Be Breach-Ready Using Microsegmentation

THE CHALLENGE OF MODERN CYBER THREATS 2

WHAT IS A BREACH AND WHY SHOULD ORGANIZATIONS PREPARE? 4

The Timeline of breach from the point-of-view of the Attacker 4

The Breach from the Point-of-View of the Cyber Responder 4

THE GAP IN CYBERSECURITY TOOLS IN THE CONTEXT OF A BREACH 5

Filling the gap: Proactive Cyber Defense 5

THE BENEFITS OF BEING BREACH READY 6

Before the breach 6

During the breach 6

After the breach 6

HOW COLORTOKENS HELPS ORGANIZATIONS BE BETTER PREPARED FOR BREACHES 7

Business continuity with isolation and quarantine 8

Actionable visibility of your enterprise landscape 8

Implementation without disruption 8

ColorTokens Gives You Measurable Security Increases in Less than 30 Days 8

ColorTokens lets you Visualize and Communicate Security Gains 9

GETTING STARTED 9

APPENDIX–THE ANATOMY OF A BREACH 10

Attack timeline of the City of Dallas breach in 2023 10

Affected systems 11

Recovery phases 13

The Challenge Of Modern Cyber Threats

For enterprises today a breach of their cyber security is a matter of when, not if. Every one of the high-profile breaches we've heard of in the last few years has, by definition, gotten through the perimeter security: firewalls, anti-virus, authentication, and endpoint detection. These breaches resulted in significant business disruption, multi-million-dollar financial losses, reputational loss and in some cases, restructuring of the IT/security teams and leadership. And for every breach we've heard of there are probably a thousand we haven't.

CISOs and IT leaders want to do everything possible to prevent a breach, but there's an insurmountable problem in cyber security: the attacker only needs to be right once, the perimeter security must be right every time.

Leaders want to know that they'll have resilience to continue their critical business processes and protect their precious data, despite the inevitable breach. They need wide visibility of their enterprise network so they can understand risk and be proactively positioned to contain the effect of any attack. In a phrase, they want to be breach ready.

This paper will describe a solution to this challenge which provides resilience through defense-in-depth. Going beyond traditional perimeter cybersecurity, the solution approach provides proactive cyber defense. It will stop the spread of ransomware and malware despite the inevitable breach before catastrophic damage occurs. It will protect all types of assets and environments—IT, IoT and OT, on-premise, in the cloud, and in containers—so there are no soft spots in the defense. And it will provide this capability with fast time-to-value, and without disruption of on-going business processes.

What Is A Breach And Why Should Organizations Prepare?

A security incident (compromise of confidentiality, integrity, data exfiltration, or loss of availability of digital assets) becomes a breach when there is confirmed and severe loss to the business. Some high profile breaches of familiar brand names that occurred in recent months include[1] :

- American Airlines
- UPS Canada
- Reddit
- Intellihartx
- Apria Healthcare
- Suzuki
- PharMerica
- US Dept. of Trans.
- Discord
- T-Mobile
- Pizza Hut/KFC
- MSI
- Western Digital
- ChatGPT
- Forever 21
- Duolingo
- IBM MOVEit
- Northern Ireland Police
- Maximus
- Gov't of Norway
- US House of Reps.
- Activision
- Atlassian
- Optus
- Weee!
- Sharp HealthCare
- MGM Resorts
- Caesars Entertainment
- Topgolf Callaway
- Freecycle

[1] Data Breaches That Have Happened in 2023 So Far - Updated List (tech.co)

Beginning on Dec. 18, 2023, in addition to annual reporting, new SEC rules require publicly traded companies to report material cyber incidents to the SEC within four days if the incident is determined to be material. The disclosure must be made on SEC Form 8-K.[2] It's safe to assume that the number of unreported incidents in private companies and organizations is much higher than the publicly disclosed breaches.

We can predict with confidence that the risk level will only increase in the foreseeable future. Some macro factors that cause increased risk in the cyber landscape include:

- Increasing digital transformation and convergence
- The advent of AI enabling threat actors
- Increasing regulation and liability to penalties
- The increase in remote working
- Vanishing perimeter due to partners and extended supply chain integration
- IT integration with Operational Technology to gain increased efficiency and competitive advantage.

Methods of attack include e-mail phishing, social engineering, telephone-oriented attack delivery (TOAD), multifactor authentication bypass, exploitation of open-source code and many others. Whatever the mode of attack, the result is that organizations can suffer financial loss through interruption of their business processes, liability due to the loss of customer (or patient) information, and significant but less tangible loss of brand reputation. In fact, the average cost of a breach worldwide in 2023 was $4.35 million and in the United States it was more than twice that at $9.44 million.[3]

Recent attacks have been executed through people or devices inside the network trying to access services or servers that they are not supposed to connect with. In most organizations, approximately 85% of all network traffic occurs internally, in the so-called east-west axis, compared to 15% of traffic occurring with the external internet, or the north-south axis. Since most cybersecurity strategies focus on the north-south traffic, 85% of inside traffic is far less controlled and that becomes the vector for attack.

This is the motivation behind the zero trust architecture approach. While no prudent CISO or IT leader would abandon their perimeter defense strategies, a defense-in-depth strategy is needed in accordance with the zero trust concept of assuming a breach. An architecture is needed that has the resilience to continue business operations—despite a successful attack.

This is our goal at ColorTokens. Our microsegmentation platform is a foundational part of an overall zero trust architecture. It gives you resilience to continue business operations when the inevitable breach occurs. We help you view, analyze, prevent, and isolate any breach so that you can control its impact on your business.

In addition to the peace-of-mind that CISOs and IT leaders can gain from knowing that they have a breach-ready posture, they will be more comfortable when articulating their defense-in-depth strategy—a proactive cyber defense—to their stakeholders. This is especially true for public companies, which must document their processes for managing risks from cybersecurity threats in the new SEC Regulation S-K, Item 106, as well as describe the board of directors' oversight of cybersecurity risks.[4]

[2] SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies
[3] Cost of a data breach 2023 | IBM
[4] Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

The Timeline of breach from the point-of-view of the Attacker

1. **Recon and Develop**
   This is where an attacker is decerning what is a valuable and a vulnerable target and sending out feelers.

   Timeline of detection and mitigation: there is no way to determine how long the attackers prepared before starting.

2. **Initial Access and Escalation**
   There is some sort of phishing or compromised remote access to gain entry and establish a foothold.

   Methods of detection and mitigation: there are many tools and technologies to prevent and detect this phase. In fact, the challenge is that noise hides the actual signal, so determining severity and impact is hard. This phase takes minutes.

3. **Stealth Discovery and Lateral Movement**
   This is where the attacker is stealthily trying to discover assets and spread malware laterally through the systems.

   Timeline of detection and mitigation: not a lot of tools to detect this. Post log analysis helps with forensics.

   This may last for months as the attacker is trying to be stealthy and fly under the radar.

4. **Execution and Impact**
   This is where data is being exfiltrated, and systems are being stopped.

   Timeline and detection and mitigation: detection is not hard as the business systems start getting impacted unless it is purely a data theft. This is where the cyber breach responder really starts getting involved and they are now in crisis management mode.

The Breach from the Point-of-View of the Cyber Responder

1. **Determine if it is a real breach**
   Verify the indication is real and severe and warrants immediate action and investigation. This task is complicated by the signal-to-noise problem in perimeter cyber security tools. Success in this phase is largely driven by the experience and expertise of the security team. This need in impacted by the shortage in cyber security staffing.

2. **Who needs to be informed and involved?**
   Inform the appropriate organizations and personnel. Protocols for notification must be developed for each organization, and as mentioned above, if the company is subject to SEC or other regulation this includes external communications.

3. **How do I stop the spread?**
   Proactive measures should be put in place to control traffic if an incident is detected. This should be automated and instant if possible. The idea is to stop the spread by disconnecting systems, but the effect on valid business processes of the traffic controls imposed should be understood in advance.

4. **How do I understand the impact?**
   Identify what systems are infected because of the breach. Understand the impact to data and services.

5. **Determine a recovery plan and execution timeline**
   Establish phases and recovery of business operations.

[5] The cybersecurity industry is short 3.4 million workers—that's good news for cyber wages | Fortune Education

The Gap In Cybersecurity Tools in The Context Of A Breach

Cybersecurity tools like firewalls, anti-virus and Endpoint Detection and Response (EDR) technology are used to identify and stop threats and alert administrators accordingly. They do this by collecting and aggregating data from endpoints. They are an important and necessary security strategy. Their focus is to prevent a beach from occurring. They can identify which assets are infected, but do not give context of what that asset is used for or its criticality to business operations, privacy, or financial systems.

A properly planned approach to proactive cyber defense using microsegmentation addresses this gap. Microsegmentation is an integral part of cyber defense. It differs from EDR, firewall and anti-virus defense strategies in that it assumes that a successful breach has already occurred. Microsegmentation stops the spread of malware or ransomware after a breach by establishing a micro-perimeter around every asset in the enterprise network and preventing their lateral movement. It is a tool to decrease the blast radius of a breach, and the attack surface available to attackers. It allows you to define which groups of assets should communicate, which should normally not communicate, and what the context of that asset is in terms of the business. Microsegmentation policy is defined using this context:

- Assets which are most valuable in terms of confidentiality, availability, and business integrity.
- Business functions which are impacted when these assets are compromised.
- Assets which are necessary for business continuity.

When an attacker successfully breaches a device undetected, the extent of the damage will be determined by where the attacker can move next. The goal of microsegmentation is to create groups of network resources fenced-in by micro-perimeters which limit the lateral, or east-west, movement of an attack that has penetrated the perimeter cybersecurity. Microsegmentation stops ransomware and other malware before catastrophic damage occurs by using application ringfencing, granular traffic controls, and threat-mitigation policies. It ensures that attacks that have managed to enter the network will ultimately hit a roadblock.

Filling the gap: Proactive Cyber Defense

Preparing microsegmentation policy proactively before the inevitable breach addresses the necessary tasks defined in the section above:

- **Who needs to be informed and involved:** microsegmentation policy lets you understand the context of the asset so you know the appropriate organizations and personnel affected.
- **How do I stop the spread:** Microsegmentation lets you establish proactive measures to control traffic if an incident is detected, in an automated and instant way. It lets you stop the spread by disconnecting and isolating microsegments to alleviate the effect on valid business processes.
- **How do I understand the impact:** microsegmentation lets you Identify which systems are infected and which other assets or applications are impacted because of the compromised asset.
- **Determine a recovery plan and execution timeline:** It lets you establish phases and recovery of business operations, in terms of business criticality of each microsegment.

Microsegmentation provides a cyber defense approach that both seeks to prevent breaches from occurring, provides the capability to stop the spread of an attack in the event of a breach, and provides for a containment and recovery strategy. Essentially, it allows organizations to be resilient even in the face of a successful attack. It gives IT and security leaders peace of mind from being breach ready.

The Benefits Of Being Breach Ready

Being "breach-ready" means that you have prepared in advance with a defense-in-depth strategy in accordance with the zero trust model of assuming a breach. To back up your cybersecurity measures you have in place a proactive cyber defense. The perimeter is well protected, but you also have measures in place to provide a contingency "plan B" so you can maintain resilience even in the case of a successful attack. During a breach you are in control and can reduce the impact of the breach by 90% or greater.

Before the breach

Planning and preparation phase

- Contain and limit the spread and lateral movement.
- Microsegment all your systems
- Ensure mitigation plans work regardless of the breach scenario
- Simulate and test all your response plans against attacks
- Design and simulate breach readiness and response plans

During the breach

- Know exactly which segments and systems are affected
- This will help determine who to inform, whether to classify as a breach
- Quickly ensure core business continuity
- Isolate critical business systems, quarantine affected systems
- Keep the core business continue to operate.
- Employ/deploy mitigation plans (quarantine/isolation) with one click or even automated.

After the breach

- Understand the impact of the attack
- Execute recovery plans and accelerate recovery to days instead of months
- Have full context not just of the server count but what business functions are impacted with full context of the microsegments
- Recover in short pre-determined phases
- Pull back on isolation of business functions based on impact and criticality.
- Pull back on quarantined microsegments as the affected systems are investigated and restore business processes.

How Colortokens Helps Organizations Be Better Prepared For Breaches

ColorTokens' **Xshield Enterprise Microsegmentation Platform** compliments and extends your cyber strategy with a defense-in-depth approach. It's a foundational part of a Zero Trust Architecture. It goes beyond perimeter firewalls, VLAN segmentation and anti-virus solutions by enforcing micro-perimeters around all your resources, applications, and devices. It prevents malware and ransomware from spreading despite a breach by stopping unauthorized lateral traffic. Xshield makes you breach-ready so you can continue operations despite the inevitable attack.

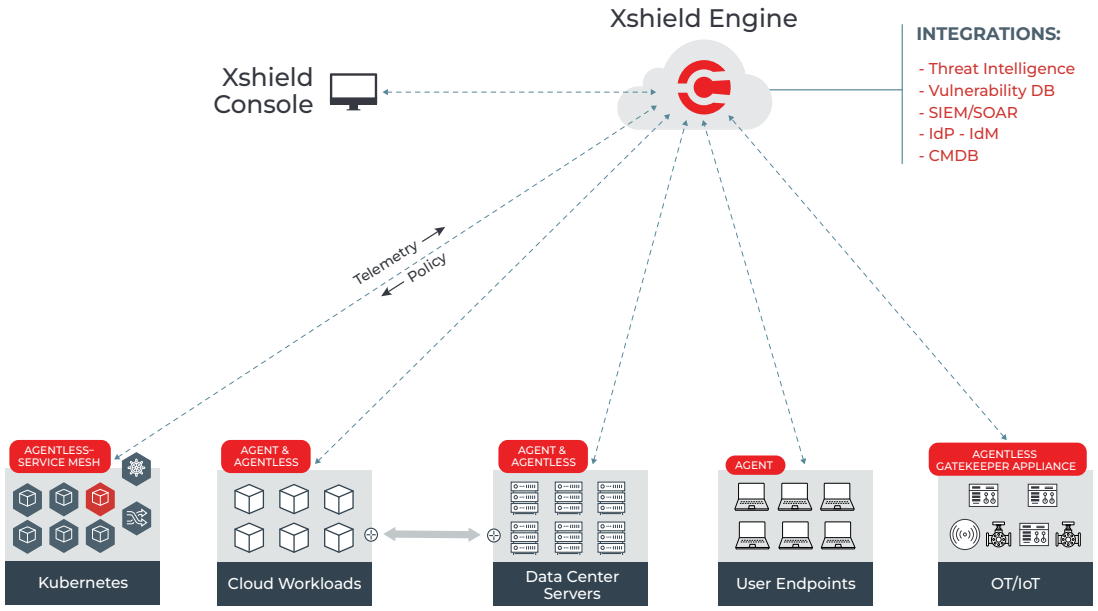
At ColorTokens we have built the only microsegmentation solution designed to help organizations protect themselves at all points of breach so there are no soft spots in your defense. Xshield protects lets you configure and control multiple types of policy enforcement points, both agent-based and agentless, from a unified administration console, reducing complexity and saving on staffing and training. The traffic policies you configure in the Xshield console are automatically expressed in the rules formats required by the different enforcement points. The policy enforcement points that are controlled by the Xshield SaaS-based policy engine include:

For datacenter servers, VMs and user endpoints: the lightweight Xshield agent enforces your traffic policies by configuring the host-based OS firewalls on Windows and Linux computers.

For Kubernetes containers: agentless enforcement using a sidecar proxy leveraging the existing service mesh architecture (such as Istio Envoy).

For IoT and OT devices: the Xshield Gateway Appliance allows you to control traffic to microsegment IoT and OT devices on which no agent can be installed.

For Legacy OS devices: devices in your environment that have out-of-support operating systems, but which are still important to your business processes can be microsegmented in an agentless way using the Xshield Gateway Appliance.



At ColorTokens, we have helped organizations in many sectors, both commercial and public sector; some of whom had already suffered breaches despite large security investments:

- Clinical healthcare and large hospital systems
- State and local governments
- Pharmaceutical manufacturing
- Energy and utilities
- IT and Engineering Services
- US Federal Government

Business continuity with isolation and quarantine

Xshield uses templates to automate responses during a breach to quarantine compromised assets. You can isolate core business assets to ensure critical business processes continue to operate.

Actionable visibility of your enterprise landscape

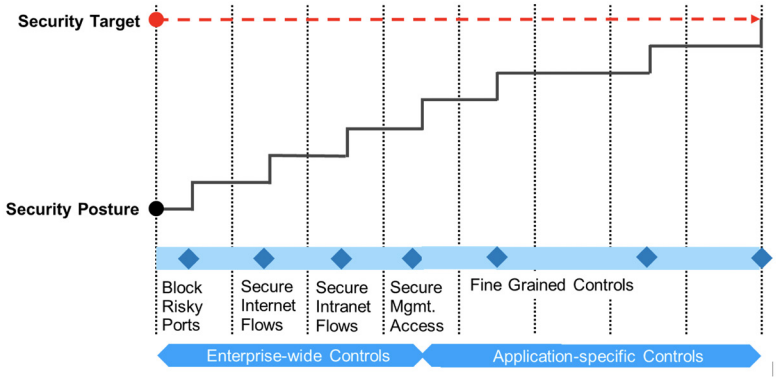
The Xshield visualizer gives you a global, panoptic view across your network landscape, which you can analyze with multiple filters and dimensions, by location, application, criticality, etc. This lets you plan which assets you should segment together, which you should protect with the tightest policies, and which you should identify as key to business continuity in the event of a breach.

Implementation without disruption

Xshield gives you a non-disruptive workflow for implementing microsegmentation. Xshield separates policy authoring from policy push, and lets you simulate policies on historical data before enforcement. You can see the effectiveness of your planned breach response and refine it.

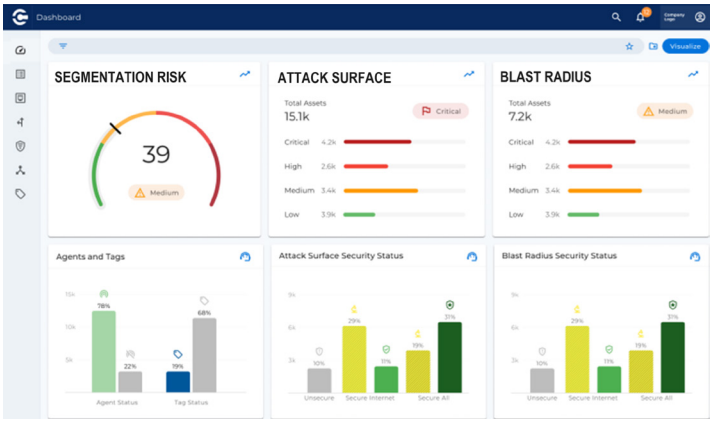
ColorTokens Gives You Measurable Security Increases in Less than 30 Days

ColorTokens quick-starts your security initiative with an innovative approach that immediately improves your security by giving you enterprise-wide controls for risky ports and sensitive flows, then progresses to continuous improvement with application-specific zero-trust controls.



ColorTokens Xshield lets you Visualize and Communicate Security Gains

Xshield's dashboards and reports let you see your security gains and communicate them to your stakeholders, measured by business risk, attack surface, and blast radius. This helps you build consensus for your cyber defense initiative and comply with oversight and regulatory requirements.



Getting Started

To learn more about how ColorTokens can help your enterprise become breach-ready, contact us at +1 844-486-1050 or sales@colortokens.com. We can support your journey to zero trust architecture with:

- A Business Value Assessment of Zero Trust Microsegmentation for your organization
- Software demonstration
- Proof-of-Value engagement

About ColorTokens

ColorTokens is a leader in delivering innovative and award-winning cyber security solutions. It is a US corporation headquartered in Silicon Valley with offices in the US, the UK, Europe, the Middle East, and India serving a diverse client base in both the public and private sector. For more information, please go to **colortokens.com**

APPENDIX—THE ANATOMY OF A BREACH

Attack timeline of the City of Dallas breach in 2023

Intrusion or Recovery Action/Activity	Approximate Date
Likely entry into network	April 07, 2023
Intrusion Surveillance Phase	April 07 – May 03, 2023
Account Credentials First Obtained	April 07 – May 03, 2023
Attack Beacons Installed	April 07 – May 03, 2023
Identification of Possible Attack	May 03, 2023, at 2:54 am
Security Team Begins Analysis	May 03, 2023, at 2:54 am
Likely Lateral Movement through Network Begins	May 03, 2023, at 2:54 am
Attack Mitigation Procedures Initiated	May 03, 2023, at 5:00 am
Bridge Call Opened	May 03, 2023, at 5:23 am
Sanitation Servers Identified as affected	May 03, 2023, at 5:32 am
Set of Servers Identified as Infected	May 03, 2023, at 6:00 am
Team expanded to include additional IT disciplines	May 03, 2023, at 7:00 am
Disaster Recovery Manager Notified of Ongoing Incident	May 03, 2023, at 7:46 am
Citywide Announcement of Widespread Service Outage Made to City Staff	May 03, 2023, at 8:05 am
IT Executive Leadership Notified of Ongoing Incident (CIO, CFO)	May 03, 2023, at 8:22 am
Incident Response Plan (IRP) Initiated	May 03, 2023, at 8:30 am
Communication to Federal Authorities	May 03, 2023, at 8:30 am
City's Office of the City Attorney (CAO) and Office of Emergency Management (OEM) Notified of Ongoing Incident	May 03, 2023, at 8:30 am

Intrusion or Recovery Action/Activity	Approximate Date
Likely entry into network	April 07, 2023
Intrusion Surveillance Phase	April 07 – May 03, 2023
Account Credentials First Obtained	April 07 – May 03, 2023
Attack Beacons Installed	April 07 – May 03, 2023
Identification of Possible Attack	May 03, 2023, at 2:54 am
Security Team Begins Analysis	May 03, 2023, at 2:54 am
Likely Lateral Movement through Network Begins	May 03, 2023, at 2:54 am
Attack Mitigation Procedures Initiated	May 03, 2023, at 5:00 am
Bridge Call Opened	May 03, 2023, at 5:23 am
Sanitation Servers Identified as affected	May 03, 2023, at 5:32 am
Set of Servers Identified as Infected	May 03, 2023, at 6:00 am
Team expanded to include additional IT disciplines	May 03, 2023, at 7:00 am
Disaster Recovery Manager Notified of Ongoing Incident	May 03, 2023, at 7:46 am
Citywide Announcement of Widespread Service Outage Made to City Staff	May 03, 2023, at 8:05 am
IT Executive Leadership Notified of Ongoing Incident (CIO, CFO)	May 03, 2023, at 8:22 am
Incident Response Plan (IRP) Initiated	May 03, 2023, at 8:30 am
Communication to Federal Authorities	May 03, 2023, at 8:30 am
City's Office of the City Attorney (CAO) and Office of Emergency Management (OEM) Notified of Ongoing Incident	May 03, 2023, at 8:30 am

Intrusion or Recovery Action/Activity	Approximate Date
Preservation of Evidence Procedures Initiated	May 03, 2023, at 8:31 am
Notification to City Mayor and Council of Ongoing Incident	May 03, 2023, at 9:05 am
Preservation and Restoration of Public Safety CAD Services Set as a Priority	May 03, 2023, at 9:35 am
Infected Server Inventory Tracking Initiated	May 03, 2023, at 9:44 am
Content of Royal README.txt Message Shared with Incident Team	May 03, 2023, at 9:45 am
Critical Public Safety Servers Infected	May 03, 2023, at 11:10 am
Begin Disconnecting Servers	May 03, 2023, at 11:00 am
Rebuild of CAD Servers Begin	May 03, 2023, at 12:00 pm
News Outlets Announce the Attack to the Public	May 03, 2023, at 12:30 pm
New Servers Become Infected	May 03, 2023, at 1:22 pm
Infected Databases Identified	May 03, 2023, at 1:30 pm
Print Servers Are Disconnected	May 03, 2023, at 2:11 pm
Initial Analysis Determines 173 Servers Are Impacted	May 03, 2023, at 2:15 pm
Multiple Domains Impacted	May 03, 2023, at 2:15 pm
Assessment that Multiple Departments Impacted	May 03, 2023, at 2:15 pm
Server Reinfection Confirmed	May 03, 2023, at 5:00 pm
Additional Blocks by CrowdStrike	May 03, 2023, at 5:30 pm
Confirmation of a Development Services server infected	May 03, 2023, at 6:00 pm
Confirmed Database GIS Servers Infected	May 03, 2023, at 6:09 pm
Malware Execution Extinguished by the City	May 04, 2023, at 5:58 am
Incident Support Team (IST) Activation	May 08, 2023, at 9:00 am
Incident Support Team (IST) De-activation	June 09, 2023, at 5:00 pm

Affected systems

Service/Application	Brief Service Description	Affected City Department
GIS	Enterprise Geographic Information System	DWU, Dallas Police, Dallas Fire-Rescue, Other
Fusion Center	Dallas Police multi-source intelligence fusion solution	Dallas Police
Computer-Aided Dispatch (CAD)	Emergency Services Computer-Aided Dispatch Service	Dallas Police, Dallas Fire-Rescue, Dallas EMS, Dallas Marshals
Report Management Service/Code Compliance Management System	DPD-Web Report Management System (RMS) and Code Compliance Management System (CCMS)	Dallas Police, Code Compliance Services

[6] dallas-ransomware-incident-may-2023-incident-remediation-efforts-and-resolution.pdf (dallascityhall.com)

Service/Application	Brief Service Description	Affected City Departments
Public Safety File Shares	Remote data stores (server-based, cloud-based) for individual and group use	Dallas Police
Surveillance Cameras Management System	Street cameras used for Police surveillance of a venue (e.g., Fair Park) or of a location (e.g., Starlight program)	Dallas Police
Animal Management Services	Animal and animal support monitoring, system management solution	Dallas Animal Shelter
Building Permitting System	Building Inspection plan and permitting management solution	Development Services
Secure File Transfer Service	Secure file transfer protocol server physically present within the City Data Center	Information & Technology Services (ITS), all other City departments
Library Management Service	Dallas Library book, media, and artifact management solution	Dallas Library
Warrants Management Service	Court ordered warrant management solution	Dallas Police, Dallas Marshals, Dallas Municipal Courts, other local agencies interoperating with City warrant resources.
Remote Water Meter Reading Service	Remote water meter reading technology supporting Dallas Water Utilities billing and operations divisions	Dallas Water Utilities
Payment Card Acceptance Solution	Payment card acceptance services supporting Dallas Water Utilities Billing solution operations.	Dallas Water Utilities, other departments using ePay for payment acceptance.
Public Safety Mobile Data Computer Services	Mobile Data Computer (MDC) predominately used by polices, fire, Emergency Medical Services (EMS), and emergency services for remote digital communications between deployed assets and between deployed assets and City Computer-Aided Dispatch Services.	Dallas Police, Dallas Fire-Rescue, Dallas EMS, Dallas Emergency Services, and other City departments and agencies using Mobile Data Computer for the capture and presentation of service information.
Alerting Service	Fire Station Alerting solutions designed to reduce response times and improve first responders' quality of life.	Dallas Fire-Rescue
Secure Print Services	Citywide secure print services used to monitor and manage print of secure documents at designated print stations.	All departments.
Fax Services	These applications and systems securely transmit paperless, digital faxes. This digital faxing solution greatly reduces the faxing costs by connecting to onsite analog or	All departments.

Recovery phases

Date Restored	Restoration Phase	Color Status	Application/Service
5/5/2023	Phase 1	Green	Computer Aided Dispatch
5/8/2023			Incident Support Team Activated
5/9/2023	Phase 1	Green	Financial Server
5/9/2023	Phase 1	Green	City Website
5/9/2023	Phase 1	Green	Development Service System
5/10/2023	Phase 1	Green	Police/Fire Automated Dispatch
5/11/2023	Phase 2	Green	City Controller System
5/11/2023	Phase 1	Green	Payment Card Acceptance Solution
5/11/2023	Phase 2	Green	Warrants Management Service
5/11/2023	Phase 1	Green	Cyber Security Server
5/11/2023	Phase 1	Green	Remote Meter Reading Service
5/12/2023	Phase 1	Green	Records Management System
5/15/2023	Phase 2	Green	Dallas Police Crime System
5/15/2023	Phase 2	Green	Code Management Service
5/15/2023	Phase 1	Green	Field Base Reporting Service
5/15/2023	Phase 1	Green	Citizen Request Management Service
5/16/2023	Phase 3	Green	Dallas Police Crimes Server
5/16/2023	Phase 2	Green	Animal Management Service
5/16/2023	Phase 3	Green	Financial Management Service
5/16/2023	Phase 2	Green	Dallas Fire Rescue System
5/17/2023	Phase 4	Green	Application and Data Workflow Orchestration
5/17/2023	Phase 2	Green	City Secretary System
5/17/2023	Phase 2	Green	Sanitation System
5/19/2023	Phase 4	Yellow	Virtual Viewer
5/22/2023	Phase 5	Green	Dallas Police Narcotic System
5/22/2023	Phase 4	Green	Dallas Fire Rescue Incident System
5/22/2023	Phase 4	Green	City Attorney System
5/22/2023	Phase 5	Green	Evidence Management Service
5/22/2023	Phase 5	Green	Dallas Police Safety Servers
5/22/2023	Phase 2	Green	Dallas Fire Rescue Safety Servers

Date Restored	Restoration Phase	Color Status	Application/Service
5/22/2023	Phase 5	Green	Dallas Police System
5/22/2023	Phase 4	Green	Virtual Viewer Service
5/23/2023	Phase 4	Green	Print Server
5/24/2023	Phase 2	Green	Financial Service Reporting Service
5/24/2023	Phase 5	Green	Merchant Accounting Software
5/25/2023	Phase 4	Green	Life Event Certificate Management Service
5/25/2023	Phase 4	Green	GIS Water Server
5/26/2023	Phase 1	Green	Court Management System
5/26/2023	Phase 3	Green	Dallas Police Enhanced Neighborhood System
5/30/2023	Phase 5	Green	Payment Management System
5/30/2023	Phase 5	Green	Dallas Police Specialized Server
5/30/2023	Phase 3	Green	Dallas Police Impound System
5/30/2023	Phase 3	Green	Internal Workflow Management Service
5/31/2023	Phase 5	Green	Vital Statistics
6/2/2023	Phase 3	Green	Court Docket Management System
6/2/2023	Phase 5	Green	Dallas Fire Specialized Server
6/2/2023	Phase 4	Green	Dallas Police Warrants System
6/6/2023	Phase 6	Green	Employee Management System
6/6/2023	Phase 6	Green	Survey Management Service
6/8/2023	Phase 5	Green	Dallas Police Traffic Data System
6/8/2023	Phase 5	Green	Vehicle Management Safety Report System
6/13/2023	Phase 6	Green	Back-Up Site Servers
6/13/2023	Phase 6	Green	Dallas Water Billing Payment File Service
6/13/2023	Phase 6	Green	Street Maintenance and Repair Management Service
6/13/2023	Phase 6	White	Financial Services Management Service
6/13/2023	Phase 4	Yellow	File Share Resources
6/13/2023	Phase 6	Green	GED Testing Management Service
6/13/2023	Phase 3	Yellow	Dallas Fire Rescue Personnel Server
6/13/2023	Phase 3	White	Library System
6/13/2023	Phase 2	Yellow	Library Resource Reservation Service
6/13/2023	Phase 4	Yellow	Building Services Server
6/13/2023	Phase 6	Yellow	Library Resource Reservation Service
6/13/2023	Phase 2	Yellow	Library Resource Management Service
6/13/2023	Phase 5	Yellow	Dallas Fire Rescue Case Entry System
6/13/2023	Phase 5	White	Public Safety Back-up Site Server
6/13/2023	Phase 6	Yellow	Security Gate Server
6/13/2023	Phase 4	Yellow	Stormwater Management Service
6/13/2023	Phase 6	Yellow	Development Services System
6/13/2023	Phase 6	Green	Waste Management Server