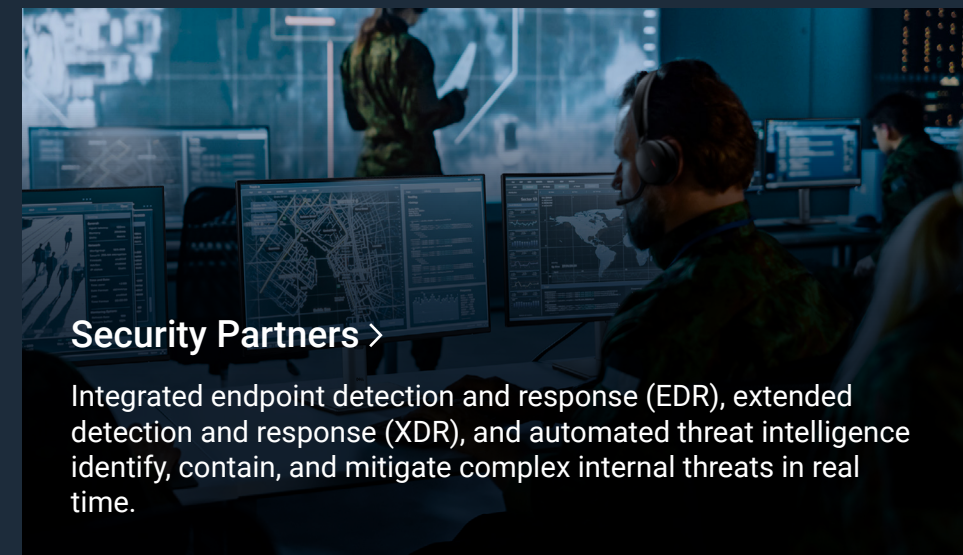
PowerProtect Portfolio >

Unmodifiable, isolated backups ensure data integrity, quick restoration, and early detection of data manipulation attempts, enabling recovery from insider incidents.



Security and Resilience Services >

Expert-led training, penetration testing, threat hunting, incident response, and breach recovery services strengthen readiness and resilience against insider-driven events.



Security Partners >

Integrated endpoint detection and response (EDR), extended detection and response (XDR), and automated threat intelligence identify, contain, and mitigate complex internal threats in real time.

A woman with short dark hair and glasses is sitting at a wooden table in a coffee shop, working on a laptop. She is wearing a light-colored blazer over a white top. The background is softly blurred, showing other people and warm lighting.

Attack Type: Man-in-the-Middle (MITM)

An unsuspecting customer connects to a free, unsecured Wi-Fi at a coffee shop to finalize last-minute updates to a shared team document.

Moments later, their company's IT receives notifications of unusual login attempts from the employee's account, as well as unauthorized data access from multiple locations worldwide.

After investigating, they confirm the attacker has intercepted and manipulated the wireless connection, accessing sensitive information.

[Test Your Knowledge →](#)

Attack Type: Man-in-the-Middle (MITM)



Where is the first place the IT team should investigate after detecting unusual login attempts?

Firewall, intrusion detection system (IDS), intrusion prevention system (IPS) logs and extended detection response (XDR)

The affected employee's laptop

Network traffic on the coffee shop's unsecured Wi-Fi

Authentication logs from the company's systems

[See The Correct Answer →](#)



Attack Type: Man-in-the-Middle (MITM)



Where is the first place the IT team should investigate after detecting unusual login attempts?

- Firewall, intrusion detection system (IDS), intrusion prevention system (IPS) logs and extended detection response (XDR)
- The affected employee's laptop
- Network traffic on the coffee shop's unsecured Wi-Fi
- Authentication logs from the company's systems

By analyzing these firewall and IDS/IPS and authentication logs, IT teams can trace unauthorized access attempts, assess compromised accounts, and gain a better understanding of the incident's scope.

[Next Question →](#)



Attack Type: Man-in-the-Middle (MITM)



What immediate action should be taken by the IT team after confirming the MITM attack?

Disconnect the compromised employee's device from the network immediately and isolate it for analysis

Update firewall rules and network configurations to stop further unauthorized access

Reset passwords for all employee accounts

Disable affected systems to prevent data exfiltration

[See The Correct Answer →](#)



Attack Type: Man-in-the-Middle (MITM)



What immediate action should be taken by the IT team after confirming the MITM attack?

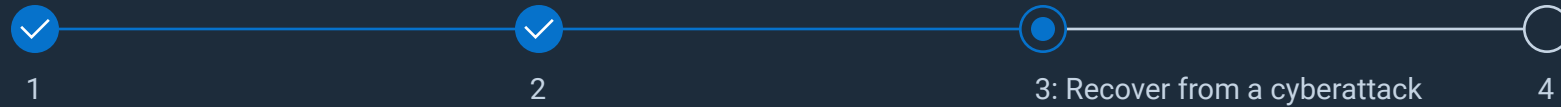
- Disconnect the compromised employee's device from the network immediately and isolate it for analysis
- Update firewall rules and network configurations to stop further unauthorized access
- Reset passwords for all employee accounts
- Disable affected systems to prevent data exfiltration

Immediately disconnecting and isolating the compromised device stops attacker access and preserves forensic evidence, while updating firewall and network rules blocks further malicious connections and protects the broader network from ongoing compromise.

[Next Question →](#)



Attack Type: Man-in-the-Middle (MITM)



What preventative measures could have reduced the vulnerability to the MITM attack?

Enforce the use of virtual private network (VPN) for all employees

Implement zero trust security principles like multi-factor authentication (MFA)

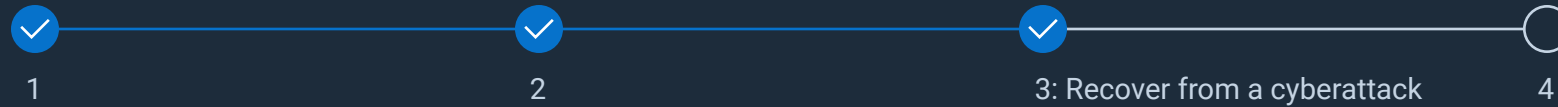
Avoid public Wi-Fi

Encrypt sensitive files shared via email

[See The Correct Answer →](#)



Attack Type: Man-in-the-Middle (MITM)



What preventative measures could have reduced the vulnerability to the MITM attack?

- ✓ Enforce the use of virtual private network (VPN) for all employees
- ✓ Implement zero trust security principles like multi-factor authentication (MFA)
- ✗ Avoid public Wi-Fi
- ✗ Encrypt sensitive files shared via email

Enforcing VPN use over unsecured networks encrypts employee internet traffic to prevent interception, while implementing zero trust security and MFA ensures every access request is continuously verified.

[Next Question →](#)



Attack Type: Man-in-the-Middle (MITM)



After addressing the breach, what long-term strategies should your organization implement?

Regularly audit and patch systems

Increase network segmentation to isolate sensitive data and systems

Deploy endpoint detection and response (EDR) and managed detection and response (MDR) solutions

Implement robust and regular training for employees

All of the above

[See The Correct Answer →](#)



Attack Type: Man-in-the-Middle (MITM)



After addressing the breach, what long-term strategies should your organization implement?

- ✓ Regularly audit and patch systems
- ✓ Increase network segmentation to isolate sensitive data and systems
- ✓ Deploy endpoint detection and response (EDR) and managed detection and response (MDR) solutions
- ✓ Implement robust and regular training for employees
- ✓ All of the above

To protect against different threats, these long-term strategies combine to create a comprehensive, resilient security posture that blocks attackers from exploiting gaps and ensures rapid, effective response to breaches.

[See Solutions →](#)



ATTACK TYPE: MAN-IN-THE-MIDDLE (MITM)

Recap

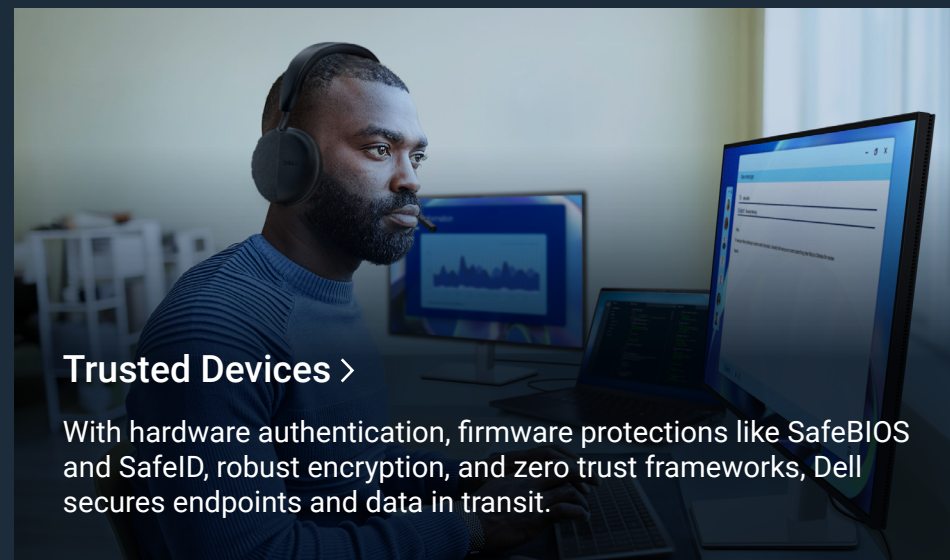
A MITM attack happens when a cybercriminal secretly intercepts communications between two parties, such as between an employee and a corporate server or a customer and a business website. The attacker's goal may vary, but the result is the same: a breach of trust and security.

At Dell, we deliver innovative, scalable security solutions, empowering organizations to neutralize MITM threats, safeguard assets, and maintain business integrity with the tools and expertise needed to detect, respond to, and recover with confidence.

Learn more about advanced cyber resilience strategies and see how Dell can help you safeguard your organization against MITM attacks.

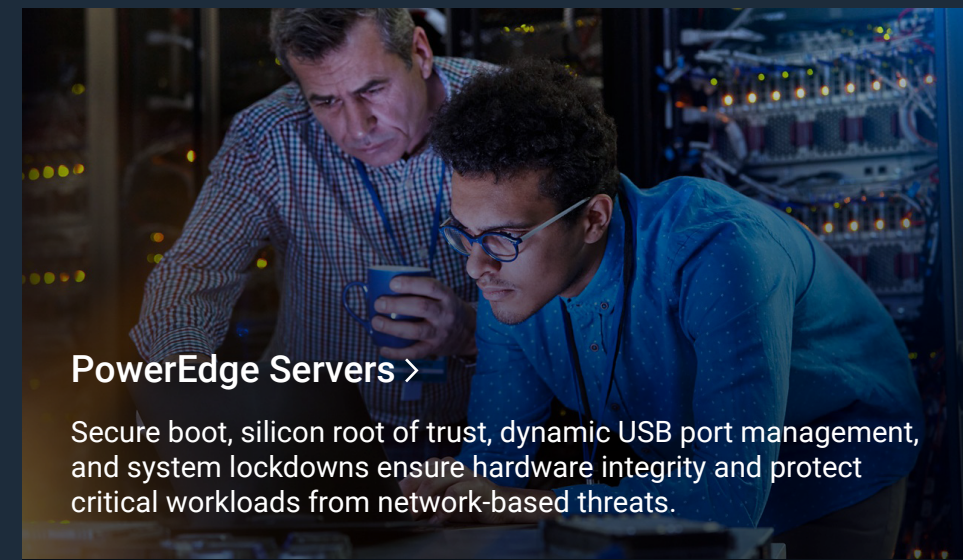
[Read MITM Attacks Brief →](#)

[🏠 Back to Scenarios](#)



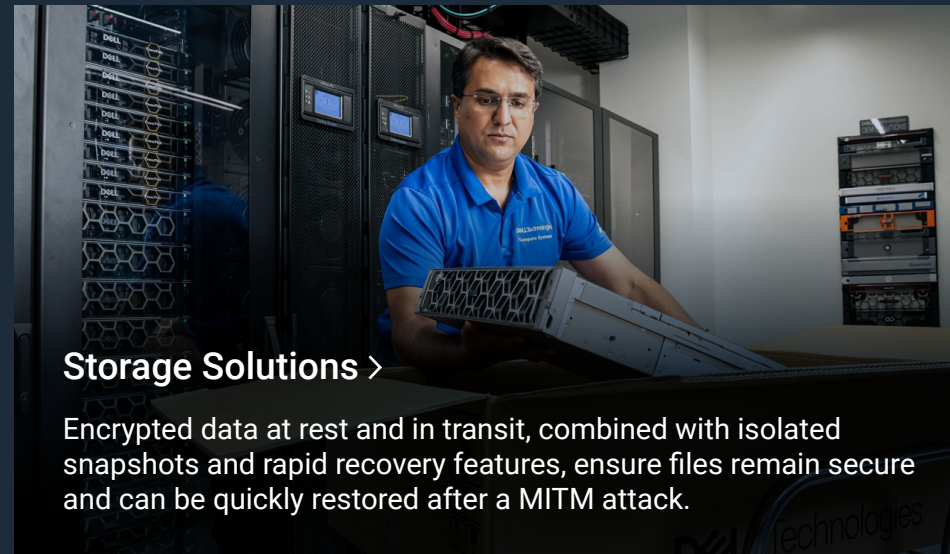
Trusted Devices >

With hardware authentication, firmware protections like SafeBIOS and SafeID, robust encryption, and zero trust frameworks, Dell secures endpoints and data in transit.



PowerEdge Servers >

Secure boot, silicon root of trust, dynamic USB port management, and system lockdowns ensure hardware integrity and protect critical workloads from network-based threats.



Storage Solutions >

Encrypted data at rest and in transit, combined with isolated snapshots and rapid recovery features, ensure files remain secure and can be quickly restored after a MITM attack.



PowerProtect Portfolio >

Unmodifiable, isolated backups and AI-driven CyberSense analytics enable swift recovery and trusted data restoration in the event of a MITM attack.



Security and Resilience Services >

From vulnerability assessments and user training to penetration testing and incident response, Dell's experts and partners provide comprehensive support to strengthen your defenses.



Attack Type: Prompt / SQL Injection

You work in customer service for an airline that predominantly conducts service through a chatbot.

You start to notice that you and your colleagues are getting an influx of calls from customers stating that they can't get into their frequent flyer accounts, and when they do, they see all their frequent flyer miles are gone.

[Test Your Knowledge →](#)

Attack Type: Prompt / SQL Injection



Upon investigation you see some errors in the logs; *Syntax error in Structured Query Language (SQL) statement or Invalid column name 'admin'*. What type of a cyber incident is this?

Stolen credentials

Prompt or SQL injection

Man-in-the-Middle attack

Phishing

[See The Correct Answer →](#)



Attack Type: Prompt / SQL Injection



Upon investigation you see some errors in the logs; *Syntax error in Structured Query Language (SQL) statement* or *Invalid column name 'admin'*. What type of a cyber incident is this?

- Stolen credentials
- Prompt or SQL injection
- Man-in-the-Middle attack
- Phishing

'Prompt or SQL injection' is correct because log errors like "Syntax error in SQL statement" or "Invalid column name 'admin'" reveal that attackers exploited the chatbot's input fields with malicious SQL code to access or alter customer account data, which are clear technical indicators of an SQL injection attack matching the suspicious activity described.

[Next Question →](#)



Attack Type: Prompt / SQL Injection



You realize you have been hit with a Prompt / SQL Injection through your customer service chatbot. What should you do?

Take the bot offline

Investigate database logs for unauthorized access and stolen, modified, or deleted data

Comply with all data breach disclosure laws

All of the above

[See The Correct Answer →](#)



Attack Type: Prompt / SQL Injection



You realize you have been hit with a Prompt / SQL Injection through your customer service chatbot. What should you do?

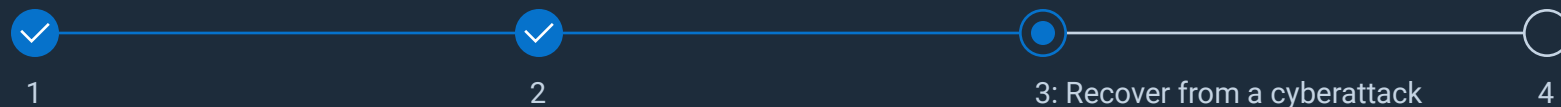
- Take the bot offline
- Investigate database logs for unauthorized access and stolen, modified, or deleted data
- Comply with all data breach disclosure laws
- All of the above

Responding to a Prompt / SQL Injection attack requires taking the chatbot offline, investigating database logs for unauthorized access, and ensuring compliance with disclosure laws. These steps are essential to stop exploitation, assess damage, and meet regulatory and ethical obligations.

[Next Question →](#)



Attack Type: Prompt / SQL Injection



What capabilities should you put in place to help stop Prompt / SQL Injections?

Educate the development teams to use prepared statements and parameterized queries as a coding practice

Manage detection and response (MDR) tools

Implement least privilege access, such as multi-factor authentication (MFA), role-based access control (RBAC), web application firewall (WAF), etc.

Segment backend databases / knowledge bases.

[See The Correct Answer →](#)



Attack Type: Prompt / SQL Injection



What capabilities should you put in place to help stop Prompt / SQL Injections?

- Educate the development teams to use prepared statements and parameterized queries as a coding practice
- Manage detection and response (MDR) tools
- Implement least privilege access, such as multi-factor authentication (MFA), role-based access control (RBAC), web application firewall (WAF), etc.
- Segment backend databases / knowledge bases.

Training development teams to use prepared statements and parameterized queries blocks SQL injection attacks at the source, while enforcing least privilege access controls, such as MFA, RBAC, and WAF, limits the impact of any attempted injection by preventing attackers from escalating privileges or moving laterally.

[Next Question →](#)



Attack Type: Prompt / SQL Injection



What steps would you take to get the airline customers data back?

Track down the stolen data

Have customers rebuild their profiles

Buy it back from the cyber attackers

Restore from most recent uncompromised backup to restore frequent flyer miles and notify the customers that they should change their passwords and check their credit cards

[See The Correct Answer →](#)



Attack Type: Prompt / SQL Injection



What steps would you take to get the airline customers data back?

- Track down the stolen data
- Have customers rebuild their profiles
- Buy it back from the cyber attackers
- Restore from most recent uncompromised backup to restore frequent flyer miles and notify the customers that they should change their passwords and check their credit cards

Recovering lost account data from the latest uncompromised backup helps maintain data integrity and reduce downtime. Promptly notifying customers to reset passwords and monitor credit card activity further supports regulatory compliance following a destructive injection attack.

[See Solutions →](#)



ATTACK TYPE: PROMPT / SQL INJECTION

Recap

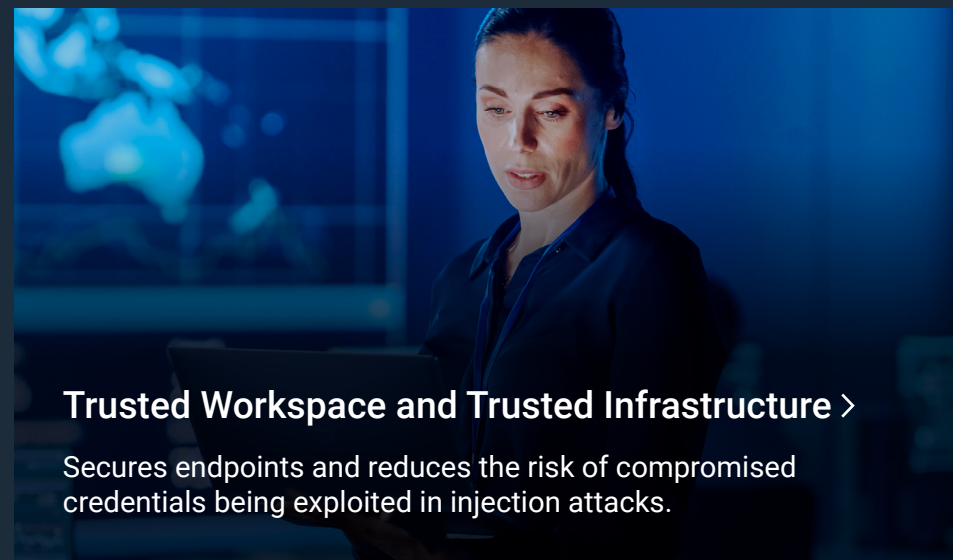
Prompt and SQL injection attacks have repeatedly proven to be among the most damaging and pervasive methods of cyberattack used by cybercriminals. These attacks exploit vulnerabilities in user-query or database systems, allowing malicious actors to manipulate servers, steal data, or disrupt workflows.

Protecting your organization from evolving Prompt / SQL Injection threats and attacks are part of Dell's ongoing commitment to cybersecurity, and we provide the tools and expertise needed for detection, response, and recovery.

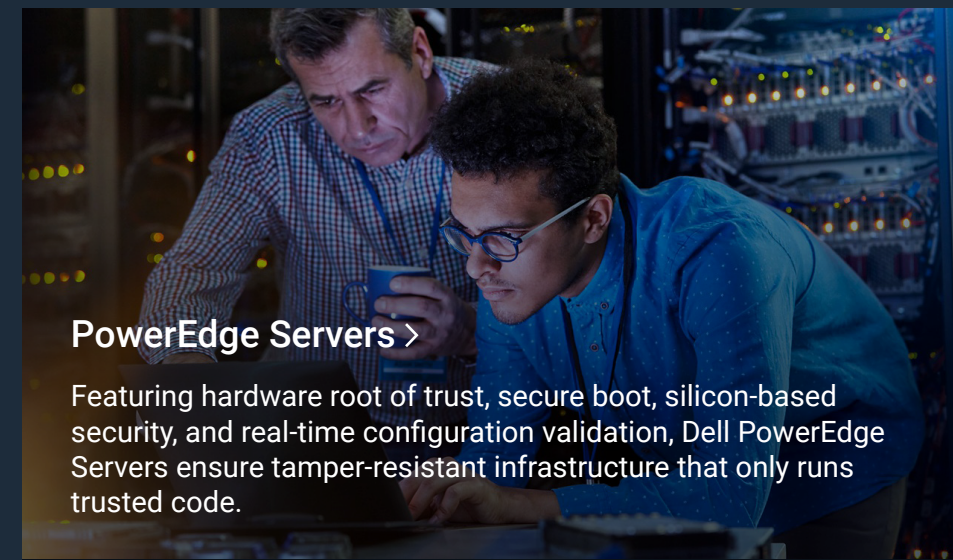
Discover advanced cyber resilience strategies and see how Dell can empower your organization to defend against Prompt and SQL injection attacks.

[Explore Prompt / SQL Injection Brief →](#)

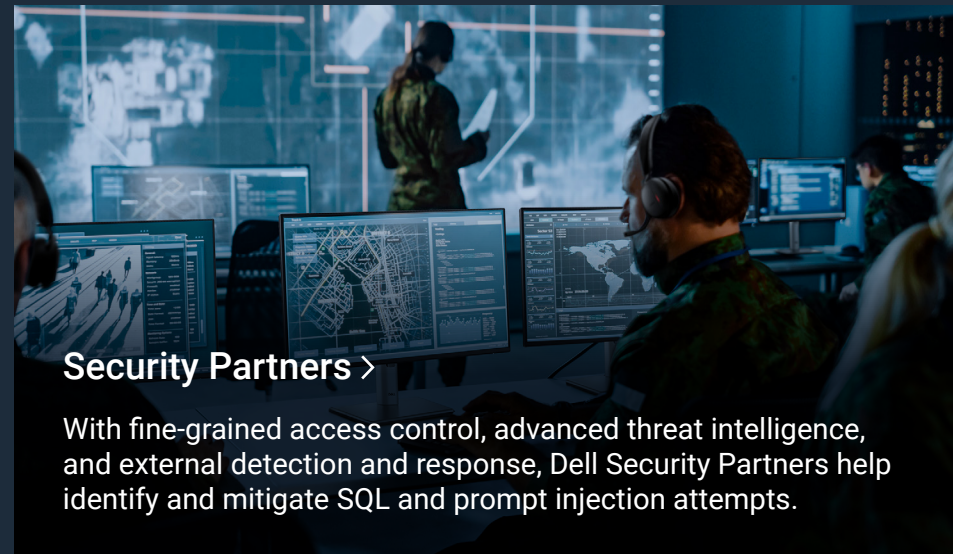
[🏠 Back to Scenarios](#)



Trusted Workspace and Trusted Infrastructure >
Secures endpoints and reduces the risk of compromised credentials being exploited in injection attacks.



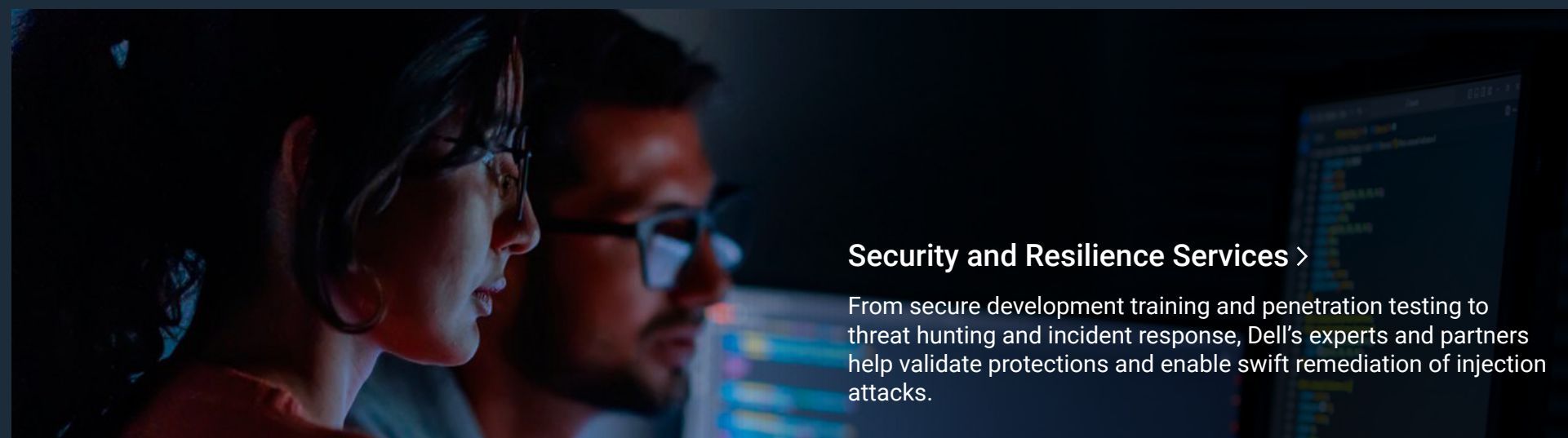
PowerEdge Servers >
Featuring hardware root of trust, secure boot, silicon-based security, and real-time configuration validation, Dell PowerEdge Servers ensure tamper-resistant infrastructure that only runs trusted code.



Security Partners >
With fine-grained access control, advanced threat intelligence, and external detection and response, Dell Security Partners help identify and mitigate SQL and prompt injection attempts.



PowerProtect Portfolio >
Dell's unmodifiable, air-gapped backups, and advanced cyber recovery analytics provide trusted restore points, enabling rapid recovery from data corruption or exfiltration.



Security and Resilience Services >
From secure development training and penetration testing to threat hunting and incident response, Dell's experts and partners help validate protections and enable swift remediation of injection attacks.



Attack Type: Ransomware

You are an IT professional at a regional hospital known for its connected medical systems—including electronic health records (EHR), smart infusion pumps, and radiology imaging all tied into a centralized network.

Last night, several systems began crashing simultaneously. By morning, clinical staff report being locked out of patient records.

The following ransom note appears on several terminals:

“Your files are encrypted. Pay 20 Bitcoin in 72 hours or patient data will be released.”

[Test Your Knowledge →](#)

Attack Type: Ransomware



The help desk receives over 100 reports of file encryption and application errors. Security logs show unusual file renaming activity from an internal domain account. What is your first step?

Pay the ransom immediately to restore critical services

Notify law enforcement and legal counsel

Begin reimaging all affected endpoints

Disconnect infected systems from the network

[See The Correct Answer →](#)



Attack Type: Ransomware



The help desk receives over 100 reports of file encryption and application errors. Security logs show unusual file renaming activity from an internal domain account. What is your first step?

- Pay the ransom immediately to restore critical services
- Notify law enforcement and legal counsel
- Begin reimaging all affected endpoints
- Disconnect infected systems from the network

Immediately disconnecting and isolating infected hospital systems stops ransomware from spreading, protects critical medical devices and sensitive patient data, preserves evidence for investigation, and buys vital time for a coordinated response and recovery.

[Next Question →](#)



Attack Type: Ransomware



The Incident Response team discovers that the attack likely started from a compromised account that was used to access a server with no multi-factor authentication (MFA). Which of the following contributed most directly to the attack?

Outdated antivirus definitions

An exposed electronic health record (EHR) database

Lack of MFA on remote access

Weak email filtering

[See The Correct Answer →](#)



Attack Type: Ransomware



The Incident Response team discovers that the attack likely started from a compromised account that was used to access a server with no multi-factor authentication (MFA). Which of the following contributed most directly to the attack?

- Outdated antivirus definitions
- An exposed electronic health record (EHR) database
- Lack of MFA on remote access
- Weak email filtering

Lack of MFA on remote access enabled the server breach by allowing attackers to log in with stolen or guessed credentials without an extra verification step. With MFA, even compromised accounts would require a second factor, dramatically reducing the risk of unauthorized access.

[Next Question →](#)



Attack Type: Ransomware



Medical staff now rely on paper-based workflows. Patients scheduled for surgery today cannot be verified in the system. What is the best short-term action to support hospital operations?

Reboot the core database server to attempt reinitialization

Enable all old backups, even if they are six months old

Activate hospital's manual downtime procedures and escalate to the emergency response team

Let staff decide how to proceed on a case-by-case basis

[See The Correct Answer →](#)



Attack Type: Ransomware



Medical staff now rely on paper-based workflows. Patients scheduled for surgery today cannot be verified in the system. What is the best short-term action to support hospital operations?

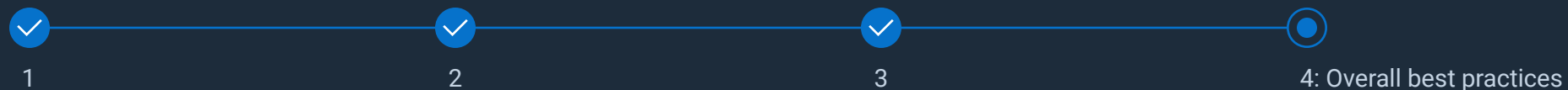
- Reboot the core database server to attempt reinitialization
- Enable all old backups, even if they are six months old
- Activate hospital's manual downtime procedures and escalate to the emergency response team
- Let staff decide how to proceed on a case-by-case basis

Activating manual downtime procedures and escalating to the emergency response team ensures the immediate continuity of critical clinical workflows, safeguards patient safety, and establishes a standardized process for verifying and documenting care. This approach minimizes errors, efficiently manages risks and resources, and supports specialists in safely restoring digital systems.

Next Question →



Attack Type: Ransomware



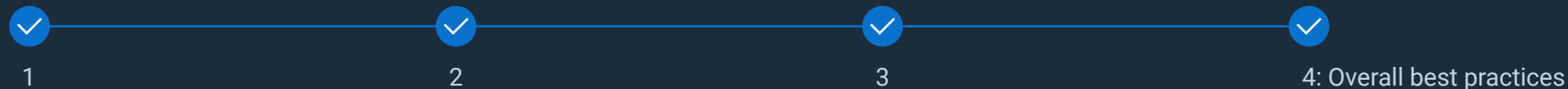
The local media has picked up the story. Leadership wants to know if they should issue a public statement, and legal is asking about Health Insurance Portability and Accountability Act (HIPAA) obligations. Which is the most appropriate next step?

- Deny the incident publicly until more information is available
- Issue a press release blaming the third-party IT vendor
- Notify regulators and begin internal breach notification procedures
- Immediately pay the ransom and avoid public attention

[See The Correct Answer →](#)



Attack Type: Ransomware



The local media has picked up the story. Leadership wants to know if they should issue a public statement, and legal is asking about Health Insurance Portability and Accountability Act (HIPAA) obligations. Which is the most appropriate next step?

- Deny the incident publicly until more information is available
- Issue a press release blaming the third-party IT vendor
- Notify regulators and begin internal breach notification procedures
- Immediately pay the ransom and avoid public attention

Promptly reporting breaches of protected health information to authorities and affected individuals, as required by HIPAA and state laws, ensures regulatory compliance, legal protection, and best-practice transparency to prevent legal and reputational damage, fulfilling mandatory disclosure obligations, and establishing proper communication with patients, staff, and stakeholders.

[See Solutions →](#)



ATTACK TYPE: RANSOMWARE

Recap

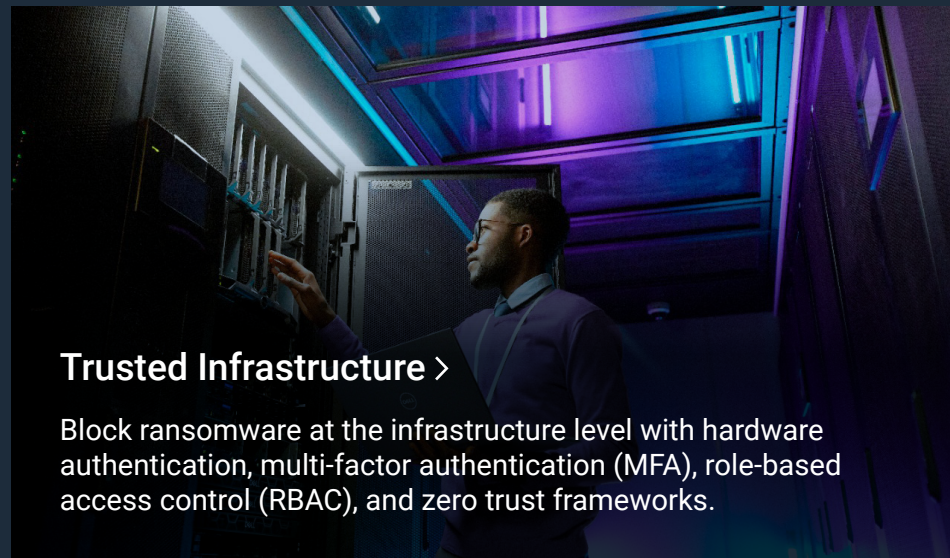
Ransomware is a type of malware that blocks access to a computer system or data until a ransom is paid. It's one of the most disruptive types of cyberattacks. Fifty percent of organizations globally have been hit by ransomware at least once in the past year and the average downtime following a ransomware attack is three weeks, leading to significant operational disruptions.

At Dell, we prioritize safeguarding your organization with zero trust frameworks, endpoint protection, and network segmentation to block ransomware entry and limit its spread. With expert-led incident response planning, we help you stay resilient and recover quickly from attacks.

Learn more about advanced cyber resilience strategies and see how Dell can help you safeguard your organization against Ransomware Attacks.

[Explore Ransomware Attacks Brief →](#)

[🏠 Back to Scenarios](#)



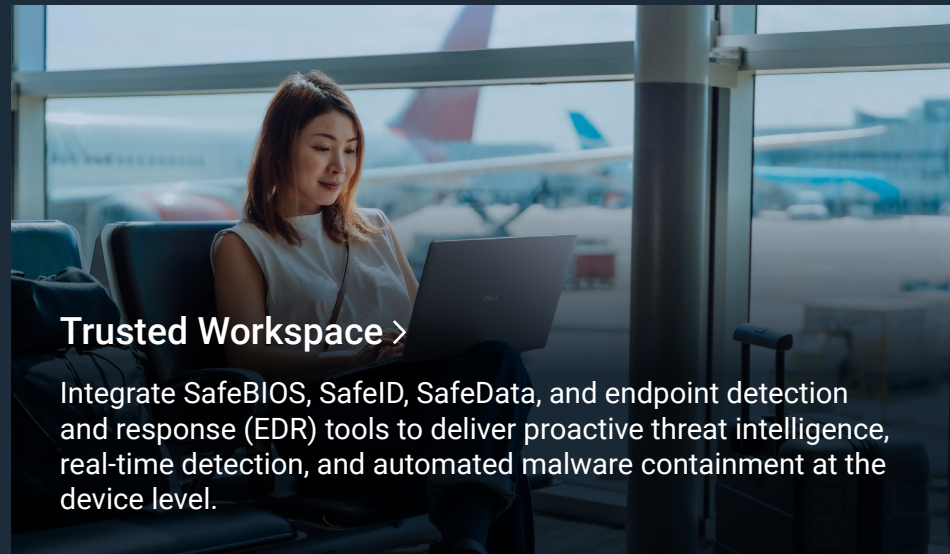
Trusted Infrastructure >

Block ransomware at the infrastructure level with hardware authentication, multi-factor authentication (MFA), role-based access control (RBAC), and zero trust frameworks.



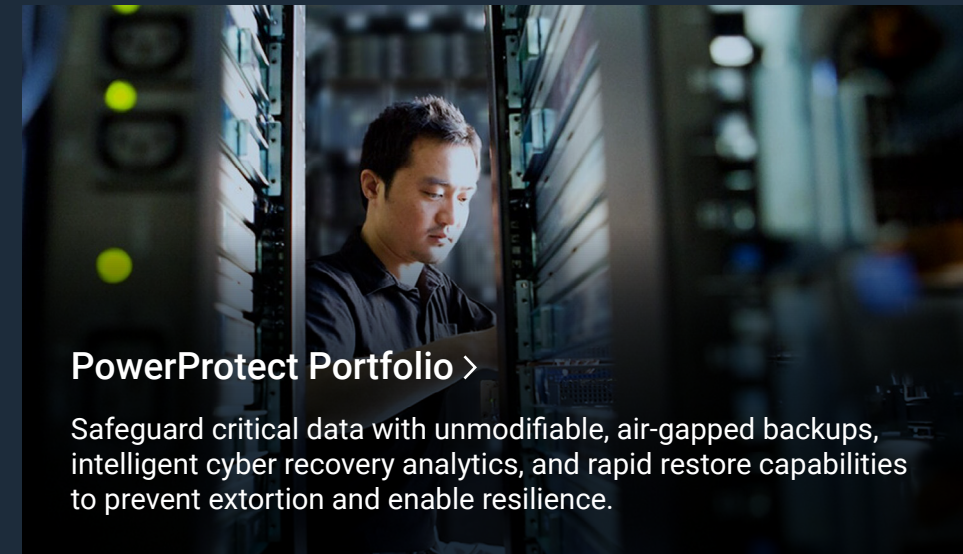
Networking and PowerEdge Servers >

Restrict ransomware movement. Featuring network segmentation, secure boot, silicon root of trust, dynamic USB port management, and system lockdown.



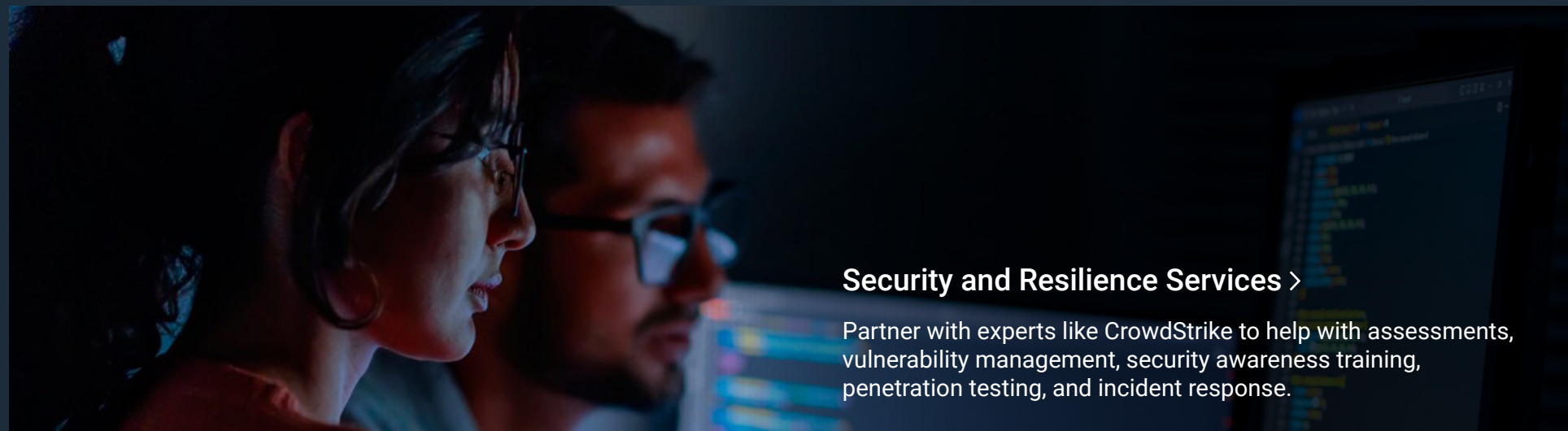
Trusted Workspace >

Integrate SafeBIOS, SafeID, SafeData, and endpoint detection and response (EDR) tools to deliver proactive threat intelligence, real-time detection, and automated malware containment at the device level.



PowerProtect Portfolio >

Safeguard critical data with unmodifiable, air-gapped backups, intelligent cyber recovery analytics, and rapid restore capabilities to prevent extortion and enable resilience.



Security and Resilience Services >

Partner with experts like CrowdStrike to help with assessments, vulnerability management, security awareness training, penetration testing, and incident response.

Attack Type: Supply Chain Hardware

Your company rolls out 500 new laptops across its global offices. To speed things up, you outsourced imaging and hardware preparation to a third-party IT logistics vendor. They ship pre-configured machines directly to employees.

Within a few days, you receive several calls from the field stating:

- Multi-factor authentication (MFA) requests are being bypassed and are not working properly.
- The security team sees a number of unauthorized admin logins at odd hours.
- They also see virtual private network (VPN) traffic from users who are supposedly offline.

[Test Your Knowledge →](#)



Attack Type: Supply Chain Hardware



An employee reports receiving multi-factor authentication (MFA) push notifications when they were not attempting to log in. Your organization's security dashboard shows that the login originated from a device with a company-issued asset tag. What is the most logical first step for the security operations center (SOC) team?

Disable the user's account and wipe their laptop remotely

Compare the login IP and device fingerprint to other known compromised users

Escalate to HR assuming the user is at fault

Issue a company-wide alert to change passwords immediately

[See The Correct Answer →](#)



Attack Type: Supply Chain Hardware



An employee reports receiving multi-factor authentication (MFA) push notifications when they were not attempting to log in. Your organization's security dashboard shows that the login originated from a device with a company-issued asset tag. What is the most logical first step for the security operations center (SOC) team?

- Disable the user's account and wipe their laptop remotely
- Compare the login IP and device fingerprint to other known compromised users
- Escalate to HR assuming the user is at fault
- Issue a company-wide alert to change passwords immediately

When your SOC team determines if suspicious activity is part of a broader attack or an isolated attack to enable rapid pattern recognition, targeted incident response and containment of further risk is the logical first step when identifying a Supply Chain Hardware attack.

[Next Question →](#)



Attack Type: Supply Chain Hardware



Your incident response team finds that multiple affected laptops are running SSD firmware versions that don't match official vendor release notes. Endpoint detection response (EDR) shows no malicious processes. What does this most likely indicate?

- A configuration error from the IT vendor
- A new type of ransomware that deletes itself
- A firmware-level supply chain compromise
- Normal behavior during imaging

[See The Correct Answer →](#)



Attack Type: Supply Chain Hardware



Your incident response team finds that multiple affected laptops are running SSD firmware versions that don't match official vendor release notes. Endpoint detection response (EDR) shows no malicious processes. What does this most likely indicate?

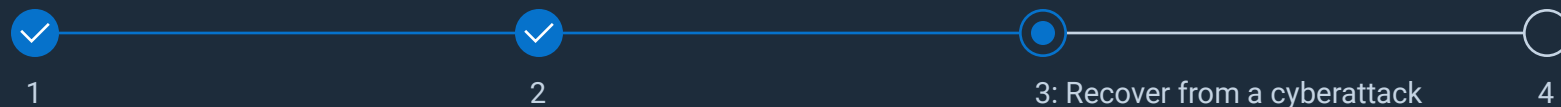
- A configuration error from the IT vendor
- A new type of ransomware that deletes itself
- A firmware-level supply chain compromise
- Normal behavior during imaging

Unauthorized SSD firmware on multiple laptops, undetected by EDR and mismatched with official releases, indicates deliberate hardware or firmware tampering—a hallmark of a firmware-level supply chain compromise.

[Next Question →](#)



Attack Type: Supply Chain Hardware



You've isolated 100 suspected devices with rogue SSD firmware. You need to decide how to move forward without tipping off the attacker, who may have remote access. What's the best next move?

Power down all devices and ship them to forensics

Conduct memory dumps live and investigate while systems are running

Notify the third-party vendor that they've been breached

Wipe all devices and reissue new laptops to all users globally

[See The Correct Answer →](#)



Attack Type: Supply Chain Hardware



You've isolated 100 suspected devices with rogue SSD firmware. You need to decide how to move forward without tipping off the attacker, who may have remote access. What's the best next move?

- Power down all devices and ship them to forensics
- Conduct memory dumps live and investigate while systems are running
- Notify the third-party vendor that they've been breached
- Wipe all devices and reissue new laptops to all users globally

Live memory dumps are crucial for preserving volatile evidence like active malware and rootkits, enabling targeted incident response by uncovering hidden threats and access points before they are lost or attackers are alerted.

[Next Question →](#)



Attack Type: Supply Chain Hardware



Your Chief Information Security Officer asks for a summary of how this attack entered your environment. You need to present a concise explanation to the executive team. How should you explain the attack?

A virus was accidentally downloaded from a phishing link

We experienced a network misconfiguration that allowed external access

Malicious firmware was introduced through a compromised hardware vendor during laptop provisioning

One of our developers pushed insecure code to production

[See The Correct Answer →](#)



Attack Type: Supply Chain Hardware



Your Chief Information Security Officer asks for a summary of how this attack entered your environment. You need to present a concise explanation to the executive team. How should you explain the attack?

- ✗ A virus was accidentally downloaded from a phishing link
- ✗ We experienced a network misconfiguration that allowed external access
- ✓ Malicious firmware was introduced through a compromised hardware vendor during laptop provisioning
- ✗ One of our developers pushed insecure code to production

The mismatched firmware versions and absence of active malware confirm that this was a firmware-level attack originating from the vendor, not user error or misconfiguration.

[See Solutions →](#)



ATTACK TYPE: SUPPLY CHAIN HARDWARE

Recap

Supply chain attacks have grown substantially in recent years. By tampering with physical devices during production, shipping, or deployment or finding weaknesses in software providers, attackers gain the means to inject malicious components or code, corrupt systems, or exfiltrate sensitive data. Victims can range from small businesses to global enterprises, with results including severe financial losses, compromised customer trust, and legal repercussions.

Dell mitigates Supply Chain Hardware attacks by integrating rigorous vendor risk assessments and embedding zero trust principles alongside continuous device validation and independent integrity checks. We fortify hardware integrity across its entire lifecycle.

Learn more about advanced cyber resilience strategies to see how Dell can help you safeguard your organization against Supply Chain Hardware attacks.

[Explore Supply Chain Hardware Attacks Brief →](#)

[🏠 Back to Scenarios](#)



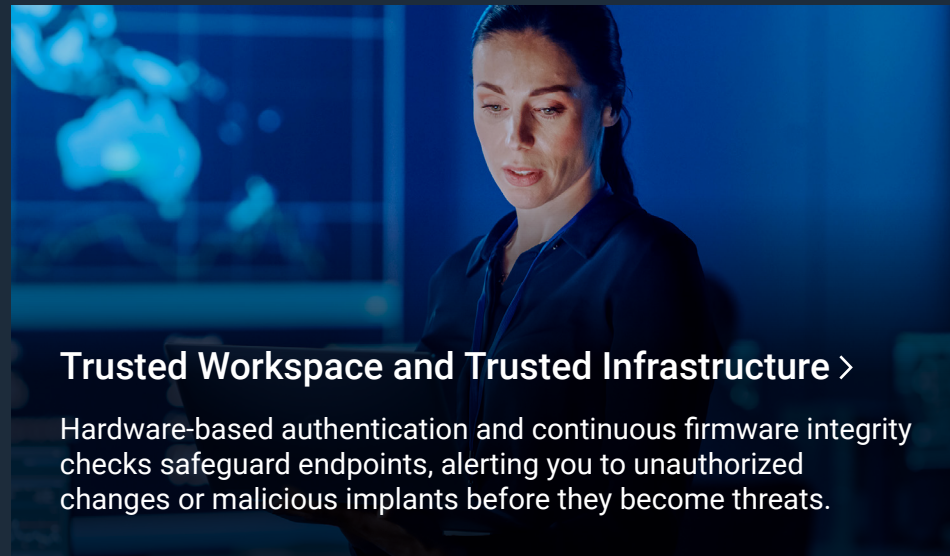
Supply Chain Assurance >

With advanced provenance, tamper-resistant logistics, and transparent sourcing, Dell's supply chain ensures hardware, firmware, and suppliers are rigorously verified before reaching your organization.



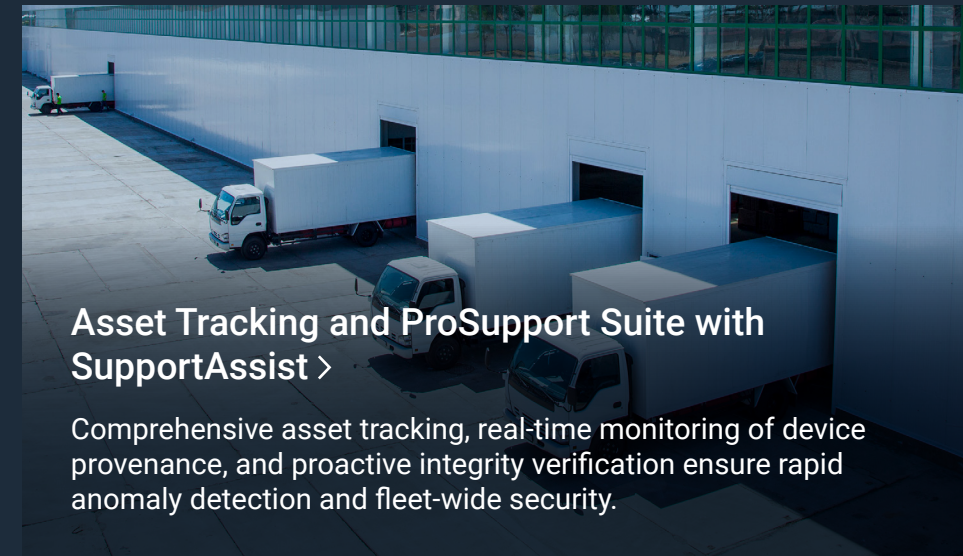
Secure Component Verification (SCV) >

Cryptographic verification of PC components at the factory and during installation ensures authenticity, detects hidden alterations, and mitigates supply chain tampering risks.



Trusted Workspace and Trusted Infrastructure >

Hardware-based authentication and continuous firmware integrity checks safeguard endpoints, alerting you to unauthorized changes or malicious implants before they become threats.



Asset Tracking and ProSupport Suite with SupportAssist >

Comprehensive asset tracking, real-time monitoring of device provenance, and proactive integrity verification ensure rapid anomaly detection and fleet-wide security.



Security Partners: AI-powered Detection and Response >

AI-driven security tools enable continuous monitoring, forensic investigations, and automated containment of tampering or anomalous device behavior, ensuring swift action against supply chain threats.



Attack Type: Supply Chain Software

Your company provides cloud-based analytics software used by hospitals. Your backend services depend on a widely used open-source logging library maintained by a trusted third-party developer on GitHub.

Unbeknownst to your dev team, attackers compromised the GitHub account and inserted a malicious update that includes hidden code designed to:

- Exfiltrate environment variables, including application programming interface (API) keys and JavaScript object notation web tokens (JWT) secrets
- Create a reverse shell when specific IPs make requests
- Remain dormant unless triggered remotely

[Test Your Knowledge →](#)

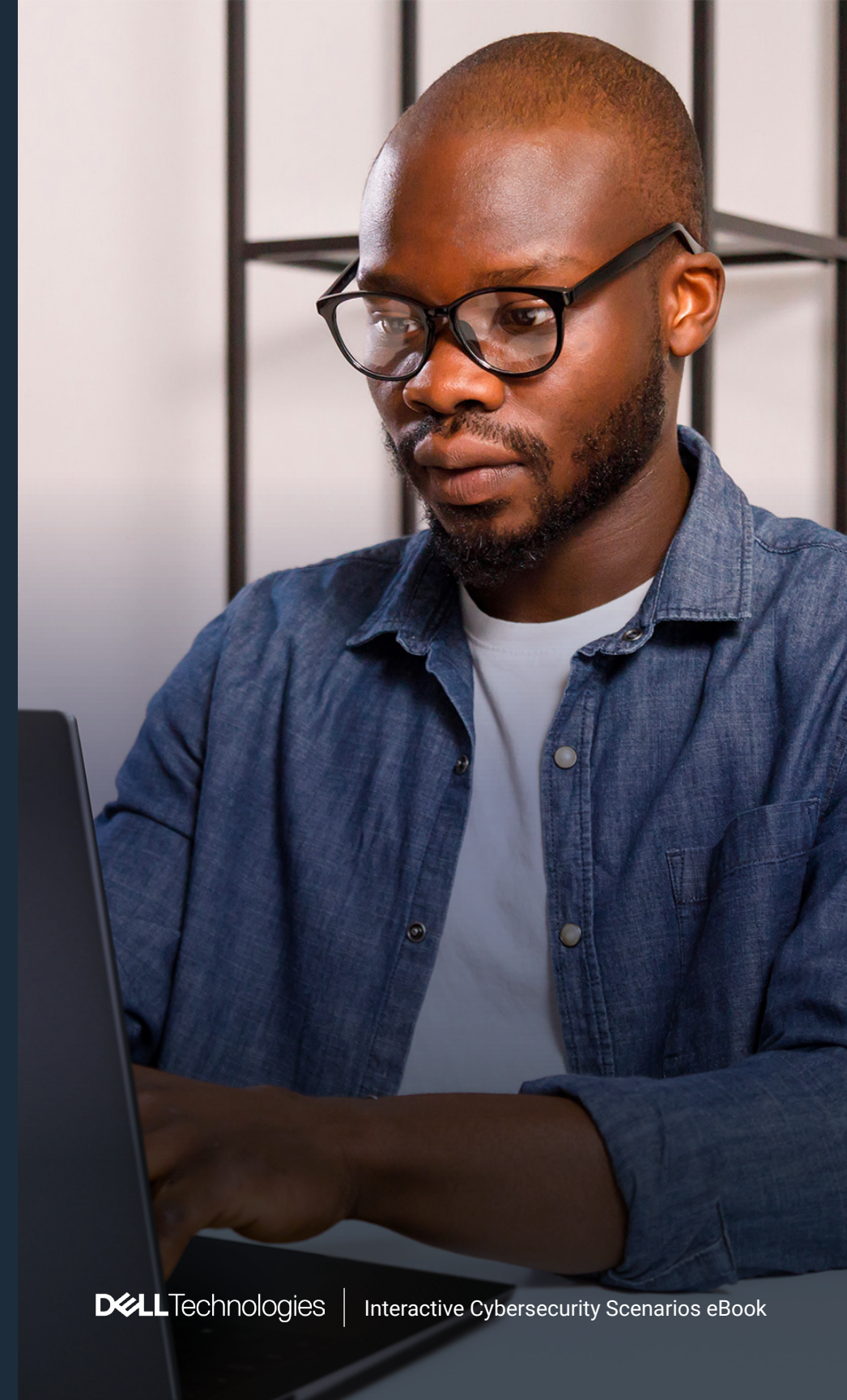
Attack Type: Supply Chain Software



Your API suddenly starts returning 500 errors to key clients. Cloud monitoring flags outbound connections from your containerized services to a domain not previously seen. What is your first response?

- Disable all outbound network traffic from containers
- Reboot affected services to clear any memory issues
- Check for recent code commits in your GitHub repo
- Reach out to the domain's hosting provider

[See The Correct Answer →](#)



Attack Type: Supply Chain Software

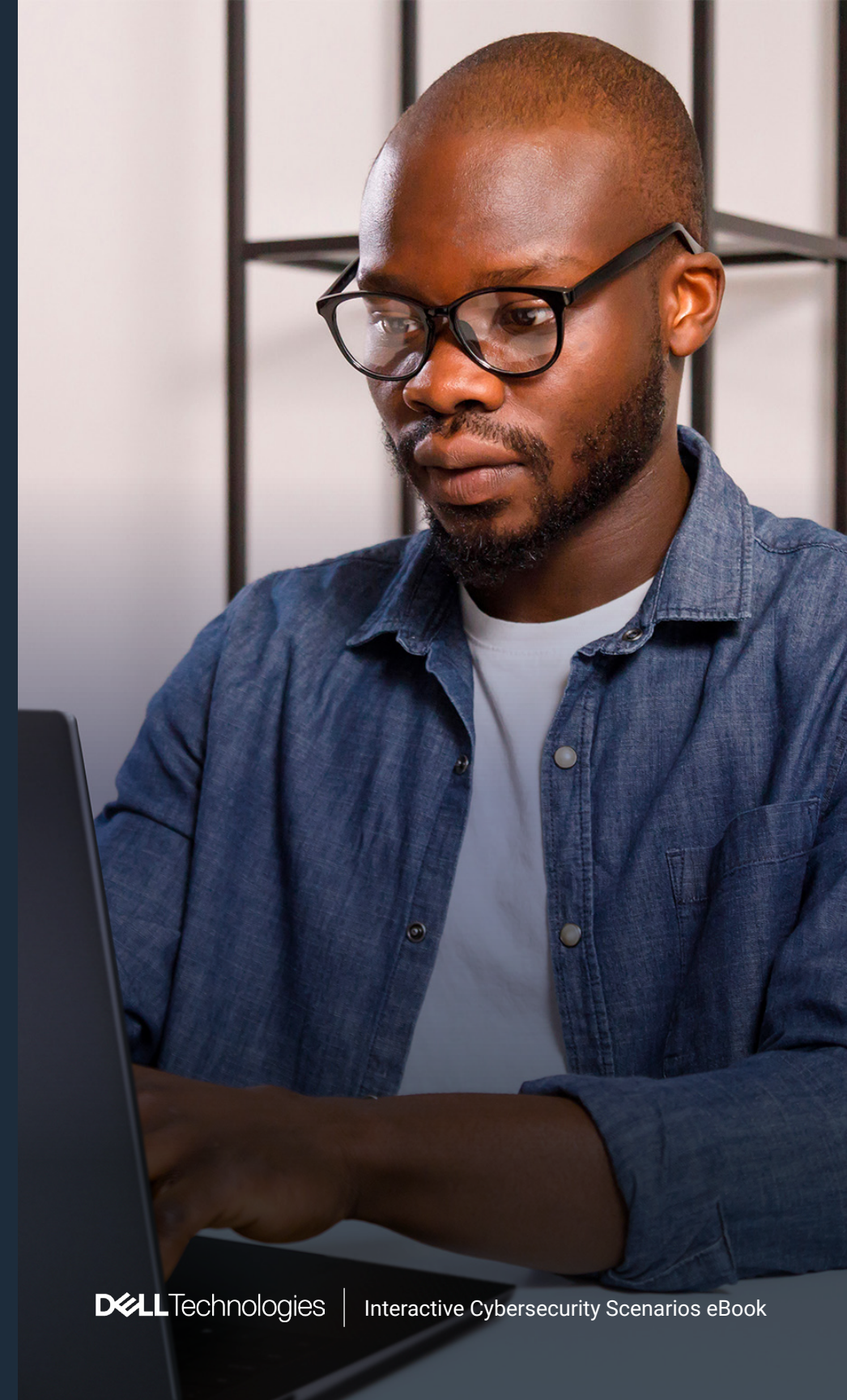


Your API suddenly starts returning 500 errors to key clients. Cloud monitoring flags outbound connections from your containerized services to a domain not previously seen. What is your first response?

- Disable all outbound network traffic from containers
- Reboot affected services to clear any memory issues
- Check for recent code commits in your GitHub repo
- Reach out to the domain's hosting provider

Disabling all outbound network traffic from containers immediately blocks attackers from exfiltrating sensitive data or establishing remote access via the compromised logging library, isolating your environment in real time and buying critical time to investigate, safeguard API keys and secrets, and prevent activation of dormant attack mechanisms.

[Next Question →](#)



Attack Type: Supply Chain Software



Your engineering lead confirms the application auto-pulled code from GitHub three days before the issues began. That version is not yet marked as malicious in any public databases. What's the most responsible immediate action?

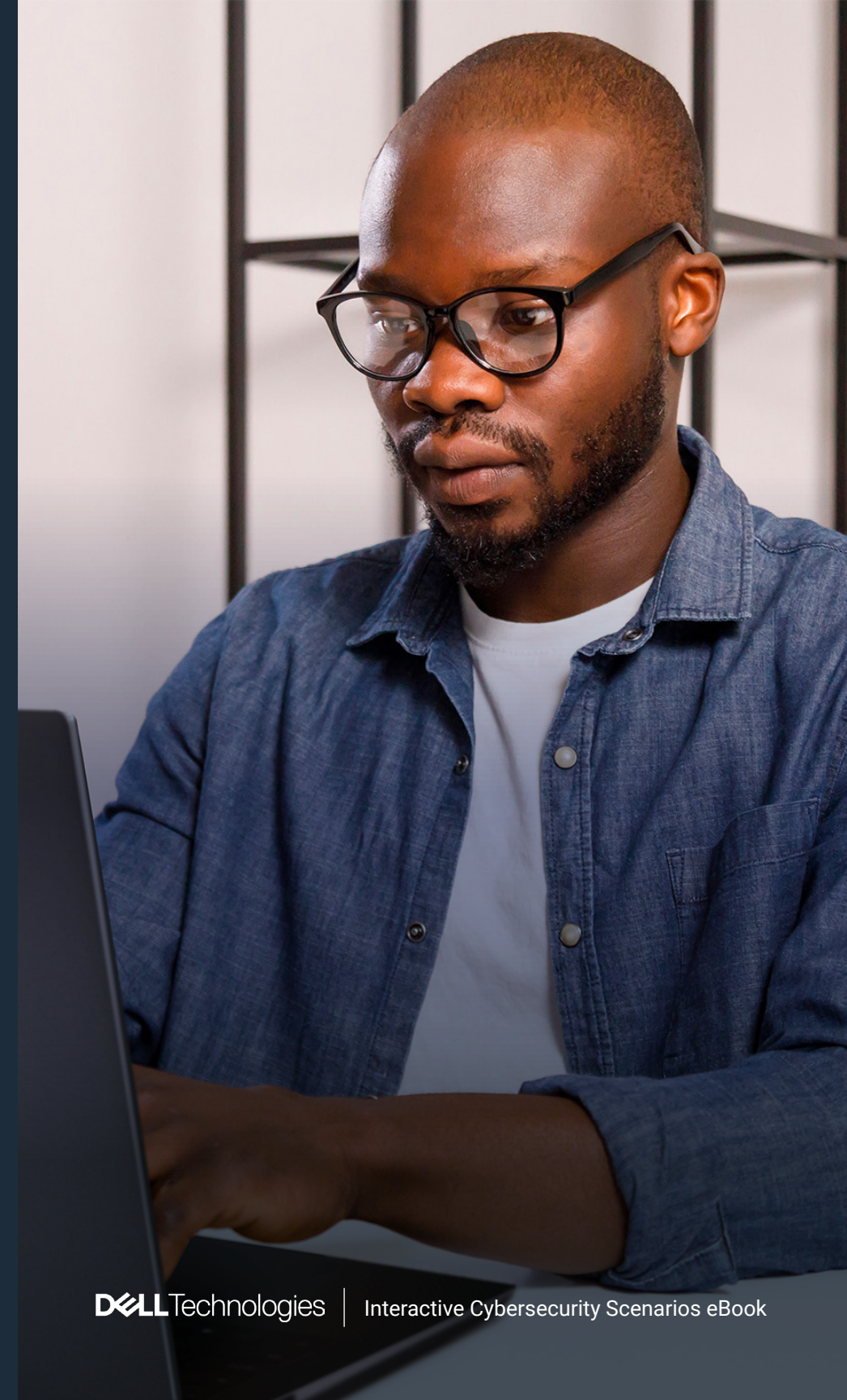
Contact the library maintainer directly via GitHub

Delete all local project dependencies and rebuild

Wait for common vulnerabilities and exposures (CVE) before taking further action

Roll back to the last known safe version of code

[See The Correct Answer →](#)



Attack Type: Supply Chain Software

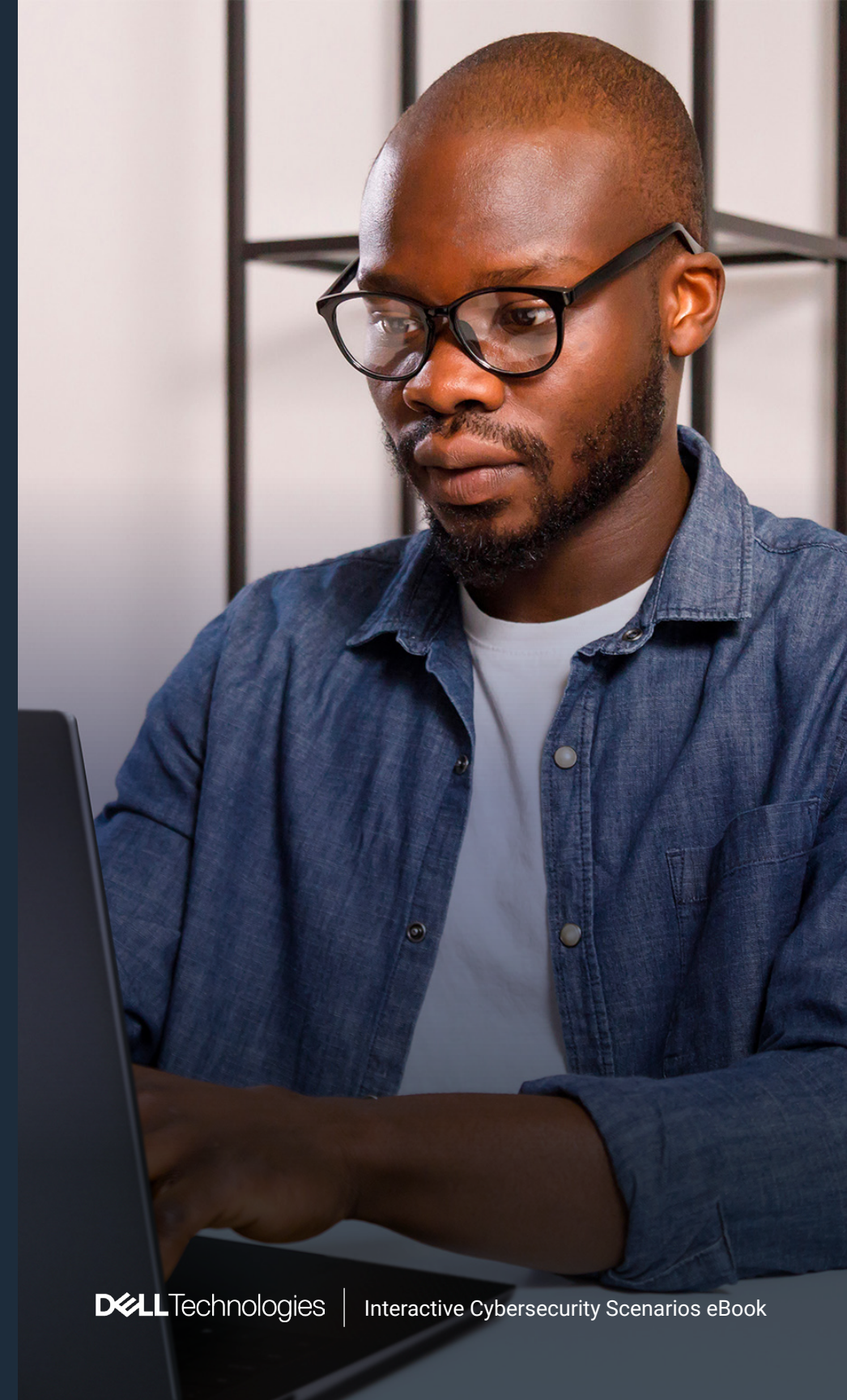


Your engineering lead confirms the application auto-pulled code from GitHub three days before the issues began. That version is not yet marked as malicious in any public databases. What's the most responsible immediate action?

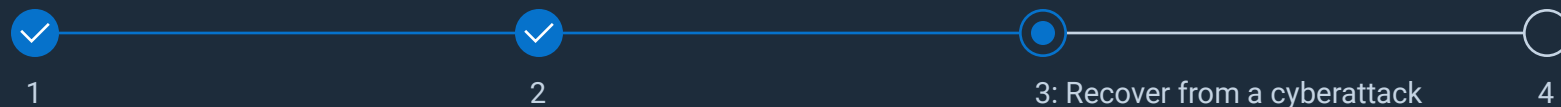
- Contact the library maintainer directly via GitHub
- Delete all local project dependencies and rebuild
- Wait for common vulnerabilities and exposures (CVE) before taking further action
- Roll back to the last known safe version of code

Rolling back to the last known safe code version immediately removes the compromised update, eliminates the attacker's foothold, and restores operational integrity to proactively contain risk and protect sensitive data.

[Next Question →](#)



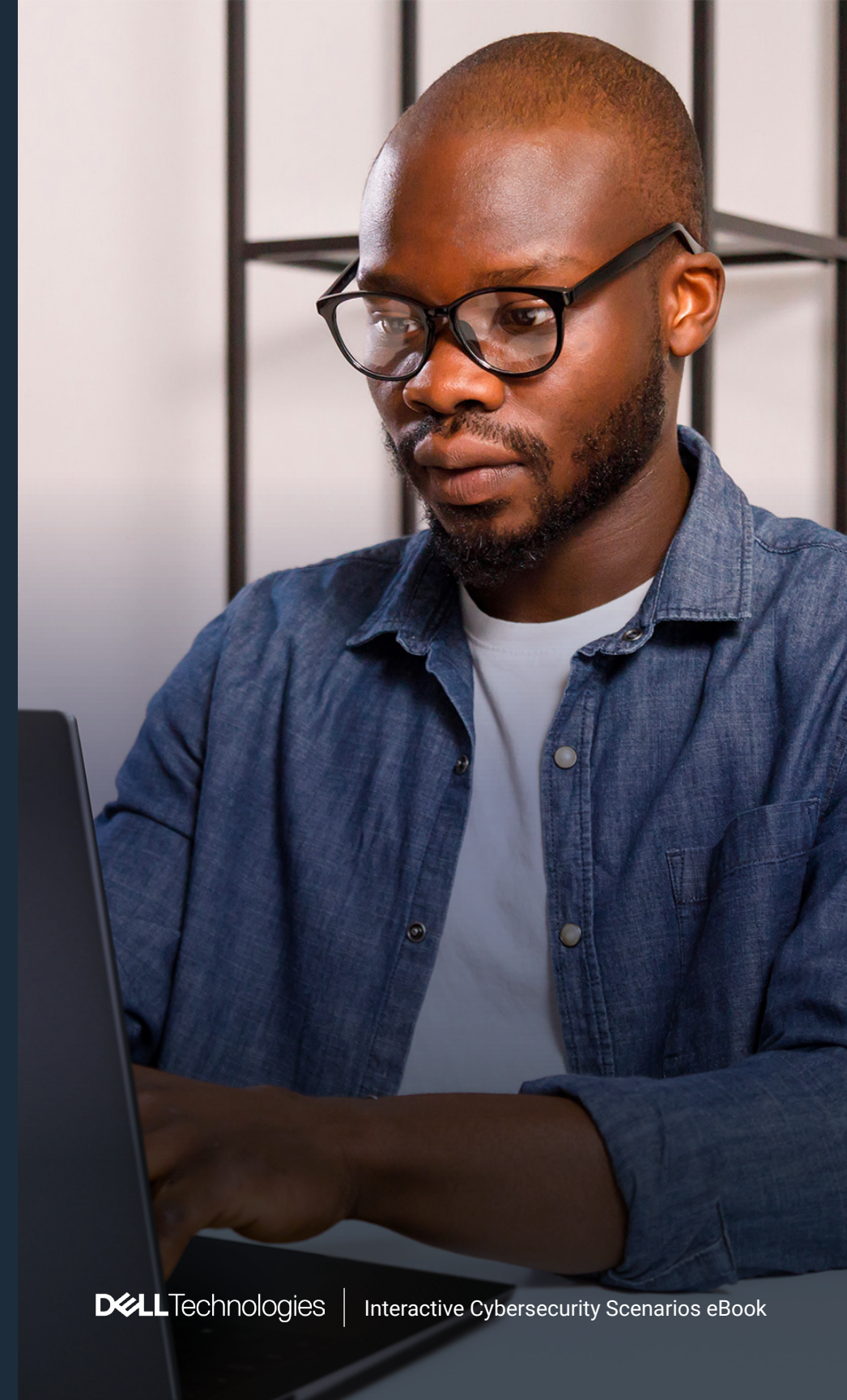
Attack Type: Supply Chain Software



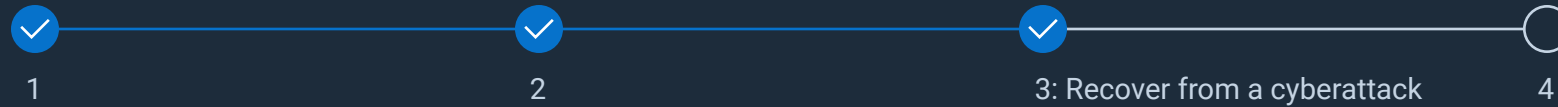
Analysis confirms the library was exfiltrating API keys and cloud credentials. You've identified multiple containers built with the compromised version. Which step is most critical in your containment strategy?

- Revoke and rotate all credentials across affected environments
- Reimage the containers using an updated operating system (OS) image
- Wipe the development team's laptops
- File a takedown notice for the GitHub repo

[See The Correct Answer →](#)



Attack Type: Supply Chain Software



Analysis confirms the library was exfiltrating API keys and cloud credentials. You've identified multiple containers built with the compromised version. Which step is most critical in your containment strategy?

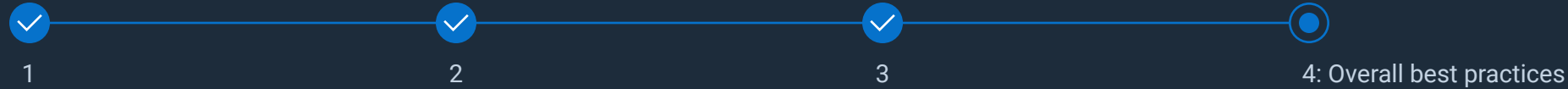
- Revoke and rotate all credentials across affected environments
- Reimage the containers using an updated operating system (OS) image
- Wipe the development team's laptops
- File a takedown notice for the GitHub repo

Revoking and rotating credentials is the first critical step after a cloud compromise, blocking attackers from accessing services, halting data theft, and securing systems regardless of the breach's scope.

[Next Question →](#)



Attack Type: Supply Chain Software



You're asked to explain what happened to your Chief Technology Officer and legal/compliance teams. What is the most accurate and clear explanation? How do you summarize the incident?

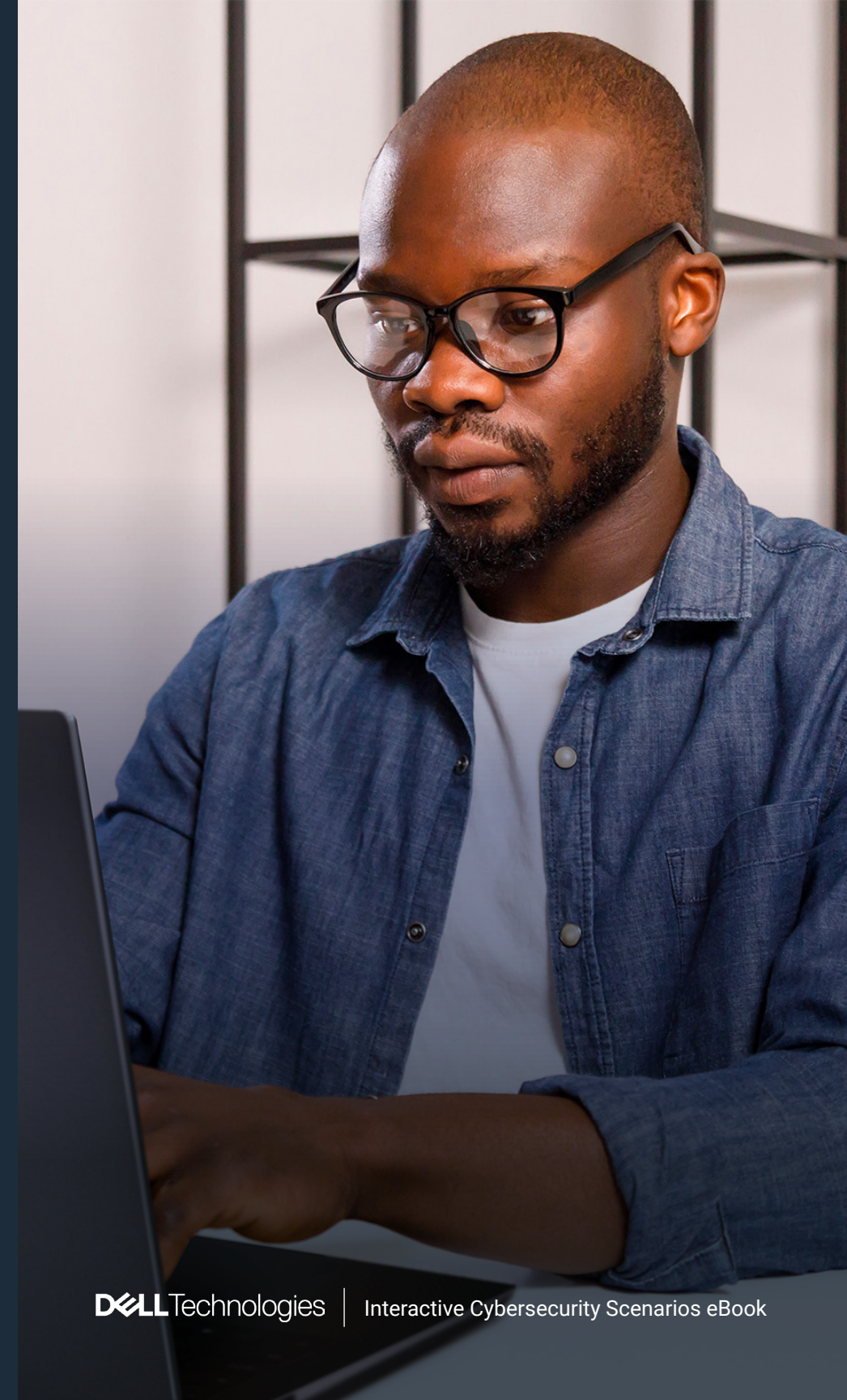
Our internal continuous integration and continuous deployment/delivery (CI/CD) tooling failed, allowing bad code to be deployed

A third-party software dependency was compromised, and our automation pulled it into production

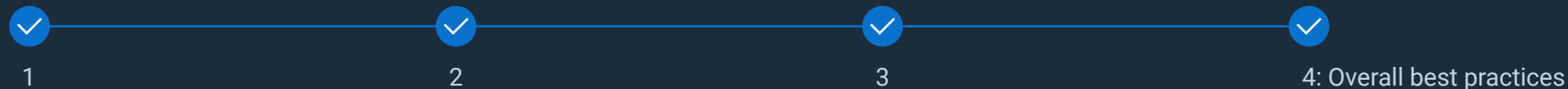
A developer included untested code in a rushed release

An attacker brute-forced our GitHub repository

[See The Correct Answer →](#)



Attack Type: Supply Chain Software

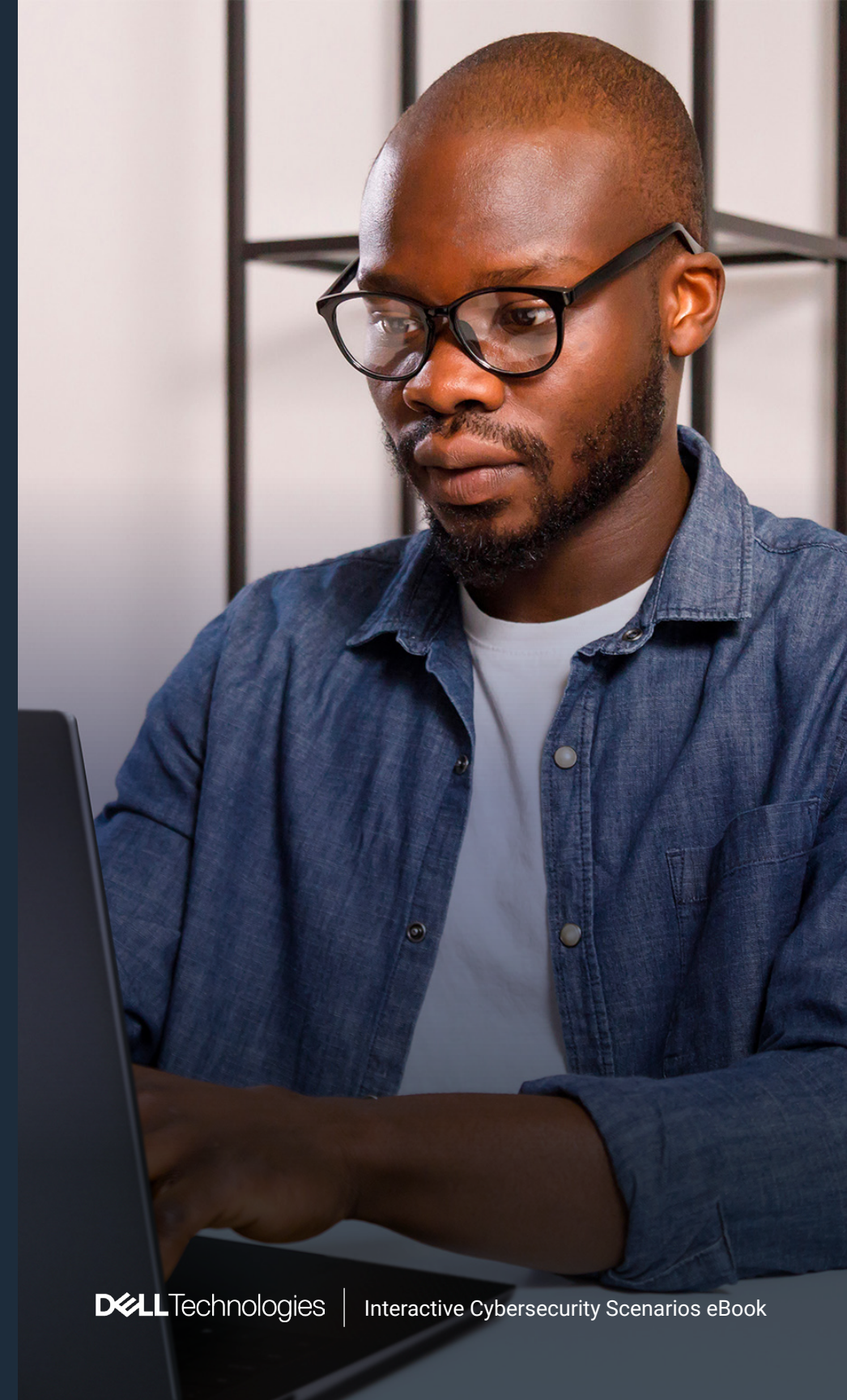


You're asked to explain what happened to your Chief Technology Officer and legal/compliance teams. What is the most accurate and clear explanation? How do you summarize the incident?

- Our internal continuous integration and continuous deployment/delivery (CI/CD) tooling failed, allowing bad code to be deployed
- A third-party software dependency was compromised, and our automation pulled it into production
- A developer included untested code in a rushed release
- An attacker brute-forced our GitHub repository

The root cause was a supply chain attack: attackers compromised a third-party software dependency, and the automated build process pulled the malicious update directly into production, impacting application integrity and sensitive environments and highlighting the risk of malicious updates in trusted external dependencies.

[See Solutions →](#)



ATTACK TYPE: SUPPLY CHAIN SOFTWARE

Recap

Supply chain software cyberattacks exploit vulnerabilities in software updates, third-party integrations, and development environments to embed malicious code that spreads across networks. These attacks can cause widespread data breaches, operational disruptions, and compromise entire ecosystems, impacting businesses of all sizes.

Dell is dedicated to cyber resilience by emphasizing transparency, secure development, and continuous monitoring while maintaining a robust incident response plan to ensure rapid recovery and stakeholder communication.

Learn more about advanced cyber resilience strategies and see how Dell can help you safeguard your organization against Supply Chain Software attacks.

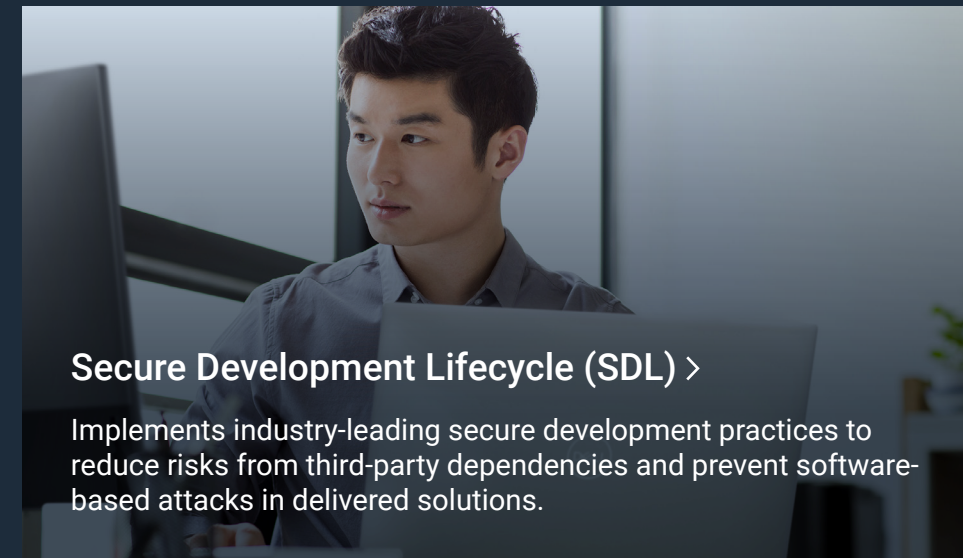
[Explore Supply Chain Software Attacks Brief →](#)

[🏠 Back to Scenarios](#)



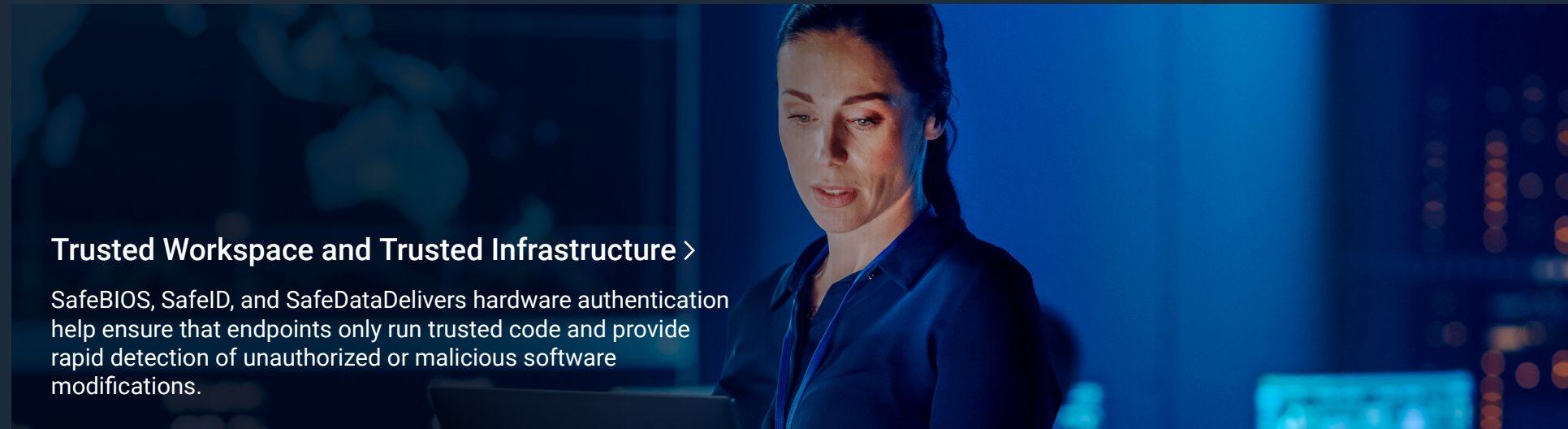
Supply Chain Assurance >

With advanced provenance, tamper-resistant logistics, and transparent sourcing, Dell's supply chain ensures hardware, firmware, and suppliers are rigorously verified before reaching your organization.



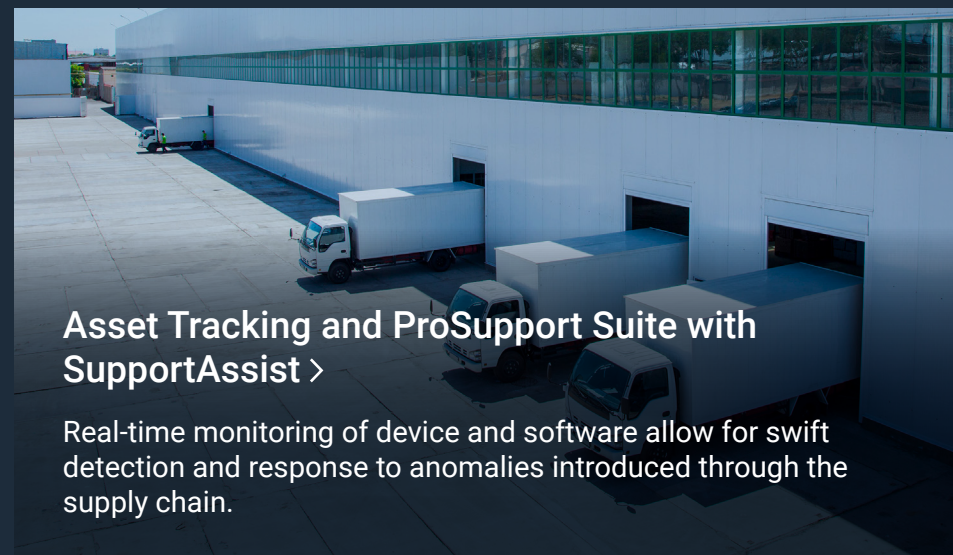
Secure Development Lifecycle (SDL) >

Implements industry-leading secure development practices to reduce risks from third-party dependencies and prevent software-based attacks in delivered solutions.



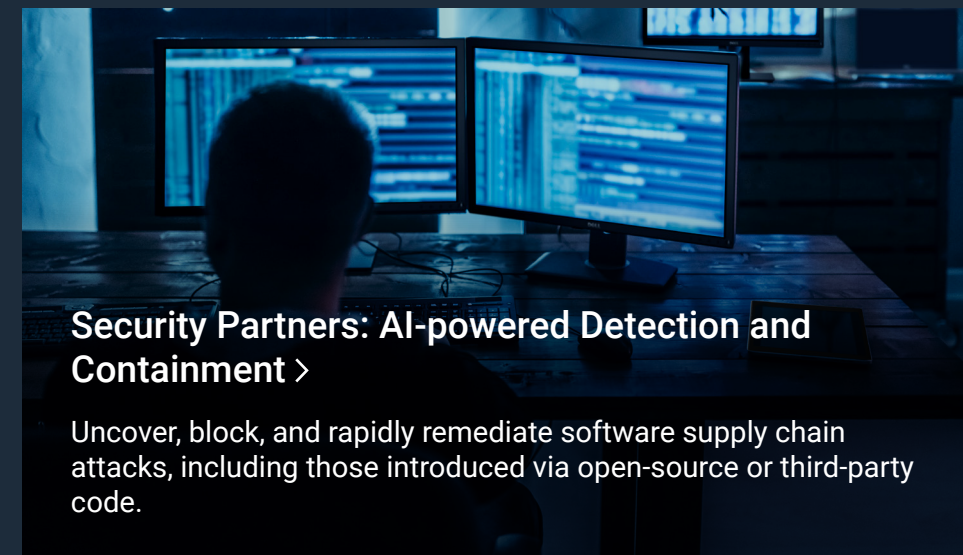
Trusted Workspace and Trusted Infrastructure >

SafeBIOS, SafeID, and SafeDataDelivers hardware authentication help ensure that endpoints only run trusted code and provide rapid detection of unauthorized or malicious software modifications.



Asset Tracking and ProSupport Suite with SupportAssist >

Real-time monitoring of device and software allow for swift detection and response to anomalies introduced through the supply chain.



Security Partners: AI-powered Detection and Containment >

Uncover, block, and rapidly remediate software supply chain attacks, including those introduced via open-source or third-party code.

Attack Type: Zero-Day

You're a security analyst monitoring a company's authentication logs. Recently, users have reported unauthorized access to their accounts, even though they haven't shared their credentials.

Upon investigating the logs, you find the following activity:

```
[INFO] 2025-04-02 14:05:12 - User Login - UserID: 1023 - IP: 192.168.1.15 - JWT Token Issued
[INFO] 2025-04-02 14:07:35 - User Login - UserID: 1023 - IP: 5.62.60.12 - JWT Token Reused
[INFO] 2025-04-02 14:08:00 - User Login - UserID: 1023 - IP: 203.0.113.45 - JWT Token Reused
```

At the same time, a security researcher identifies a vulnerability in the application programming interface (API):

- JavaScript object notation web tokens (JWT) never expire.
- Tokens are stored in local storage instead of HTTP-only cookies.
- No multi-factor authentication (MFA) is enforced.

[Test Your Knowledge →](#)

```
USER AUTHENTICATION SUCCESSFUL | USER_ID=USER123 | IP=192.168.1.100 | USER_AGENT="MOZILLA/5.0 (WINDOWS NT 10.0; WIN64; X64)
CESS TOKEN GENERATED | USER_ID=USER123 | TOKEN_ID=TK_7AB89C2D | EXPIRES_AT=2025-04-02 11:15:23Z | ALGORITHM=HS256
.FRESH TOKEN GENERATED | USER_ID=USER123 | TOKEN_ID=RTK_4E5F6G7H | EXPIRES_AT=2025-09-23T00:15:23Z
OKEN VALIDATION SUCCESSFUL | USER_ID=USER123 | TOKEN_ID=TK_7AB89C2D | ENDPOINT=/API/USER/PROFILE | IP=192.168.1.100
OKEN REFRESH SUCCESSFUL | USER_ID=USER123 | OLD_TOKEN_ID=TK_7AB89C2D | NEW_TOKEN_ID=TK_9X8Y7Z6W | IP=192.168.1.100
MULTIPLE FAILED LOGIN ATTEMPTS | USERNAME=ADMIN | IP=203.0.113.45 | ATTEMPTS=3 | TIME_WINDOW=5MIN
ACCOUNT TEMPORARILY LOCKED | USER_ID=ADMIN_USER | IP=203.0.113.45 | REASON=TOO_MANY_FAILED_ATTEMPTS | LOCK_DURATION=15MIN
INVALID TOKEN SIGNATURE | TOKEN_ID=TK_INVALID123 | IP=198.51.100.78 | ENDPOINT=/API/ADMIN/USERS | ERROR="SIGNATURE VERIFICATION FAILED"
SUSPICIOUS JWT MANIPULATION ATTEMPT | IP=198.51.100.78 | USER_AGENT="CURL/7.68.0" | TOKEN_HEADER_MODIFIED=TRUE
EXPIRED TOKEN USED | TOKEN_ID=TK_EXPIRED456 | USER_ID=USER456 | IP=172.16.0.50 | EXPIRES_AT=2025-04-02 10:35:22Z
- REDIRECT TO LOGIN | USER_ID=USER456 | REASON=TOKEN_EXPIRED
EC - SQL INJECTION ATTEMPT DETECTED | IP=185.199.108.153 | ENDPOINT=/API/SEARCH | PAYLOAD="'; DROP TABLE USERS; --" | BLOCKED=TRUE
IP ADDED TO TEMPORARY BLOCKLIST | IP=185.199.108.153 | DURATION=1HOUR | REASON=SQL_INJECTION_ATTEMPT
TOKEN USED FROM DIFFERENT IP | USER_ID=USER789 | TOKEN_ID=TK_MOBILE987 | ORIGINAL_IP=10.0.0.25 | CURRENT_IP=203.0.113.89 |
- GEO-LOCATION CHANGE DETECTED | USER_ID=USER789 | PREVIOUS_LOCATION="NEW YORK, US" | CURRENT_LOCATION="LONDON, UK"
BULK TOKEN REVOCATION | ADMIN_USER_ID=ADMIN123 | REVOKED_COUNT=25 | REASON=SECURITY_INCIDENT | INCIDENT_ID=INC-2025-0916-001
- CSRF TOKEN MISMATCH | SESSION_ID=SESS_ABC123 | IP=192.168.1.200 | ENDPOINT=/API/PROFILE/UPDATE | EXPECTED_TOKEN=CSRF_DEF456 |
- POTENTIAL CSRF ATTACK | SESSION_ID=SESS_ABC123 | IP=192.168.1.200 | USER_AGENT="MACINTOSH; INTEL MAC OS X 10.15.7"
- TOKEN BLACKLISTED | TOKEN_ID=TK_COMPROMISED111 | USER_ID=USER555 | REASON=USER_REPORTED_COMPROMISE | BLACKLIST_EXPIRES=2025-09-23T11:00:55Z
- RATE LIMIT EXCEEDED | USER_ID=USER888 | IP=198.51.100.44 | ENDPOINT=/API/DATA/EXPORT | REQUESTS=1000 | TIME_WINDOW=1HOUR | LIMIT=100
C - RATE LIMIT APPLIED | USER_ID=USER888 | THROTTLE_DURATION=30MIN
5 SEC - PRIVILEGE ESCALATION ATTEMPT | USER_ID=USER999 | CURRENT_ROLE=USER | ATTEMPTED_ROLE=ADMIN | ENDPOINT=/API/ADMIN/SYSTEM/CONFIG |
SEC - SECURITY INCIDENT CREATED | INCIDENT_ID=INC-2025-0916-002 | SEVERITY=HIGH | USER_ID=USER999 | TYPE=PRIVILEGE_ESCALATION
WT - KEY ROTATION COMPLETED | OLD_KEY_ID=KEY_V1_2025 | NEW_KEY_ID=KEY_V2_2025 | GRACE_PERIOD=24HOURS
WT - LEGACY TOKENS MARKED FOR RE-ISSUANCE | COUNT=1500 | AFFECTED_TOKENS=1500 | STATUS=SUCCESS
SEC - ANOMALOUS USER BEHAVIOR DETECTED | USER_ID=USER777 | PATTERN=UNUSUAL_API_USAGE | SCORE=8.5/10 | ACTIONS=["LOGIN_FROM_NEW_COUNTRY",
JRS_ACTIVITY"]
SEC - ADDITIONAL MONITORING ENABLED | USER_ID=USER777 | MONITOR_DURATION=72HOURS
- USER LOGIN - USERID: 1023 - IP: 192.168.1.15 - JWT TOKEN ISSUED
- USER LOGIN - USERID: 1023 - IP: 5.62.60.12 - JWT TOKEN REUSED
- USER LOGIN - USERID: 1023 - IP: 203.0.113.45 - JWT TOKEN REUSED
AUTH - LOGOUT SUCCESSFUL | USER_ID=USER123 | SESSION_DURATION=4HOURS.0MIN | TOKENS_REVOKED=2 | IP=192.168.1.100
JWT - ACCESS TOKEN REVOKED | TOKEN_ID=TK_NEW456 | USER_ID=USER123 | REASON=USER_LOGOUT
JWT - REFRESH TOKEN DETECTED | TARGET_ENDPOINT=/API/AUTH/LOGIN | SOURCE_IP=203.0.113.67 | ATTEMPTS=500 | TIME_WINDOW=10MIN
15 SEC - BRUTE FORCE ATTACK DETECTED | IP=203.0.113.67 | BAN_DURATION=24HOURS | REASON=BRUTE_FORCE_ATTACK
30-15 SEC - EMERGENCY IP BAN ACTIVATED | IP=203.0.113.67 | BAN_DURATION=24HOURS | EXPORT_ID=EXP_20250916_001 | RECORDS_COUNT=10000 | TIME_RANGE="2025-09-15T00:00:00Z
2 AUDIT - SECURITY LOG EXPORTED | ADMIN_USER_ID=SECURITY_ADMIN | EXPORT_ID=EXP_20250916_001 | RECORDS_COUNT=10000 | TIME_RANGE="2025-09-15T00:00:00Z"
```


Attack Type: Zero-Day



As a security team, since no warning bells went off you suspect this as a Zero-Day attack, how would you go about confirming this?

Log all users off their systems

Identify key anomalous authentication behaviors in logs

Call friends in other companies to see if they are having the same issue

Try to correlate with other security abnormal activity

[See The Correct Answer →](#)



Attack Type: Zero-Day



As a security team, since no warning bells went off you suspect this as a Zero-Day attack, how would you go about confirming this?

- Log all users off their systems
- Identify key anomalous authentication behaviors in logs
- Call friends in other companies to see if they are having the same issue
- Try to correlate with other security abnormal activity

Pinpointing anomalous authentication behaviors, like as unusual login times, credential reuse, or access from atypical devices, and correlating them with other abnormal security activity like data access anomalies or privilege escalation confirms a coordinated Zero-Day attack.

[Next Question →](#)



Attack Type: Zero-Day



Since the vulnerability is unknown, security teams must limit damage while investigating. How would you go about doing this?

- 1. Invalidate all authentication sessions system-wide
- 2. Focus all resources on the point of entry of the attack
- 3. Enforce multi-factor authentication (MFA) logins only
- 4. Rely on current static firewalls or web application firewall (WAF) rules

[See The Correct Answer →](#)



Attack Type: Zero-Day



Since the vulnerability is unknown, security teams must limit damage while investigating. How would you go about doing this?

- Invalidate all authentication sessions system-wide
- Focus all resources on the point of entry of the attack
- Enforce multi-factor authentication (MFA) logins only
- Rely on current static firewalls or web application firewall (WAF) rules

Together, these actions strengthen security and minimize risk while cutting off attacker access so security teams can investigate and resolve the underlying vulnerability.

[Next Question →](#)



Attack Type: Zero-Day



Dell PCs have technologies such as Secure Boot, trusted platform modules (TPM), basic input/output system (BIOS) Password Protection, and SafeBIOS. How can these help in a Zero-Day attack?

Protects against credential dumping attacks that steal application programming interface (API) tokens

Prevents an attacker with physical access from bypassing operating system (OS) security to install malware that steals authentication tokens

Ensures that attackers cannot manipulate BIOS settings to weaken OS security, which could lead to API session hijacking

All of the above

[See The Correct Answer →](#)



Attack Type: Zero-Day



Dell PCs have technologies such as Secure Boot, trusted platform modules (TPM), basic input/output system (BIOS) Password Protection, and SafeBIOS. How can these help in a Zero-Day attack?

- ✓ Protects against credential dumping attacks that steal application programming interface (API) tokens
- ✓ Prevents an attacker with physical access from bypassing operating system (OS) security to install malware that steals authentication tokens
- ✓ Ensures that attackers cannot manipulate BIOS settings to weaken OS security, which could lead to API session hijacking
- ✓ All of the above

This layered approach provides comprehensive protection against Zero-Day attacks targeting BIOS, firmware, credentials, and system configurations. By preventing manipulation, unauthorized access, and credential theft, these technologies remain effective even when new vulnerabilities are discovered by attackers.

Next Question →



Attack Type: Zero-Day



What is the best way to try to prevent Zero-Day attacks from happening?

Don't use open-source software

Leverage zero trust principles

Keep everything patched including operating systems (OS), firmware, application programming interfaces (APIs), libraries, and containers

Put up an electrified gate around the company to keep the threat actors out

[See The Correct Answer →](#)



Attack Type: Zero-Day



What is the best way to try to prevent Zero-Day attacks from happening?

- Don't use open-source software
- Leverage zero trust principles
- Keep everything patched including operating systems (OS), firmware, application programming interfaces (APIs), libraries, and containers
- Put up an electrified gate around the company to keep the threat actors out

If unknown vulnerabilities or unpatched systems exist, zero trust principles prevent Zero-Day attacks by removing implicit trust from users and devices, enforcing continuous authentication, restricting access to necessary information only, and containing adversary movement to significantly reduce organizational risk from undiscovered threats.

[See Solutions →](#)



ATTACK TYPE: ZERO-DAY

Recap

A Zero-Day attack involves exploiting an undisclosed security vulnerability in software or hardware before a patch or fix is available. Attackers take advantage of the window of opportunity, often causing widespread disruption before the vulnerability is discovered and addressed.

Dell tackles Zero-Day attacks with zero trust controls, network segmentation, rapid containment, and user education further strengthening defenses against emerging threats.

Learn more about advanced cyber resilience strategies and see how Dell can help you safeguard your organization against Zero-Day attacks.

[Explore Zero-Day Attacks Brief →](#)

[🏠 Back to Scenarios](#)



Trusted Workspace and Trusted Infrastructure >

Defend endpoints and infrastructure. With SafeBIOS, SafeID, SafeData protections, and zero trust frameworks like multi-factor authentication (MFA) and role-based access control (RBAC), Dell delivers layered defenses to limit exploit paths and ensure hardware authentication.



PowerEdge Servers >

Secure Boot, silicon root of trust, and SmartFabric network segmentation restrict lateral movement, ensuring only trusted code runs on your infrastructure.



Security Partners >

Advanced threat intelligence, manage detection and response (MDR), extended detection and response (XDR), and fine-grained access controls help detect, hunt, and contain Zero-Day attacks before they spread.



PowerProtect Portfolio >

Immutable backups, isolated cyber recovery vaults, and AI-driven CyberSense analytics ensure fast restoration and resilience after zero-day breaches.



Security and Resilience Services >

From patch management to incident response, Dell's experts provide rapid containment, forensic investigation, and resilience planning to counter zero-day threats.



DELL Technologies