WHITE PAPER

Minimize the Risk and Impact of a Breach in the Cloud

Top 5 Strategies for Success

Executive Summary

Cloud computing is transforming organizations, offering the benefits of agility, flexibility and innovation. Security has often been cited as an inhibitor to cloud adoption, but high levels of public cloud adoption across the globe signify that cloud computing benefits outweigh perceived security risks. New risks and vulnerabilities are created when non-IT teams scale cloud instances up and down and when organizations incorrectly assume that their cloud services provider (CSP) is responsible for all of their data and asset security. According to Gartner Research, by 2020, 95 percent of cloud security failures will be the customer's fault.[1]

Data breaches are the number one cloud security concern cited by industry professionals, according to the Cloud Security Alliance. The multi-tenant, always-on features of cloud computing create unique security considerations for organizations of all sizes and in all industries. The inability to identify and resolve advanced threats rapidly can result in publicity-generating breaches, business downtime, financial losses and customer defections.

Data breaches can impact on-premises systems and cloud infrastructure alike. More than 169 million personally identifiable information records were exposed globally in 781 data breaches during 2015, according to the Identity Theft Resource Center.[2]

In this paper, we outline strategies for enhancing cloud security and facilitating the agility and organizational transformation that organizations require.

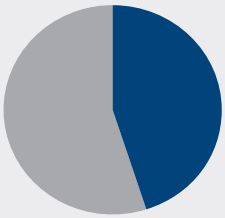
> "By 2020, 95% of cloud security failures will be the customer's fault."
>
> —Jay Heiser
> Research Vice President, Gartner Research

What You Will Learn

- How a cloud Incident Response Plan is unique
- How 24x7 monitoring reduces speed to detect
- Why threat intelligence enhances your security
- When to augment the expertise of your staff
- How to protect your brand reputation and financial bottom line

Who Should Read This White Paper

- Boards of Directors
- CISOs/CSOs
- Directors of Security
- IT Operations/Security Operations
- Security Architects



45%
Uncovered a security breach by accident

33%
Discovered a breach 24 months after the incident

Source: Ponemon Institute, *2014 State of Endpoint Risk* report, December 2013.

Strategy 1: Develop a Cloud Incident Response Plan in Advance

A Cybersecurity Incident Response Plan is a critical document that outlines in advance the people, processes and technology needed to respond to a cyber threat. Many organizations don't have a Cybersecurity Incident Response Plan (CIRP) in place or, if they have a plan, it is not regularly tested and updated. Being in the midst of a data breach and company crisis is no time to try and figure out the process and players that need to be involved.

The CIRP is a master document that can help you and your organization plan for and deal with a security breach. This plan outlines the roles, responsibilities and detailed steps needed to detect and stop computer threats. Organizations must understand the current threat landscape of persistent threat actors who evade detection and are persistent for months, even years, if you are their chosen target. CIRPs should take into account the nuances and unique aspects of cloud computing and cloud security. Your industry may also have specific mandates and best practices for an Incident Response Plan.

Work with executive leadership and senior management as part of the incident response process to obtain leadership buy in.

Questions to Consider:

- What is your organization's risk posture?
- Do you have an existing Incident Response Plan?
- Is cloud security included in your Incident Response Plan?
- Have you performed tabletop exercises to simulate real-world threats?

One reason to plan for and prepare the Cybersecurity Incident Response Plan in advance is to involve your cloud services provider (CSP) up front and prior to any potential incident. Your CSP typically has an acceptable use policy (AUP) that outlines what you and your firm can and cannot do in terms of access, network pinging and network activity. You will also want to determine who in your CSP's organization to communicate with — and how — in the event of an emergency.

Regular testing of your CIRP is another critical function. Some SecureWorks clients test aspects of their plan weekly to see how their teams perform under real-world conditions and to take immediate action to fill any gaps. Your testing should include a variety of breach scenarios such as cloud-based, on-premises and supply chain threats.

Security breach implications are multifaceted and will span a number of functional areas and touch senior leadership across your organization. As a result, your overall ability to detect and resolve a breach effectively will be contingent on advance planning and involvement across your organization and with your cloud services provider. SecureWorks offers cloud-centric incident response services such as risk assessment, incident response plan development, training, exercises, digital forensics and threat analysis.

Strategy 2: Enhance Visibility to Improve Security

With a move to the public cloud, you give up some of the hands-on control that existed with on-premises data centers and server rooms. Continuous visibility can enhance your protection by compensating for this loss of control and ensuring that security and compliance is built into your cloud approach.

IT and security teams should integrate threat intelligence into their environment in order to train incident response (IR) staff on the tactics, techniques and procedures (TTP) of threat actors. This in-depth insight provides warning of emerging threats and improves your ability to prevent, detect and respond to advanced threats wherever they reside.

Ongoing operational reporting across multiple portals, dashboards and tools is no longer effective as you look to make faster and better decisions on resources, assets and threat vectors. Data that resides in different silos and is not integrated or correlated makes it challenging to reconcile impacts and more likely that threat patterns will be overlooked. Real-time data with anywhere, anytime visibility, including mobile, can provide you with a comprehensive threat picture across cloud and on-premises systems. Best-in-class reporting and portals provide a "single pane of glass" insight across your organization with productivity-enhancing tools such as compliance templates. Portals and dashboards such as those from SecureWorks help you differentiate routine events from potentially dangerous and suspicious events.

Questions to Consider:

- How and where did the attack start?
- Has your data been exfiltrated or removed?
- Do you have access to the logs and alert data needed from your cloud services provider?
- Are the attackers still lurking in your environment?
- Do you have a client portal with detailed and broad visibility?
- How can you prevent evasive attacks in the future?

Strategy 3: Implement Cloud Monitoring

All of your physical and virtual servers, appliances, firewalls, routers and endpoints generate large quantities of raw log files. These log files need continuous monitoring to assess internal and external threats. Internal threats by insiders could include privileged unauthorized activity and access. External threats include zero-day exploits and other compliance-specific events for your industry and organization. Compliance mandates such as PCI DSS (Payment Card Industry Data Security Standard) may also require continuous log monitoring depending on your industry. Security event monitoring is the first level of defense in a defense-in-depth strategy for your business-critical applications and data in the cloud.

Targeted attacks and evasive threats have unfortunately become more frequent and sophisticated. Speed to detection is critical to detect anomalies and data compromise so you can remediate and get back up and running quickly. Organizations often underestimate the resources and expertise needed to conduct continuous 24x7 monitoring of physical and virtual devices and assets.

Important Cloud Data Sources

- Web server logs
- Application server logs
- Cloud-provider logs
- Database logs
- Packet capture logs
- Network captures
- Management portal logs
- API logs
- Logs from DNS servers

Cloud services providers often have their own monitoring services and capabilities, as well as log storage and reporting tools. But telemetry and technology alone don't offer in-depth understanding of possible attackers and their objectives. Log files require real-time analysis and correlation against known threat data and behavioral data to determine which events pose a risk to your data and brand reputation. Most of your events are routine and don't require action. But which ones are suspicious and should be flagged for follow up? Dedicated, skilled resources are needed 24x7 to review and interpret the logs to detect threats before damage can be done. You may have the existing staff and expertise to perform in-house log management, or you may need external assistance to centralize, analyze and report on patterns and anomalies. SecureWorks has a wide range of Security Event Monitoring (SEM) services in the cloud and on-premises to augment your capabilities.

Cyber threats are no longer script kiddies wreaking havoc for fun; cybercrime is a global, well-armed big business with black market earnings in the billions of dollars.

Should a breach occur, raw log data and historical alert data will help incident responders determine when and how the breach occurred and trace the threat actor within your cloud infrastructure. Storing log files can also provide valuable forensic data to law enforcement for criminal prosecution. The best practice for log retention is keeping a minimum of 3 to 6 months of historical data. This historical logging is vital to identify when and how a threat actor first compromised your infrastructure.

Questions to Consider:

- Do you have the staff and skill sets for continuous 24x7 monitoring?
- Do you have full visibility across on-premises and cloud-based assets?
- Can your team perform threat correlation across your environment?
- Do you have real-time visibility into your CSP and historical visibility going back months?

Strategy 4: Adopt Threat Intelligence

A new approach is needed to detect and eradicate advanced and evasive threats from persistent threat actors. You can reduce the magnitude of a breach by using a defense-in-depth strategy that includes threat intelligence to zero in on impacted assets and anomalies for further investigation.

Threat actors continue to evolve and improve their tradecraft and, likewise, next-generation threat intelligence should advance to help organizations improve on threat detection and remediation. You may find your organization challenged with understanding the scope and severity of cyber threats, both on-premises and in the cloud, and how to fund and staff accordingly. Cyber threats are no longer script kiddies wreaking havoc for fun; cybercrime is a global, well-armed big business with black market earnings in the billions of dollars.

The SecureWorks Counter Threat Unit™ (CTU) research team monitors the threat landscape for emerging threats that impact clients. They deliver actionable guidance via subscription and research services that assesses true threats and practical guidance to overcome them.

"Our Global Threat Intelligence feed puts threats on clients' radar screen as they emerge."

— Kevin Houle
Director of Counter Threat Intelligence, SecureWorks

It is inevitable that as business-critical data moves to the cloud, threat actors will likewise accelerate their efforts to target virtual systems and cloud workloads, along with human vulnerabilities, to capitalize on security gaps in the cloud. Indicators such as domain names, IP address sources and hashes are useful, but this does not constitute advanced threat intelligence. Best-in-class threat intelligence provides context around threat actors based on studying threat adversary behavior and their tools, techniques and procedures. Organizations with high security maturity can utilize threat intelligence to provide more insight and advance warning of emerging threats to their decision making.

Questions to Consider:

- Is your organization using multiple sources and experts to inform its threat intelligence?
- Are you in a vertical industry that threat actors are likely to target?
- Are you interested in making better security decisions?

Strategy 5: Seek Outside Expertise

Evasive and persistent threats create a new imperative for staffing and skill set development. Security professionals with the threat detection and reverse engineering skills are now highly paid and recruited. One public sector IT director recently shared his frustration at serving as the "training ground" for commercial business to hire away skilled employees with higher salaries. The combination of marrying robust security expertise and deep cloud capabilities makes this skills gap even more acute.

It may be possible for you to retrain existing staff, but this takes time and may not be sufficient. Some organizations utilize their own in-house staff to resolve commodity threats that are more routine while engaging external experts for remediating targeted threats and advanced persistent threats (APTs). Organizations often overestimate their capacity to resolve threats internally and can actually prolong resolution or destroy forensic evidence in the failed attempt. SecureWorks has been engaged by firms that mitigated some threats internally but did not perform a root cause analysis and faced the unpleasant task of re-compromise and a more costly remediation. You need to conduct an honest assessment of your team's security and cloud capabilities, identify staff and expertise gaps and outline proactive options to fill the gaps.

SecureWorks helps organizations of all sizes and industries prepare for, respond to and recover from even the most complex security incidents in the public cloud and on-premises. Advanced planning and cloud-centric security strategies can help reduce the likelihood and duration of a security breach.

Questions to Consider:

- Have you experienced a data breach and, if so, how did your staff perform under pressure?
- Do you handle commodity threats differently from advanced and evasive threats?
- Will leveraging third-party expertise help fast track your security maturity level?

Conduct an honest assessment of your team's security and cloud capabilities, identify staff and expertise gaps and outline proactive options to fill the gaps.

Conclusion: Optimize Cloud Security to Accelerate Transformation

Reduce the scope and duration of a data breach in the cloud with a multi-pronged approach to security. Augment your existing security to encompass unique aspects of cloud computing and your business risk posture and organizational objectives. Public cloud computing with its multi-tenancy is a shared responsibility, and you must understand where your security responsibilities begin and that of your cloud services provider end.

Today's cyber threat actors can adapt and evade detection so you need a blend of people, processes, technology and intelligence to thwart sophisticated adversaries in the cloud. Every second counts when trying to stop sensitive data from being stolen and sold on the underground market. The benefits of being prepared for a potential data breach in the cloud include:

- Resuming operations more quickly
- Minimizing time and cost to mitigate
- Optimizing finite resources and staff
- Ensuring root cause determination to avoid re-compromise
- Protecting brand reputation, financial bottom line, and compliance posture

Most organizations have a mix of infrastructure and assets on-premises as well as in the cloud called hybrid IT. The Top 5 Strategies to minimizing risk and impacts of a data breach in the cloud are:

1. Develop a Cybersecurity Incident Response Plan for the Cloud
2. Enhance visibility to improve security
3. Implement cloud monitoring
4. Adopt threat intelligence
5. Seek outside expertise

Cloud security can help you transform your organization and accelerate IT agility and speed to market. SecureWorks can help you navigate this transformation with a proactive and comprehensive approach to security.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com/cloud

[1]Heiser, Jay, Gartner Research, "Clouds Are Secure. Are You Using Them Securely?", July 21, 2016.
[2]Identity Theft Resource Center, "Identity Theft Resource Center Breach Report Hits Near Record High in 2015," http://www.idtheftcenter.org/Data-Breaches/2015databreaches.html, January 25, 2016 (accessed July 18,2016)