InfoTrust

netskope CROWDSTRIKE mimecast

EXECUTIVE SUMMARY

DRIVING CONNECTIVITY ACROSS YOUR SECURITY ECOSYSTEM

CONNECTIVITY ACROSS YOUR SECURITY ECOSYSTEM

Cybersecurity threats are one of the most significant business risks we face. Data breaches hit the headlines on almost a weekly basis, with businesses of all sizes losing money and customer trust. However, while data breaches and cybersecurity threats are certainly nothing new, they are far more complex than they once were.

58% of Australian security breaches occur due to malicious actors or criminal activity according to the latest Notifiable Data Breaches Report by the OAIC

The security landscape has changed immeasurably as our focus has shifted to collaboration and mobilisation. Our workforces are very different to what they were ten years ago. Today, people can work from anywhere using multiple connected devices. Meanwhile, the rapid adoption of cloud computing has put sensitive data at risk as it moves outside the enterprise perimeter. The result is that data can exist everywhere across applications, services, email, and websites which creates new opportunities for our adversaries. Ultimately, every piece of technology that we adopt in aiding collaboration, flexible working and productivity, creates a new level of risk.

Today's threats are more sophisticated and targeted than ever before as cybercriminals take advantage of new technology as well as weaknesses in human nature. According to the latest **Notifiable Data Breaches Report** by the OAIC, 58% of Australian security breaches occur due to malicious actors or criminal activity. Phishing attacks are still the leading source of malicious attacks, with breach reports highlighting the same figures time and again. As of the end of 2020, **more than 90%** of cyber attacks were email-borne. Whilst malware used to be associated with websites and emails, over **60% is now cloud delivered**.

As the volume and sophistication of cyberattacks such as ransomware and phishing increase alongside the attack surface, effective threat protection is vital. However, traditional defences that focus on the network perimeter are no longer sufficient to defend against attacks on multiple endpoints. Email perimeter protection no longer works when such a huge volume of employees are working remotely. Meanwhile, the native security controls of cloud protection offer limited defence against data loss and exposure. Organisations need to adopt an integrated, comprehensive yet manageable solution if they are to thrive. In such a complicated security landscape, jumping between multiple systems to oversee security measures, respond to a threat or investigate an incident no longer scales. Employing the right security controls and then optimising and managing them efficiently is key.

DEFENCE IN DEPTH

As our businesses have evolved, three common attack vectors have emerged: email, endpoint, and cloud. Businesses need to work on protecting these three areas to expand the email perimeter beyond the office network, to account for multiple devices and to understand where data is and who is accessing it, at all times.

EMAIL

A secure email ecosystem requires a comprehensive approach that can address today's sophisticated and targeted attacks. To ensure businesses can address both security and email management requirements, they should employ:

- **Secure Email Gateway (SEG)** - this is the first line of defence against a multitude of email-borne attacks, aiming to prevent the transmission of any emails that break company policy. A SEG filters both incoming and outgoing traffic and then blocks malicious emails or flags those with suspicious attachments. Additionally, automated email encryption can be used to stop cybercriminals from accessing sensitive information in the event that an attack is successful.

- **Email Security Awareness** - while an SEG can block malicious emails, it can't protect against complex social engineering attacks. To mitigate the risk of human error, cybersecurity awareness is key. Delivering a frequent, consistent, and engaging awareness program will aid in ensuring employees stay alert to the risks, thus creating a strong cybersecurity culture within the business.

- **Email Fraud Prevention** - in advanced attacks, cybercriminals often try to spoof domains and take over brands. Domain-based Message Authentication, Reporting and Conformance (DMARC) is a validation tool that aims to monitor who is sending the email, uncover anyone that is using a domain without authorisation and block delivery of related email.

ENDPOINT

Endpoint security is all about protecting computer networks that are remotely bridged to user devices. Every device, including laptops, tablets, and mobile phones that connects to the corporate network creates a potential attack path. To reduce the risk that endpoint attack vectors bring, organisations should employ:

- **Endpoint Detection and Response (EDR)** - EDR is a solution that uses machine learning and artificial intelligence to detect incidents that evade traditional preventative security measures. Solutions include advanced antivirus protection across multiple endpoints, proactive web security and insider threat protection. By having real-time deep visibility along with actionable threat forensics, security teams are empowered to investigate, prioritise, and respond to any threat.

- **Threat Intelligence and Hunting** - managed threat hunting brings in an added level of expertise to your endpoint security. As threats evolve and become ever more sophisticated, using intuition and experience trained experts can uncover the stealthiest of cybercriminals.

By having real-time deep visibility along with actionable threat forensics, security teams are empowered to investigate, prioritise, and respond to any threat.

- **Vulnerability management and IT hygiene** - one of the most obvious but often overlooked tactics is ensuring that your IT ecosystem is regularly updated and patched. This helps to ensure businesses don't fall victim to Zero Day attacks, reduces the attack surface and be better prepared to face threats.

CLOUD

As businesses increase their use of cloud services to benefit from business efficiencies, productivity, and cost savings, protecting the cloud environment needs to become a critical control point. To safely process, store and protect data in the cloud and gain comprehensive visibility and control, organisations should employ:

- **Cloud Access Security Broker (CASB)** - cloud services are used by all organisations, with their knowledge or otherwise. With so many third-party applications and services to boost productivity and facilitate collaboration and agile working, businesses need a layered security approach. CASB solutions give organisations visibility into shadow IT and allow them to govern data within cloud apps and protect against threats.

- **Data Loss Prevention (DLP)** - data loss often comes down to human error caused by weak passwords, missent emails and misconfigured systems. However, with data being shared and accessed across more endpoint devices than ever, the risk has escalated. DLP strategies help to manage the evolving landscape while still benefiting from enterprise mobility. Frameworks involve a range of measures that aim to prioritise, control, manage, monitor and backup data.

- **Secure Web Gateway (SWG)** - the web gateway has moved beyond websites. Now businesses require a next generation solution that protects its employees when using cloud services, applications and websites. For any user, location or device. A Next Gen SWG provides critical insight into the cloud and web services users are accessing, protecting them from cloud-enabled threats and enforcing policies.

THE BENEFITS OF INTEGRATED SOLUTIONS

Employing point solutions to help tackle the threats associated with email, endpoint and cloud is fundamental. However, while these solutions solve many security challenges, they create others. Multiple security solutions can be cumbersome to manage and maintaining best practice across email, endpoint and cloud can become extremely difficult.

In recent years there has been a big push across security vendors to improve native integrations to create more benefits to customers. With integration, there is the ability to share telemetry, data and information that gives each solution the edge to deliver next-generation security. With integrated best-in-breed technology, not only can businesses protect themselves against cybersecurity, but they can enhance threat detection with shared intelligence and gain a deeper understanding of the threats they face.

Netskope and **Mimecast**, the leading cloud and email security companies, provide a joint solution that addresses modern cloud security challenges and secures data regardless of where it is or who it is being used by. With the integrated solution, businesses are able to gain enhanced protection and optimised security operations with shared threat intelligence and integrated workflows. Benefits include:

- **Omnichannel Data Loss Prevention (DLP)** - detecting and protecting sensitive information across evolving cloud environments, including securing inbound and outbound email so that data is not sent outside the organisation or shared with unauthorised users.
- **Advanced Threat Protection for Email and Cloud Apps** - preventing modern attacks whether delivered via email or the cloud. Mimecast uses static file analysis and sandboxing technologies to block malicious emails and identify impersonation attacks. Meanwhile, Netskope implements sandboxing analytics, URL filtering and machine learning-based threat analysis to detect abnormal behaviour.
- **Threat Intelligence Sharing** - threat intelligence is shared in near real-time between Netskope and Mimecast so that key indicators of compromise can be continually analysed. Threat intelligence is best realised when it can be used to influence prevention actions, stop email threats in their tracks and determine the scope of any given attack surface.

With integration, there is the ability to share telemetry, data and information that gives each solution the edge to deliver next-generation security.

Mimecast and **CrowdStrike**, the industry leader in endpoint protection, help bolster defences with an integrated solution aimed at email and web gateways as well as endpoint devices. While an SEG is often the first system to detect new threats, endpoint security is the last line of defence. Together, through the sharing of intelligence from the SEG to the endpoint, joint users can:

- Protect against advanced, cloud-based malware.
- Stop email with malicious URLs or payloads from being delivered to end-users.
- Ensure all managed devices are aware of new threats as they are detected.
- Prevent infected files from executing at the moment threats are detected.
- Maximise security investment by optimising threat detection.

Netskope and CrowdStrike come together to deliver advanced threat detection across endpoints and into cloud applications. The automated exchange of information reduces the time for cloud threat detection, analysis, and prevention. The integration is able to deliver a comprehensive view across both cloud and endpoints by:

- **Exchanging threat forensics** - users gain real-time, actionable threat forensics and enhanced malware protection on both endpoints and in the cloud.
- **Closed-loop remediation** - when new malware is discovered in the cloud, Netskope passes the information to CrowdStrike, which can then alert affected endpoints and prevent malicious files from executing.
- **Adaptive access controls** - classification abilities from Netskope enable the identification of devices accessing cloud services. CrowdStrike then uses this information to secure endpoint devices according to access control policies.

+612 9221 5555 info@infotrust.com.au www.InfoTrust.com.au

InfoTrust

THE BENEFITS OF HAVING A SECURITY PARTNER & TRUSTED ADVISOR

Integrated solutions provide many business benefits. However, knowing which integrations are possible and which would most benefit any given organisation is a significant challenge. Even with integration in place, organisations are left with multiple vendors and multiple controls and portals to manage. It can be complex to know how to get the most out of the solutions and achieve the maximum return on investment. Meanwhile, lack of technical expertise, time constraints and conflicting priorities can all stand in the way. This is where working with a security partner comes into play.

A trusted partner can help businesses achieve a zero-trust framework, maintain best practice across all their solutions and get the best possible return on their investment. In fact, there are several additional benefits of partnering with a cybersecurity provider:

- Monitor and detect the latest cyber threats around the clock while leveraging advanced security techniques.
- Identify vulnerabilities by gaining a full understanding of existing cyber posture through a thorough cyber risk assessment.
- Respond quickly in the event of an incident with expert guidance as to which actions to take to prevent further harm to the business.

A trusted partner can help businesses achieve a zero-trust framework, maintain best practice across all their solutions and get the best possible return on their investment.

- Train employees with a well-developed program that includes the latest trends and can help build a dynamic awareness of risks.
- Ensure there is always a dedicated cybersecurity team on hand without the expense required for an internal team.
- Reduce the risk of fines from failing to adhere to regulatory data privacy and security compliance requirements.
- Retain the focus on core business needs while ensuring security capabilities will be able to adapt to the evolving cyber threat landscape.

HOW TO SECURE YOUR BUSINESS

When it comes to securing your business, connectivity across the whole ecosystem is vital. You need to employ the best-in-breed technology, optimise that technology with the right integrations and ensure you get the best possible return on investment. Cybersecurity is more than technology alone; you need to make that technology work for your business.

At InfoTrust, we are experts in securing email, endpoint, and cloud, and can help you build a robust security strategy that will secure your working environment, ensure business continuity, and promote business growth. To discuss your security strategy with us, **request a consultation today.**

+612 9221 5555 info@infotrust.com.au www.InfoTrust.com.au

InfoTrust