# How to Take Cyber Defense Beyond Breach Prevention

govloop

COLORTOKENS

# Introduction

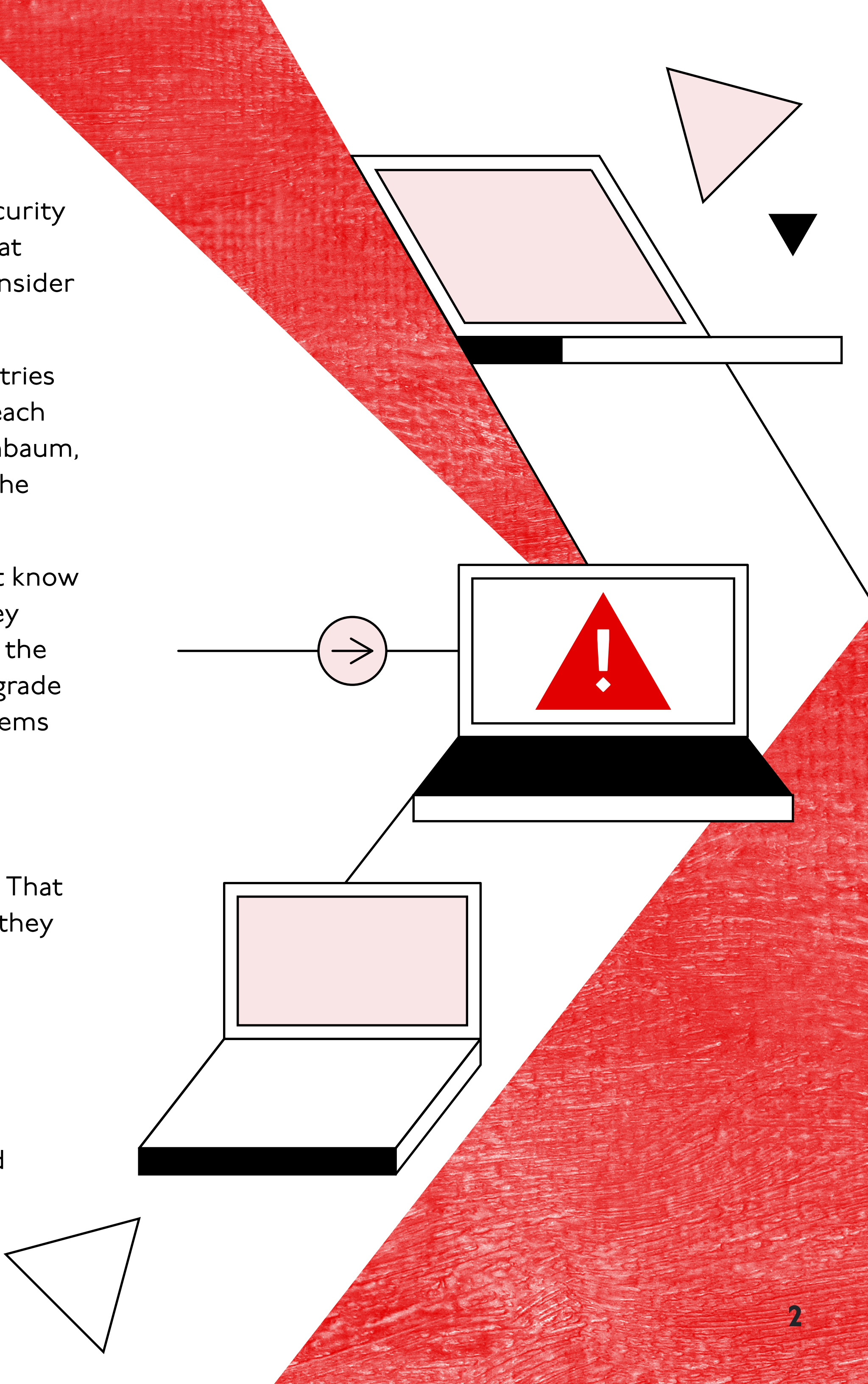
By and large, government agencies invest most of their cybersecurity budgets in trying to prevent breaches. That's important. But what happens when someone beats those defenses? It's crucial to consider because it's bound to happen.

"When the attacker only has to be right once out of thousands of tries while the defender has to be right every single time, an initial breach of the perimeter defenses becomes inevitable," said Louis Eichenbaum, Federal CTO, ColorTokens and former CISO, US Department of the Interior. And when that happens, real damage can be done.

"When an adversary gains that initial compromise, they don't yet know where your valuable assets are in the network landscape, so they have to move laterally to find them," he said. "Once they locate the high-value resources, they can then exfiltrate sensitive data, degrade the performance of critical operational systems or encrypt systems for ransom."

Key to stopping that lateral hunt is microsegmentation. It's a cybersecurity approach that involves creating isolated network segments that allow for granular traffic monitoring and control. That makes it harder for intruders to move within the network once they breach the perimeter.

The approach aligns with the MITRE ATT&CK framework, which identifies lateral movement attacks as a common threat. For government IT teams, microsegmentation supports zero-trust mandates such as the National Institute of Standards and Technology's Zero Trust Architecture and the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model.



# Need to Know

## Microsegmentation: A Foundation for Zero Trust

Agencies operate in a contested cyber environment where maintaining security is critical. A core principle of zero trust is to assume that a breach will occur — **and to be prepared to withstand it**. Although perimeter defenses remain important, organizations must also strengthen their internal network defenses.

That's where microsegmentation offers the resilience agencies need to sustain mission operations — even if the network perimeter is compromised.

Specifically, microsegmentation prevents cyberattacks from moving within network segments, ensuring that a breach of perimeter defenses does not lead to a critical degradation of operational capabilities.

## 18%

Amount of organizations planning to build microsegmentation within the next year.

## 25%

Amount of enterprises working toward a zero-trust architecture that will use more than one deployment form of microsegmentation by 2027, up from less than 5% in 2025.

## Key Resources Informing Zero-Trust Enforcement

Two key resources can help inform an effective approach to enforcing zero trust.

- The MITRE ATT&CK framework provides a detailed list of tactics, techniques and procedures that malicious actors use to gain entry and then move laterally.
- CISA maintains a dynamic database of current cyber threats, providing organizations with cyber situational awareness.

A robust microsegmentation strategy can use these two resources to anticipate adversaries' tactics and stop them from moving freely within the enterprise environment.

## The Microsegmentation Mandate

Here are some polices in which microsegmentation plays a critical role:

- The War Department's Zero Trust Strategy calls for reducing attack surface risk profiles by taking protective actions enabled by microsegmentation within the DoW Information Enterprise.
- NIST's "Guide to a Secure Enterprise Network Landscape" calls for microsegmentation in support of zero trust, and its Zero Trust Architecture highlights microsegmentation as a key strategy.
- CISA includes microsegmentation as part of the network pillar of its Zero Trust Maturity Model, but notes that the strategy involves numerous mechanisms beyond the network. The agency recently published guidance on planning a transition to microsegmentation.

## 50%–80%

Amount that microsegmentation reduces an attack surface and blast radius.

# How to Stop Intruders in Their Tracks

Agencies can leverage zero-trust microsegmentation as they shift from a posture of breach prevention to breach readiness, in which defenders assume breaches are possible and are prepared to limit their damage. Some key best practices will support that effort.

## Look for Soft Spots in Your Defenses

With microsegmentation, traffic is easier to monitor and control because the network is divided into isolated parts. Securing each enhances both protection and simplicity, with defenses that adapt to dynamic application environments.

To bring that strategy to life, start by identifying weaknesses in your current plan. This will help guide a fundamental rethinking of your security approach. “You are changing the security posture of the organization in advance of a breach so that lateral movement of the attacker becomes very difficult,” Eichenbaum said.

As you work to shore up those vulnerabilities, take a systemic approach. One key principle is that microsegmentation must be pervasive. This means agencies must apply microsegmentation to IT and operational technology networks, plus resources deployed in data centers and the cloud. What’s more, a comprehensive approach will integrate automatic updates based on CISA’s advisories and the MITRE framework’s Lateral Movement knowledge base, which focuses on preventing adversarial efforts to move through multiple systems and accounts.

“With a pervasive approach to microsegmentation, you can be assured that all possible points of breach are covered in the environment,” Eichenbaum said. “It doesn’t matter if you lock your gate if the gate isn’t connected to a continuous fence. The hackers will just walk around it.”

## Track Breach-Readiness Metrics

Measuring the effectiveness of any cybersecurity strategy is essential. As IT teams adopt microsegmentation, two key metrics can help assess their readiness to handle breaches: attack surface and blast radius.

These terms originate from kinetic warfare. In that context, the attack surface refers to the number of network resources exposed to incoming lateral traffic, and blast radius refers to the number of outgoing connections from a given resource, indicating how far an attack could spread if that resource is compromised.

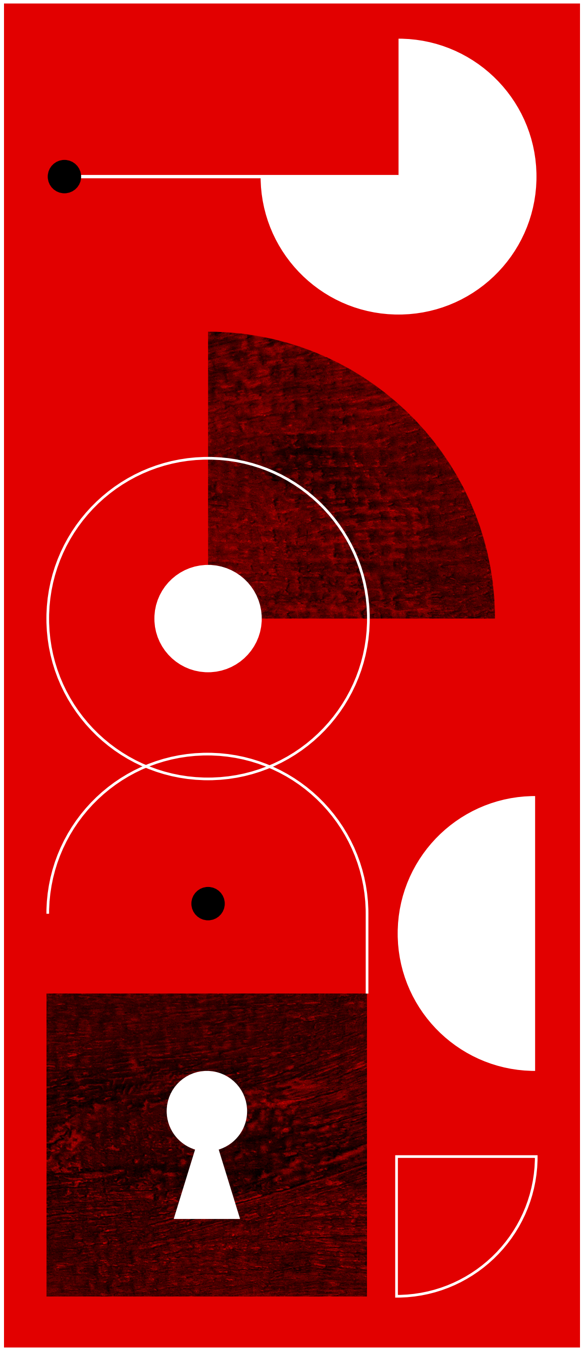
"By controlling traffic through zero-trust microsegmentation policies, we can significantly reduce both the attack surface and the blast radius available to the adversary," Eichenbaum said.

Historically, agencies haven't closely monitored these metrics because the primary focus has been on securing the perimeter against breaches. With the shift toward breach readiness, security and network infrastructure leaders must understand both the blast radius and attack surface to better assess their risk, Eichenbaum said.

Before zero-trust microsegmentation, IT teams often relied on macrosegmentation at the virtual local-area network (VLAN) level — a method that logically groups network devices so they behave as if they're on the same physical network even when they're not. "That was the primary state of the practice, and there was little to no knowledge or control over lateral movement within the large segments of the VLAN," he said.

"Microsegmentation allows you to see things granularly, right at the workload level," Eichenbaum said. "These detailed metrics empower you to block unauthorized traffic while allowing valid business processes to proceed."

By tracking these metrics, defenders gain valuable insight, and they need to take full advantage of it. "Without understanding those metrics, you really don't fully grasp the potential impact on government operations," he said. Chief information officers, "chief information security officers, and security and risk leaders all need to understand the blast radius and attack surface available to the adversary in order to assess the overall risk to their digital operations."



## Focus on Progressive Enforcement

Progressive enforcement is a microsegmentation technique of rolling out protections based on vulnerability. It enables defenders to rapidly reduce both the attack surface and blast radius, making it a key defensive strategy.

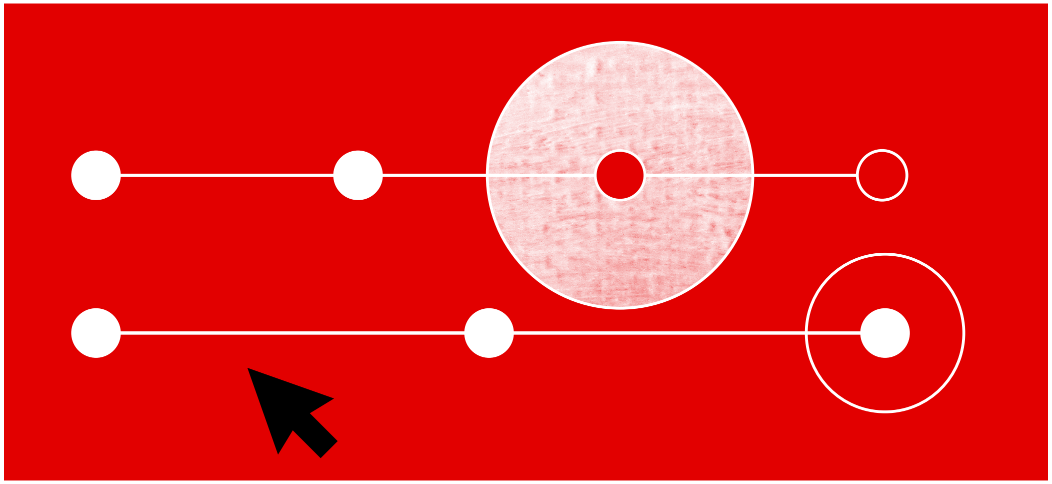
"It starts at the enterprisewide level, applying controls to the most commonly exploited ports on every asset and resource in the network — those most frequently targeted by attackers," Eichenbaum said.

From there, it controls restricted privilege access for management services — specifically, the management ports. Finally, it extends to infrastructure ports, limiting access to only the valid business processes necessary within the enterprise environment.

As the name suggests, "it…progresses to cover all inactive ports among the thousands available," he said. "You might be shocked to learn that in many enterprises, ports that have never been used for valid business communications are left open. That's an available attack surface that must be closed."

By strategically rolling out enforcement, "we can progressively tighten the network landscape to severely limit the adversary's ability to carry out a lateral movement attack," Eichenbaum added.

As IT teams implement this approach, "the final step is to institute application-specific policies for enterprise applications," he said. "Once all those progressive steps are completed, you've successfully locked down your environment. It makes the hacker's job very, very difficult."



## Conduct Deep Policy-Impact Analysis

The implementation of zero-trust microsegmentation must be nondisruptive. In a successful microsegmentation project, defenders need to block adversarial actions, "but you still have to allow all the valid business processes of the organization to proceed," Eichenbaum said.

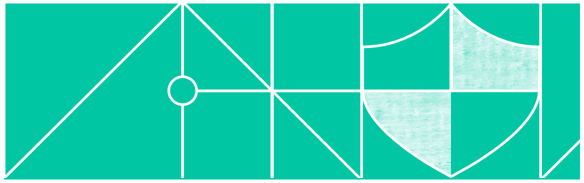
This means having the right policies in place — and executing them correctly — so business operations aren't interrupted. A deep policy impact analysis ensures everything is functioning as intended.

You can do that in two ways: through simulation and testing, Eichenbaum said. "Simulation uses historical traffic data to analyze the potential impact of your policies, ensuring they won't disrupt valid business processes," he said. "On-device testing, meanwhile, uses actual, current traffic in a non-enforcement mode. That lets you see what the effect of those policies would be if enforcement were active."

By conducting both simulation and testing, defenders can be confident they're effectively blocking adversarial actions without affecting mission-critical business processes. This analysis ensures that policies provide strong protection without being overly restrictive or interrupting the flow of work.

# Microsegmentation: Government Use Cases

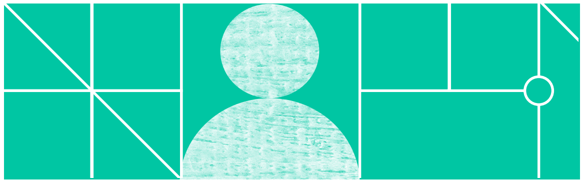
It's helpful to look at how microsegmentation would impact key government sectors: defense, civilian and healthcare agencies.



## Defense

In defense, "net-centric warfare means the network landscape is actually an area of operation — it's a battlespace. And in digital operations, just like in kinetic warfare, you have to be able to carry out your mission even with the adversary present in that battlespace," Eichenbaum said.

A core principle of zero trust is that agencies should assume a breach has already occurred and that they still can operate effectively. That's where microsegmentation plays a critical role in the defense space. "It allows you to maintain information superiority over the adversary in a net-centric warfare environment, even if the adversary has breached the perimeter defenses — and they probably have," he said.

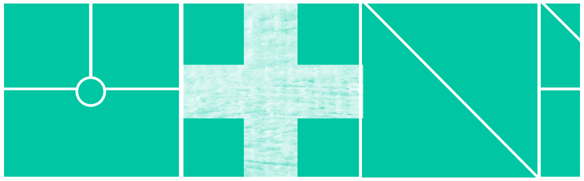


## Civilian

In federal civilian agencies, "you want to protect your crown jewel applications, the ones that contain sensitive constituent data," Eichenbaum said.

He points to the 2015 Office of Personnel Management data breach as a classic example of the risks civilian agencies face. In that incident, hackers exfiltrated from OPM systems confidential information on government contractors with secret clearance or higher.

"All of that sensitive constituent information must be kept secure," Eichenbaum said. Microsegmentation helps ensure that even if hackers breach perimeter defenses, the impact of their exploits is contained.



## Healthcare

Two key use cases stand out in government healthcare agencies. The first involves internet-connected medical devices, such as smart infusion pumps, ventilators, imaging systems and cardiac telemetry devices — often referred to as Internet of Medical Things devices. "Veterans [Health] Administration hospitals have tens of thousands of these devices, as do TRICARE medical facilities and the military hospital system," Eichenbaum said. "All of these are connected to the network, and each one can be a potential vector of attack."

In addition, these agencies must protect the vast stores of patient data housed in their electronic health records systems. "If those systems are compromised, it harms continuity of care because medical providers and nurses can't access patient data," he said.

For both biomedical devices and EHR systems, microsegmentation is key to achieving effective breach readiness.

SOLUTION SPOTLIGHT

# The Evolution of Microsegmentation

Although the concept of microsegmentation has been around for a long time, it has evolved as cyber adversaries and defenses have grown more sophisticated.

"We've gone through multiple generations of microsegmentation, with new methods and techniques to stay one step ahead of these attackers," Eichenbaum said.

First-generation macrosegmentation delivered minimal security benefits; exploits could still compromise entire VLAN segments. Implementation often took months or even years. Second-generation software-defined microsegmentation solutions brought incremental improvements, but still required time-consuming, app-by-app policy definitions.

Today's generation of microsegmentation offers progressive enforcement with enterprisewide policies and breach isolation templates. Implementation now takes just hours or days. With faster deployment and stronger, more adaptive policies, modern solutions effectively stop lateral movement, supporting true breach readiness.

Breach readiness "can give leaders the peace of mind of knowing that they're prepared for the inevitable, and that they can continue to pursue their mission and serve their constituents despite the aggressive cyber landscape we're in," Eichenbaum said.

In addition, as noted earlier, microsegmentation is vital for federal agencies operating under a variety of zero-trust mandates. It aligns with and supports the policies and requirements imposed by NIST guidelines, CISA mandates, executive orders and other guiding documents.

## Bringing It to Life

Several key differentiators define ColorTokens' approach to microsegmentation. The first is fast, frictionless implementation. ColorTokens integrates seamlessly with an agency's existing endpoint detection and response solutions, enabling rapid microsegmentation without the need to deploy additional agents. As a result, "we can achieve a 50 [percent] to 80 percent reduction in cyber risk in 90 days or less," Eichenbaum said.

Another differentiator is flexible, multidimensional visualization of network assets and traffic. "With a network-map view of every asset and its connections, teams can focus on what's most relevant to their roles," he said.

As a next-gen solution, ColorTokens integrates seamlessly with existing tools. For instance, it works with security information and event management; security orchestration, automation and response; and endpoint detection and response systems. "When an indication of compromise occurs, we can immediately isolate your critical business systems," Eichenbaum said.

ColorTokens also delivers dashboards and printable reports. That's important in government, which has a high bar for accountability. "You can measure and share the improvement in your security posture with your stakeholders, with leadership, with regulatory authorities," Eichenbaum said.

Finally, ColorTokens takes a pervasive approach, delivering protection for all asset types — whether it's IT, the Internet of Things or operational technology, both in the data center and in the cloud, he said.

# Conclusion

In government, most cybersecurity spending focuses on breach prevention, but recent high-profile attacks have shown that even significant investment doesn't guarantee safety. Leaders must pivot toward breach readiness, which means assuming a breach will occur and being prepared to stop lateral movement so that an incursion doesn't escalate into a crisis.

COLORTOKENS

## About ColorTokens

ColorTokens is a recognized leader in delivering innovative and award-winning zero-trust cybersecurity solutions. A US corporation headquartered in Silicon Valley with offices in the United States, the United Kingdom, Europe, Australia, and India, ColorTokens serves a diverse client base in both the public and private sectors. Our customers span multiple industries including healthcare, manufacturing, defense, financial services and critical infrastructure.

Learn more: colortokens.com

govloop

## About GovLoop

GovLoop's mission is to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop