



An Orchestria Whitepaper
On Securing Confidential Data

EXECUTIVE SUMMARY

Since the dawn of the computer age, there has been a mandate to keep the network and the data that traverses it safe. A virtual game of cat and mouse has played out in networks the world over. New and sophisticated technologies are introduced to thwart the newest security threats only to find the next threat looming on the horizon. This paper will examine the newest and most dangerous security threat facing every organization today. Regardless of the industry vertical, network topology or applications running in your network, there is a time bomb that if left unaddressed is likely to go off.

THE DEFENSE STRATEGY

There is no doubt that every organization with an online presence is concerned about keeping the network, its applications and data secure. The concept of keeping “the bad guys” out is not a new idea. As early as the 1980s security products were on the market that did just that. The strategy was that the bad guys were on the network exterior and as a result security products were designed to keep them there. When an attack was successful, the result was more of a nuisance than anything else. Servers may have been taken down, services were interrupted and websites were taken down.

Fast forward to early 2000 and attacks became more sophisticated. Many network compromises were a result from hackers external to the network that found a way in and then attacked from the “inside-out”. This may have been as a result of unknown attacks and backdoors. To contrast, other security breaches were insider-based. This included rogue employees who launched attacks knowingly or unknowingly did something as simple as downloading a virus from a website or opening an infected e-mail. During this period, the previous mindset of, “all attacks originating from the network exterior” was no longer the case. Furthermore, recognizing that internal personnel could do serious damage to the organization became reality. As a result, technology development was focused controlling employee behavior, as well as detecting and stopping attacks that originated on the network interior.

As we look back over the security landscape one thing has remained constant, the name of the game has always been to develop the technology that stops bad things from happening. While we have done a good job on mitigating the historical security threats that organizations faced, today’s security threats are more sophisticated, and pose a greater risk to organizations than ever before. Today’s security threats are no longer just a nuisance; they compromise data, destroy reputations and put organizations at risk. Existing security tools do not solve the issue and it is a gaping security hole that can bring down businesses.

Advanced Insider Threats By Insiders <ul style="list-style-type: none"> • Data leakage • Employee Behavior • Non Compliance • Information Exfiltration (intentional and unintentional) 	2004 – Present Policy and Control
Early Stage Insider Threats By Insiders <ul style="list-style-type: none"> • Advanced worms, trojans, backdoors, botnets, zero-day vulnerabilities, slow, stealthy and sophisticated attacks 	2002 – 2004 IPS VPN
Outside Threats <ul style="list-style-type: none"> • Viruses • DoS • Basic Worms 	1995 – 2002 Firewalls Anti-virus IDS

Fig 1: The brief history of threats and the security products devised to protect us

DATA AT RISK

Today’s security threats have changed significantly. Whereas security breaches used to revolve around website defacement and spotty application outages, today the risks are more profound. A variety of highly confidential data traverses the network including customer data, intellectual property, and other proprietary information. If this data should fall into the wrong hands, or even be mishandled in the right hands, it can cause more damage than a temporary application outage. The new “duty to disclose” legislation requires that when customer credentials are exposed, the organization must advise the affected customers of the breach. This results in the organization suffering negative PR and incurring substantial costs. In 2005, Card Systems suffered such a breach where 40 million customer records were stolen. The breach was the largest in history affecting 1 in 7 credit card holders¹. Beyond customer data, exposed corporate confidential data and intellectual property can put an organization at a competitive disadvantage that can ultimately jeopardize their competitive advantage in the market and affect the long term viability of the organization.

¹ <http://www.securityfocus.com/news/11219>

DATA LEAVING YOUR ORGANIZATION

There are two key methods by which data can leave your network:

Physical data movement

Confidential data can be removed from the network physically via removable devices such as USB drives and even via laptops. The physical loss of confidential data is largely secured by adhering to best practices including:

- Physical plant security. This includes hierarchical passkeys that limit physical access to certain areas.
- Data encryption on all devices. This ensures that in the case when a device becomes lost or stolen, the information stored on it is not compromised.
- Password protection on all applications and data files to ensure that only authorized personnel have access.
- Restriction and disabling of high risk ports and methods for transferring data such as USB drives, where appropriate.
- Anti-theft measures such as homing device software installed on portable devices.

Electronic data movement

The movement of electronic data often requires significantly more technical knowledge than physical data movement. In general, file transfers (FTP) and other means to exfiltrate confidential data require technical knowledge that is beyond the expertise of most employees in an organization. While most methods of non-authorized transfers of electronic data are secured, there still remain uncontrolled channels by which confidential data can be easily spirited out of the organization. This puts the organization at risk.

TARGETING THE UNSECURED

In order to control the leakage of confidential data, the average organization has wisely adopted a layered security approach by deploying multiple security products across its environment. The vast majority of organizations have secured themselves against external threats by deploying firewalls, anti-virus, and IDS technology. To combat insider threats, additional technology such as IPS and VPN technology have become widely used. As networks have become more sophisticated, application, transactional, and file system servers have been deployed. Not surprisingly, these application servers have robust security controls built in to them including hierarchical passwording and encryption. Hardened applications combined with the security devices provide a locked down environment that proactively endeavors to reduce any possible security risk in the environment. This is largely true with all network based applications with the exception of one - electronic communication.

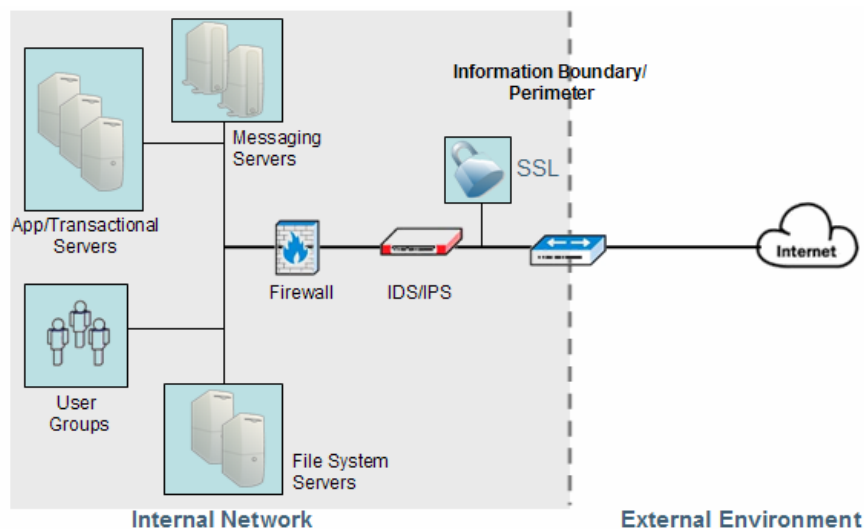


Fig 2: The typical network and its operating environment

While nearly all enterprise applications in the network are control rich, electronic messaging is control free. Messaging is perhaps the most ubiquitous application used by every level of personnel within the organization. Through electronic messaging, employees have the power to bind you to contracts, set terms, and interact with outside agencies, including the press, as a representative of the company. Furthermore, electronic messaging poses a substantial security risk as it can intentionally or unintentionally be a key instrument for data exfiltration and can also be used to leak intellectual property as well as customer credentials. Electronic messaging remains the biggest threat to the security of networks and to the security of your organization.

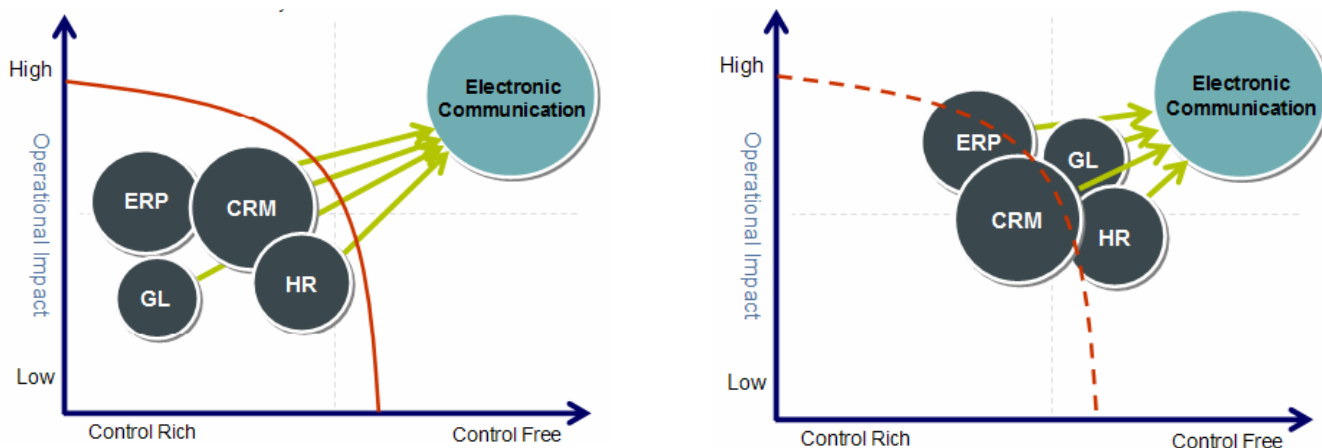


Fig 3: Most applications have built in controls. Electronic communication which has high operational impact is control free which puts confidential data and previously secured data at risk.

FIRST GENERATION SOLUTIONS

Boundary solutions were an early attempt to stem the unauthorized electronic flow of confidential data. These solutions, while providing some additional security over already deployed security products, also exhibit significant limitations.

DESIGN AND PURPOSE

Boundary solution architecture is predicated on stopping electronic messages at the edge or well-defined network perimeter. Detection at the perimeter however, is based on the legacy belief that “the bad is always on the outside” and thus the solution is unable to detect messaging violations that are interoffice. Because 30% of an average organizations messaging is in-house, a substantial amount of traffic will never be seen by the information boundary solution. Furthermore, with today’s increasingly interconnected networks including peering points, remote office links, and mobile sales force, the network perimeter has virtually vanished making it a virtually impossible area to defend.

A second major design flaw in boundary solutions is its designed purpose. Boundary solutions were originally architected to detect messages that were in violation of regulatory compliance. They were not designed to stop the leakage of confidential information. In many cases the solution itself is not secure or “hardened”. By deploying a non-hardened system to the network it opens additional security risks to the organization and does not meaningfully address the security issue it was originally supposed to solve.

DEPLOYMENT

Boundary solutions are installed in-line at the network perimeter and are designed to detect messaging violations once they leave the network. Because the solution is in the critical information path, it is unable to scale and can become a bottleneck once network traffic increases. Further complications arise if the solution should fail. When a catastrophic failure occurs, network traffic can be halted if the device does not fail to a wire. Redundant solutions are generally not available and are prohibitively expensive when they are.

DETECTION METHODOLOGY

Boundary solutions also are deficient in the methods used in detection of the message violation; namely via lexicon-based filtering. Using keywords, the product attempts to match up words and phrases with those on a “blacklist”. The result is a non-adaptive system that does not learn and is unable to adapt to a particular operating environment. Words have different meanings when used in a particular context. For instance, “Sue” can be a female’s name, and it is possible to “sue” someone. Because lexicon based systems do not take into account the context of the message, false positive alerts can be as high as 99%.

FLYING BLIND

Sensitive information is often encrypted using secure socket layer (SSL) in order to ensure that only the intended audience is able to gain access to the data. In an average network 30-40% of the traffic is encrypted. Information boundary solutions, because they are deployed at the perimeter, are unable to see the data prior to encryption. As a result, the most basic way of getting around an information boundary solution is to encrypt the data. In such cases, information boundary solutions are flying blind and give the administration a false sense of security which is merely a mirage.

WORKFLOW

Any security solution that is deployed must not only deliver the security it promises, but also must preserve the business workflow. Because of the mission critical nature of electronic messaging, this is especially true.

The boundary solution approach to addressing messaging violations is primarily to “cut the connection” and not allow the message to be sent. The user is not given the opportunity to correct the message that is in violation and, in fact, the user may only be notified hours later of the violation. Due to the high importance that electronic messaging has in the business process, this is not an acceptable solution as it directly impacts the business.

Some solutions try to fix this problem by allowing all messages through and simply alert the administrator after the message is sent. What greater risk can an organization be exposed to than being advised of a message violation after it has already been transmitted?

GOOD CONTROLS ARE GOOD BUSINESS

Orchestria, the leader in Electronic Communication Control (ECC) provides unparalleled protection against the leakage of confidential data, which is the biggest security risk for businesses today. Deployed on the internal network, Orchestria is optimized for the de-facto standard operating environments of a porous network perimeter. Furthermore, this methodology stops data leakage at the source. Based on the Orchestria deployment, policy application occurs prior to file or message encryption. As a result, virtually all electronic communication can be scanned and protected.

Orchestria's flexible deployment options include deployment on the end-point, at the gateway and/or on the messaging server. The ultimate decision depends on the network topology and customer requirements. Regardless of the final decision, Orchestria is never deployed in the critical flow of data that would cause bottlenecks if traffic should increase or cause redundancy issues if the product should suffer a catastrophic failure.

Electronic communication is no longer limited to e-mail. With the proliferation of e-mail, web based access, mobile devices, instant messaging, and more, complete channel coverage is essential. Additionally, coverage for the full lifecycle of the message is crucial, from the point of creation through transmission, archiving and retrieval.

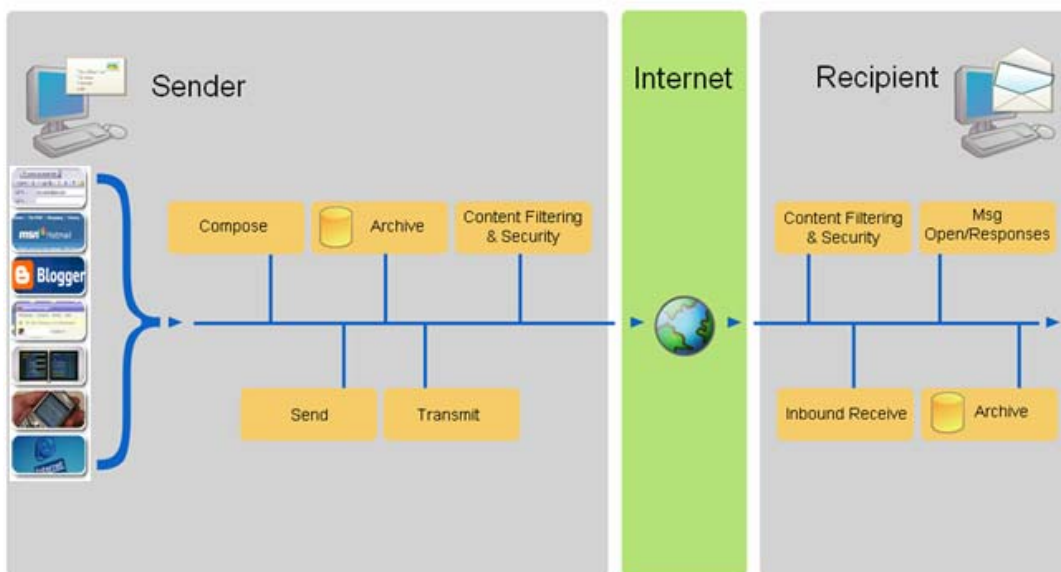


Fig 4: Orchestria offers full messaging channel coverage for the full lifecycle of the communication

Going beyond the old and inaccurate lexicon-based filtering, Orchestria utilizes highly accurate policy-based detection. Contextual analysis takes into account the full message, meta-data, the proximity of words to each other, attachments as well as whether content is present or absent. Policies are both industry-specific as well as industry-spanning and enable granular control with highly accurate results.

In order to promote workflow, Orchestria delivers alarm information to the user in real-time. This alerts the user that a message may be delayed and also provides the user with the opportunity to fix a message that is in violation. An additional benefit of training the user about what is considered an acceptable message helps reduce future message violations and overall alerts are dramatically decreased.

Reporting is a key area often overlooked in the quest to secure data. Orchestria offers the robust and secure iConsole web-based GUI that allows for both real time and historical access to executive summary and drill-down reports. Hierarchical access enables administrators access to only their message queue. This extreme visibility is not only essential for reporting purposes, but it is also important for determining points of risk that need to be dealt with.

THE BIG PICTURE

Security within the organization is top-of-mind in virtually every organization. While historical security threats were typically from the outside-in, today's security threats can come from virtually anywhere. Today's risks are more severe than ever. Confidential data can easily be lost or stolen with literally the click of the mouse, and a company may never recover. While most risks have been meaningfully addressed by organizations, the most ubiquitous and powerful application has been control-free until now.

Information boundary solutions attempt to solve this problem by using outdated deployment, detection and mitigation techniques that are not appropriate in today's business environment. In some cases, they even expose the organization to new problems.



Orchestria solves the control-free nature of electronic communication and addresses the significant security risk that it can pose to the organization. We:

- **Prevent** - Interact with the user to correct messages before they are sent
- **Tag** messages as they flow into the archive to support message categorization, selective archiving, and storage optimization
- **Hold** - Reduce the time, cost, and risk of complying with the amendments to the Federal Rules of Civil Procedure
- **Review** - Transform the review function from a process that misses virtually all non-compliant resources and wastes valuable compliance resources
- **Secure** - Close the single biggest security threat facing organizations today

Orchestria delivers a comprehensive family of control solutions by not just looking at the security issue, but by taking a more holistic approach to the problem. By providing good controls, the risk associated with control free electronic communications is eliminated and, as a result, good controls are good business

ABOUT ORCHESTRIA

Orchestra helps organizations eliminate the risks in uncontrolled electronic communication by working to prevent confidential data leakage, protecting intellectual property, encouraging appropriate employee behavior, and ensuring regulatory compliance. Our approach results in substantial return on investment (ROI) while improving both corporate governance and employee behavior.

For more information, please contact us today.

CONTACT DETAILS

New York | Orchestra
437 Madison Avenue, NY, NY 10022
Tel +1 212 364 5300
Fax +1 212 364 5301

info@orchestria.com
www.orchestria.com

London | Orchestra
One Canada Square, 29th Floor
Canary Wharf, London, E14 5DY
Tel +44 (0) 20 7725 2100
Fax +44 (0) 20 7725 2101