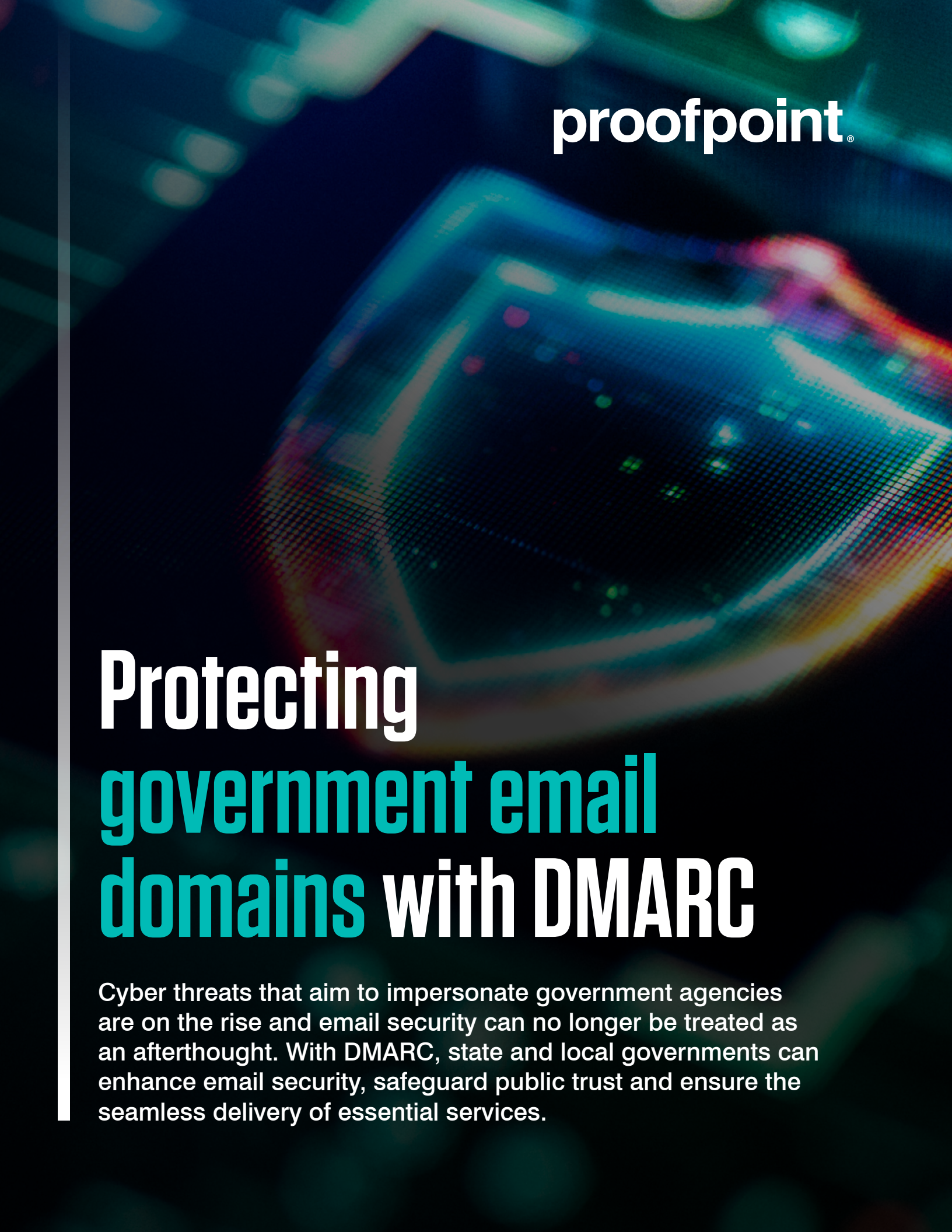

proofpoint®

Protecting government email domains with DMARC

Cyber threats that aim to impersonate government agencies are on the rise and email security can no longer be treated as an afterthought. With DMARC, state and local governments can enhance email security, safeguard public trust and ensure the seamless delivery of essential services.

State and local governments play crucial roles in delivering essential services to millions of residents. Whether they are processing driver's license renewals or distributing healthcare benefits, agencies rely heavily on email for communication. However, the rapid evolution of cyber threats such as phishing and email spoofing has made email security a top priority.

"Email was never designed with security in mind," said Ash Valeski, senior director of product management at Proofpoint. This makes it easy for malicious actors to spoof government domains and deceive both citizens and civil servants. The consequences of email fraud are severe. These can include financial loss, identity theft, unauthorized access to sensitive government data and a loss of public trust in government agencies.

Recognizing this growing threat, major email providers such as Google and Yahoo have begun to enforce authentication requirements for bulk senders – defined as entities that send more than 5,000 emails per day. The requirements include mandatory Domain-based Message Authentication, Reporting and Conformance (DMARC) policies, one-click unsubscribe functionality for marketing emails and strict thresholds for spam complaint rates.

For government agencies, these changes mean that email providers might flag non-compliant emails as spam or block them entirely, disrupting crucial services. To maintain uninterrupted communication with the public, a government agency that sends high volumes of emails — such as tax notifications, unemployment benefit updates or public health alerts — must ensure that their email infrastructure meets these new security standards.

> "The receiving community is basically saying, 'No more games.' It's time for senders to adhere to the standards and guidelines that have been provided for many years."
>
> **Ash Valeski**
> Senior Director, Product Management, Proofpoint

"The receiving community is basically saying, 'No more games.' It's time for senders to adhere to the standards and guidelines that have been provided for many years," Valeski said.

By adopting DMARC, state and local governments can enhance email security and ensure the seamless delivery of essential services. However, the implementation process can be challenging, particularly for agencies with complex email infrastructures. That's where Proofpoint comes in. Proofpoint provides a streamlined, expert-driven approach to DMARC deployment, enabling government entities to secure their domains with confidence.

THE RISKS OF EMAIL DISRUPTIONS IN GOVERNMENT

Failure to properly authenticate emails can have serious consequences for government functions. When email providers block or mark legitimate government emails as spam, citizens might miss deadlines, lose access to vital services or remain uninformed during emergencies. Essential services that rely on email communication include:

- **Tax refund notifications** – Tax agencies send millions of emails annually to inform citizens about refund statuses, filing deadlines and payment obligations. An email disruption could delay financial transactions, causing frustration to taxpayers.
- **Unemployment benefits and social service updates** – Millions of residents rely on government-issued benefits. Email is a primary way to communicate eligibility updates, payment notifications and program changes.
- **License renewal reminders** – Government agencies send routine reminders for renewals of driver's licenses, fishing and hunting permits, business registrations and other credentials. Without proper authentication, these reminders might never reach recipients, leading to compliance issues and service lapses.

Large states with complex government infrastructure face additional challenges. For example, some states have over 150 government subdomains, each potentially sending thousands of emails per day, said Charles Grindle, Proofpoint public sector executive advisor and former CIO of the Commonwealth of Kentucky.

Each subdomain might be controlled by different agencies with varying levels of IT resources and security expertise. This makes it difficult to enforce consistent email authentication policies. Without a centralized approach to DMARC implementation, government entities risk having gaps in their email security postures that cybercriminals can exploit. Aligning all subdomains with the same authentication standards is critical to preventing fraud and maintaining uninterrupted communication with the public.

"There's a huge impact on social services as well," Valeski said. "Think about emergency health services — critical communications that must reliably reach the community. If those emails aren't delivered, the consequences could be severe."

STRENGTHEN EMAIL SECURITY AND VISIBILITY

DMARC provides a structured framework to authenticate email senders and prevent domain spoofing. The protocol uses two existing authentication mechanisms: Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). If an email fails authentication, the recipient's email server can take one of three actions, as defined by the sender's DMARC policy:

- **Monitor** – The system allows emails through but generates detailed reports of email authentication activity.
- **Quarantine** – The system sends suspicious emails to the recipient's spam folder, reducing the recipient's exposure to phishing attempts.
- **Reject** – The system blocks unauthorized emails entirely, preventing them from reaching recipients.

Beyond security, DMARC also offers increased visibility of an organization's email-sending activities. When properly configured, DMARC ensures that only authorized IP addresses can send emails on behalf of a domain, effectively blocking unauthorized senders. Additionally, DMARC reports provide detailed insights into all email sources. These insights enable government agencies to detect vulnerabilities and take proactive steps to secure their email ecosystems.

"DMARC reports shine a light on all the sources of email sending on behalf of a domain," Valeski said. "This is often eye opening for domain owners."

DMARC IMPLEMENTATION SIMPLIFIED

DMARC is essential for securing government email communications. But it comes with challenges, especially for large agencies that manage multiple departments, subdomains and third-party email services.

"DMARC reports shine a light on all the sources of email sending on behalf of a domain. This is often eye opening for domain owners."

Ash Valeski
Senior Director, Product Management, Proofpoint

> State governments want to hold their cards close, but this is one of those things you need to get right the first time."
>
> **Charles Grindle**
> Public Sector Executive Advisor, Proofpoint

"Managing DMARC at the state or city level isn't simple," Grindle noted. "In Kentucky, we had 2,400 applications capable of sending email. You have to identify them all, determine how they send email and update DMARC records accordingly. That's where it gets exponentially complicated."

Securing email isn't a one-and-done task — DMARC requires ongoing monitoring to keep up with new services, evolving cyber threats and changes to authentication protocols. But government IT teams operate with tight budgets and small staffs that have limited bandwidth. These factors make it difficult for them to deploy and maintain DMARC on their own.

"State governments want to hold their cards close, but this is one of those things you need to get right the first time," Grindle said. "This is not something you can afford to trial-and-error your way through."

With automation, expert guidance and real-time monitoring, Proofpoint simplifies DMARC implementation, minimizing operational disruption while maximizing security.

According to Valeski, the automated sender identification feature from Proofpoint associates otherwise-cryptic IP addresses in DMARC records with clear, recognizable sending entities. This helps agencies to quickly verify legitimate senders and ultimately block unauthorized email activity before it becomes a problem.

"It's not just about knowing who's sending email as you — it's equally about teasing out who should and shouldn't be doing it. And then, among those who should, understanding exactly what needs to be done to get their emails to pass DMARC," Valeski said.

Proofpoint guides IT teams through SPF, DKIM and DMARC setup to prevent misconfigurations and ensure secure email authentication with expert support for troubleshooting and policy management. With a user-friendly monitoring dashboard, agencies get real-time insights into email authentication. This makes it easy to track compliance and spot potential problems before they escalate.

"When dealing with government communication, you do not have time to swing and miss," said Grindle. "You need an expert who gets it right the first time, because getting it wrong means critical messages may never reach the public."

Click to learn more about how Proofpoint is helping state and local governments secure their email infrastructure.