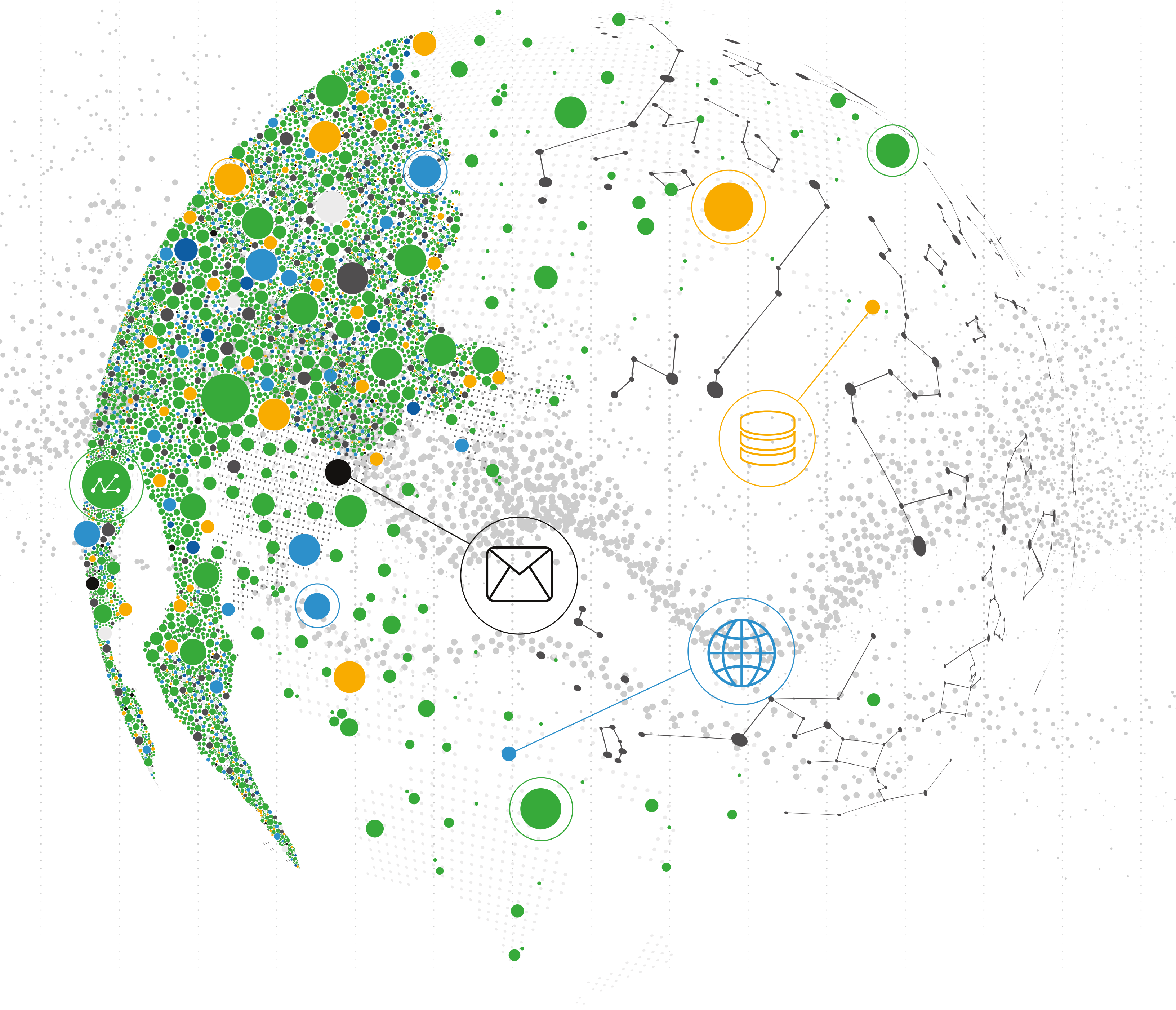
FORCEPOINT

POWERED BY Raytheon

Whitepaper

The Need for Unified Content Security



Contents

INTRODUCTION

Content is the crown jewel of your organization — your messages, images, text, data, and entire documents are the fuel that keeps any business, agency or government moving forward. Sound unlikely? Well, it's absolutely true.

Content, in all its forms, is quite similar to a capital infusion in an organization: when used wisely, its value is multiplied; when used foolishly, its value is diminished. Secure, high quality content is a key ingredient to any healthy bottom line. But if you don't leverage it effectively, you run the risk of being overtaken by those that make more out of it than you do. To stay ahead of your competitors, you must not only permit constructive sharing of your content, but also encourage — as much as possible — other ways to obtain, create, manipulate and disseminate content to help increase its value.

Still, maximizing your content use doesn't give you a license for reckless behavior. That's why you need effective security controls to balance between enabling greater business value and the risks associated with increased exposure of sensitive information. Striking that balance is the key to success, but is easier said than done.

IT teams must determine which specific controls can reduce risks to content, and then find an affordable means to deploy them in all required locations. In this regard, legacy point product approaches to security do more harm than good. They're challenging to maintain, drive up costs and complexity and may even increase the risk of data breaches. The reason is that point products are no match for determined adversaries launching increasingly sophisticated threats to your data, even as you're adopting mobile, Cloud and other new technologies to transform your IT and the way you do business.

Rather than fight that losing point product battle, adopt a unified content security solution that:

- Combines Web, email and data security in a single, integrated and consolidated offering to simultaneously and synergistically prevent sophisticated inbound internet threats, granularly control access to content resources, ensure productivity, and effectively stop outbound data loss across key channels of information exchange.
- Combines on-premises and cloud-based deployment options that are functionally equivalent and seamlessly manageable, giving you maximum use-case coverage and globally consistent policy enforcement, while also reducing the complexity, cost and user confusion that comes from having multiple, disparate "solutions" and modes of operation.

A truly unified content security solution overcomes all of the shortcomings of traditional point product approaches and gives you a much more practical way to effectively and efficiently address your steadily growing content security needs.

As Part 1 of a three-part series, this paper examines the business and technology conditions that have led to the need for unified content security. It also includes a high-level, functional description and summary of the benefits of unifying your content security.

Part 2 explores the technical requirements for a content security solution to be truly unified. Detailed insight is also provided on what a unified architecture is, including the need for unified content analysis, a unified platform and unified management.

Part 3 concludes coverage of this crucial topic by introducing Forcepoint™ TRITON® — the security industry's first and only unified content security solution. This is followed by a comprehensive treatment of the benefits of unified content security, identification of guidelines and recommended practices to help maximize available gains, and real-world examples of organizations using TRITON to successfully conquer their content security challenges.

WHY CONTENT SECURITY MATTERS

At its core, content security is a business-driven requirement. It's also one that is growing in importance.

Content is King

For our purposes, content is the object of our transactions, as opposed to the originator, recipient, means or application. More concretely, content is the message itself — e.g., in the case of email. It's also the individual elements of data, such as a Tax ID or credit card number, as well as discrete collections of data in the form of documents, Web pages, VoIP conversations or video clips.

Additional content characteristics that are important to understand include the following:

▸ *Content is an Enterprise Asset.* Content is far more than just the "fluffy stuff" of the Internet. Besides YouTube videos and Facebook status updates, it's the data and electronic information that facilitates and automates essential business processes and therefore, is the lifeblood of modern organizations.

▸ *The Value of Content is Often Derived by its Use.* With few exceptions — such as trade secrets and sensitive customer information — the more content is used and the more context that is created around it, the greater its value. In this regard, mobile, cloud and social networking applications represent tremendous opportunities for value enhancement.

▸ *Not All Content is Good.* Content in communications can involve more than the information intended by the originator. In particular, content can also include malware and other types of threats that take advantage of weaknesses in the communication mechanisms used for delivery or that hitch a ride with the data itself.

Content is at Risk

Not only does content pose a risk to your organization due to the potential of conveying embedded threats, it's also at risk. Moreover, the level of this risk is rising as all components of the classical risk equation are being driven up.

As noted, content is steadily increasing in value as enterprises explore additional ways to create, centrally mine/analyze, consume and communicate it. In turn, putting content "out there" increases its degree of exposure, rendering it more susceptible to misuse and other forms of compromise. Finally, having greater value also makes content a more attractive target, a characteristic that naturally leads to the generation of more threats intended to capture or otherwise exploit it.

↑THREAT * ↑VULNERABILITY * ↑VALUE = ↑INHERENT RISK

Saying "No" is Not an Option

One consequence of the conditions described in the preceding sections is that your organization is faced with a conundrum: the most effective way to limit the risks posed by and to content — scrupulously sequestering and controlling access to it — conflicts with the objective of generating value for the business.

As any IT professional worth their salt will tell you, just saying "no" to the business interest is simply not an option. Equally problematic are controls that are too restrictive or too cumbersome to use. In that case, users are likely to seek out workarounds that bypass existing security measures, thereby rendering them ineffective.

This is where content security comes into the picture and why it has become a strategic business issue. An effective content security solution is precisely what organizations need to maintain a reasonable balance between the benefits and risks associated with increased information sharing and collaboration. In other words, it's what enables IT to say "yes" when requests are made to allow access to innovative sites, applications, services and technologies that facilitate the consumption, creation and communication of content, and thereby help the business gain a competitive advantage.

THE CONTENT SECURITY CHALLENGE

An effective content security solution involves a combination of both business and technology requirements. Critical criteria include being able to stop advanced threats plaguing the most popular (and useful) communication channels, providing consistent protection across the full range of on-premises, cloud, and mobile use cases, and requiring fewer resources to get the job done. This is especially helpful as the scope of the content security problem continues to steadily expand.

Stopping Advanced Threats

The Dynamic, Dangerous Web. A common tactic for threat actors is to use sites that are short-lived (e.g., that are on the Web for less than one day) to facilitate their attacks. Because these sites are "new and unknown," they're able to evade commonly deployed security solutions. Add to this not only the proliferation of sites and services that support the dynamic creation of new content, but also the frequency with which legitimate web sites are falling victim to drive-by download and watering-hole attacks, and it becomes crystal clear that traditional content and Web security technologies that rely solely on periodic scanning and classification are no longer adequate. Real-time inspection and classification — ideally complemented by real-time threat intelligence — are now essential capabilities.

Email and the Curse of the Blended Threat. Email remains a primary threat vector. After all, it's a core component of phishing scams — the starting point for the vast majority of targeted attacks executed against today's organizations. Treating email as a standalone problem, however, is a mistake. Many threats feature a combination of both email and Web elements, often operating in a closely coordinated manner. Consider, for example, that 91.7% of unwanted email contains a URL.[1]

Need more convincing? Read this passage from the Verizon 2016 Data Breach Investigations Report:

> *"Generally speaking, there are three major avenues for crimeware installation, either via emails with malicious attachments, websites serving up drive-by downloads with each visit, or a hybrid of the two — emails with links to pages with, you guessed it, drive-by code installs."*

The net result is the need not just for email security, but for email and complementary Web security technologies working together to deliver maximum protection from increasingly blended, sophisticated threats.

The Fast and the Furious. As if blended threats are not enough of a challenge, organizations must also deal with the so-called, "industrialization of hacking." Along with a flourishing underground economy — where aspiring hackers can easily purchase malware and rent botnets for a few dollars a day or sell stolen data records to those prepared to further monetize them — comes the opportunity for specialization. Individual hackers can now focus on a single component or phase of a threat, such as propagation, exploit or payload, becoming experts in narrow but highly effective threat techniques.

Via the underground market, their highly specialized "product" is then combined with the output of hackers with expertise in other areas. The net result is industrialized threat production, featuring greater economies of scale, quicker build times, higher quality and more sophistication across the board. In other words, enterprises' IT teams must now contend with threat production that is "faster, better, and cheaper" than in the past. To keep pace, an effective content security solution requires a robust threat intelligence component capable of continuously arming itself with details about the latest and greatest threats emerging around the globe.

[1] Forcepoint 2016 Global Threat Report

The Outsider-Insider Dilemma. External threat actors continue to be a top concern for cybersecurity pros. After all, they remain the cause for approximately 80% of successful enterprise breaches.[2] With the balance being blamed on one's own employees, however, the issue of insider threat is also commanding significant attention these days. Even more troubling are the attacks perpetrated by external actors involving the use of stolen credentials — especially those that provide access to privileged accounts.

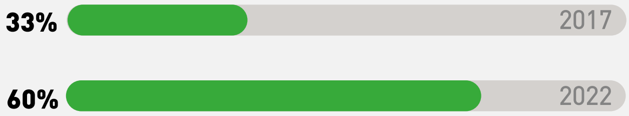
The result is the ability of external threat actors to conduct threat activities up to and including the exfiltration of sensitive data and content under the guise of a legitimate, authorized internal user. Separating this variety of threat (i.e., the compromised insider) from all of the routine traffic on an enterprise network requires a solution with advanced analytics that can distinguish subtle deviations from normal behavior, on a per-user basis.

The Dangers of Data Loss. Rapid proliferation of mobile computing platforms, widespread use of peripheral devices and easy access to file sharing and other cloud-based services have all elevated the risk for data loss. And the impact to enterprises can be substantial. Just a single incident can tarnish brand reputation, erode competitive advantage, sacrifice hard-earned customer goodwill, damage or destroy potentially irreplaceable intellectual property and lead to fines or penalties from regulators. Clearly, an effective content security solution must address more than just malware and targeted attacks; it must also account for the ultimate target — your organization's valuable data.

Providing Consistent Protection Everywhere

The Cloud Factor. For the modern enterprise, cloud services are both a blessing and a curse. By offering a flexible, utility-based model for everything from core compute infrastructure and feature-rich development environments to full-service applications, the cloud services model is enabling unprecedented degrees of business transformation and agility. On the downside, however, is the introduction of countless external datacenters to which an organization's sensitive data and valuable content are now being distributed, and where protection must now be established, monitored, and maintained. Complicating matters further is the phenomenon known as "shadow IT," where individual business units (or even users) take advantage of unsecured cloud services without IT having any knowledge of them doing so. Being able to account for all cloud-related use cases is yet another critical requirement for a truly effective, unified content security solution.

Gartner predicts that the penetration rate for cloud-based office systems will reach 33% for enterprise users by 2017 and 60% by 2022.[3]



The Distributed Workforce. Joining traditional business travelers as part of the extended enterprise, tens of millions of employees now work from home, in branch offices, or intermittently from a wide variety of highly-capable mobile devices at least part of the time. The security demand on IT teams is huge: organizations need to find an effective and affordable way to extend their content security solution to also cover all of their mobile and remote users.

Reducing Required Resources

The unfortunate reality is that IT security budgets are not growing at a rate equal to the change in scope and complexity of the security challenges facing today's organizations. Adding more fuel to the fire is the ongoing shortage of skilled security personnel. The implication, in both cases, is that enterprises need solutions that enable them to get more done with less.

ACCORDING TO THE 2016 CYBERTHREAT DEFENSE REPORT[4], THE TOP-RATED OBSTACLES FOR ACHIEVING EFFECTIVE THREAT DEFENSES ARE:

1. Low security awareness among employees
2. Too much data to analyze
3. Lack of skilled personnel
4. Lack of budget

The Compliance Mandate. Another important aspect of the content security challenge is regulatory requirements such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

[2] Verizon 2016 Data Breach Investigations Report

[3] http://www.gartner.com/newsroom/id/2514915

[4] CyberEdge 2016 Cyberthreat Defense Report

Demonstrating compliance with these and other regional legislation (e.g., the European Union General Data Protection Regulation) and industry-specific requirements (e.g., Federal Financial Institutions Examination Council (FFIEC) assessment guidelines) is a significant undertaking. It is also one that competes for scarce manpower and budgetary resources and for which there is no reasonable alternative — organizations that fail to comply run the risk of punitive penalties and negligence lawsuits. IT teams don't get to choose to provide security or compliance — they must provide both.

POINT PRODUCTS PERPETUATE PROBLEMS

With complexity and risks on the rise and resources remaining constrained, the bottom line is simple: when it comes to content security, organizations of all sizes must find a way to get more done with less. In this regard, the point product approach still in use by many IT departments, simply put, is an extremely poor fit. Undesirable characteristics of this traditional approach to security include:

Point Product Fatigue (i.e., high cost and complexity). Numerous, independent products are required to account for both different channels of communication (e.g., email, inbound and outbound Web traffic, and cloud applications), as well as different security capabilities/technologies (e.g., access control, antivirus, antispam, threat inspection, data loss prevention and data encryption). Indeed, practically every new technology, type of threat, mobile device, or application that comes along brings with it the need to purchase yet another product — or, in some cases, optionally implement yet another set of natively delivered security features. Not only that, but the organization has to juggle numerous vendor relationships, train security staff across a variety of products, and deploy, operate, maintain, support and, ideally, integrate all of them too.

The Disconnected Islands Problem. Because it has been constructed over time — mostly in a reactive manner — the security infrastructure at most organizations is largely a patchwork of standalone products. Other than a handful of one-way ties to a centralized security information and event management (SIEM), there is precious little integration between these components. In addition, there is limited cross-component data analysis or correlation, and little if any automated sharing of information or coordination of response activities. The result is a sub-optimal security posture that is riddled with gaps and inconsistencies in coverage, slow to account for newly discovered threats and inefficient to operate.

The Data Deluge Problem. With each point product and native feature set generating their own continuous stream of security events, logs and alerts, the result is that IT departments find themselves drowning in a sea of security data. For many organizations, the time and effort required to sift through and determine what it all means has become so great that they simply can't keep up. This situation is leading to steady erosion of the security posture for many businesses, confirming the need for security teams to avoid point product proliferation (where possible), while also adopting solutions that provide the advanced analytics and correlation capabilities needed to transform mountains of security data into handfuls of actionable information.

INTRODUCING UNIFIED CONTENT SECURITY

By this point, it should be clear that a disparate collection of point products is a poor match for the mounting complexity of today's content security problem. There are simply too many facets — threat types, communication channels, and locations — that require protection for such an approach to be cost effective. Security effectiveness is also a major issue, particularly as the narrowly focused and easily distinguished threats of the past have been displaced by a new generation of mixed threats.

What organizations need instead is a solution that better aligns with current and evolving conditions, as opposed to one that remains focused on the way things were in the past. This means having a content security solution that provides seamless coverage for all types of threats, across all major communication channels, and for all users and content assets, regardless of where they're located. It also requires one that alleviates the point product fatigue, disconnected islands, and and disparate solutions and data deluge problems mentioned above.

What organizations need is a solution that combines all of the requisite content security technologies — Web, email, and data loss prevention — into one unified architecture. From a high-level functional perspective, the goal is to have a solution that:

- Simultaneously accounts for all types of threats to and from content, including not only those coming from external threat actors, but also those originating from and/or masquerading as internal sources.
- Counters the "blending" capacity and sophistication of modern threats with a combination of global threat intelligence, advanced real-time inspection and analysis technologies, and extensive "collaboration" between the individual components of one's content security infrastructure.
- Supports multiple on-premises, cloud-based and mobile deployment options to enable comprehensive, best-fit coverage for all of an organization's locations, users and content assets.
- Delivers not only a single management console for controlling all of an organization's content security infrastructure in a simple and straightforward manner, but also a globally consistent set of enforcement policies and practices.

CONCLUSION

As noted as the outset of this paper, your content is the lifeblood of your organization and must be protected accordingly. But doing so effectively and efficiently is far from a trivial matter. Traditional point product approaches fail to adequately account for many of the technological and business-oriented issues facing today's enterprises, including:

- **The increasingly dynamic nature of modern Web properties and services**
- **The industrialization of hacking**
- **The blurring of the lines between external threat actors and authorized, internal users**
- **The proliferation of user mobility, collaboration and cloud solutions**
- **The ongoing pressure to get more done with less**

The right unified content security solution can address all of these shortcomings while providing a flexible and adaptable platform capable of meeting enterprise content security needs well into the future. Only with an industry-leading, unified content security solution are companies able to achieve:

- *Business Enablement Without Undue Risk.* New communication, collaboration and cloud technologies and solutions can safely and securely be leveraged, avoiding the need to say "no" to the business.
- *Consolidation and Cost Reduction Without Compromise.* Total cost of ownership (TCO) and infrastructure complexity are reduced while still providing comprehensive protection against legacy threats, modern attacks and the unwanted exposure of sensitive data.
- *Compliance Without Complexity.* Conformance with regulatory requirements is facilitated and achieved.

LEARN MORE

To learn more about unified content security:

1. Continue with part 2 of this series: *Unified Content Security Defined.* This whitepaper provides a detailed explanation of the technical capabilities that define a unified content security solution.

2. Continue with part 3 of this series: *Unified Content Security in Practice.* This whitepaper introduces Forcepoint's TRITON solution — the industry's first and only unified content security solution — and provides best practice guidelines and real-world examples for a successful implementation.

3. Visit **www.forcepoint.com.**

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT