Microsoft Cyber Defense Operations Center

STRATEGY BRIEF

Cybercriminals are all around us. Hacktivists cause disruptions to make a political statement and capture headlines. Organized crime syndicates employ sophisticated financial ruses to generate profit. Nation-state actors leverage extensive resources to advance their agenda. No person or organization is safe from the myriad of threats from around the globe. The threats we see today are not new, but the level of sophistication our adversaries employ continues to reach new heights.

This strategy brief outlines how the Microsoft Cyber Defense Operations Center (CDOC) brings together security experts and data scientists from across the company to form a unified and coordinated defense against the evolving threat landscape—to protect Microsoft's cloud infrastructure and services, products and devices, and our own corporate resources.

The CDOC has been operational for over a year and during this time we have established practices and procedures that accelerate the development of security solutions, the identification and resolution of security threats, and we have shared this information with thousands of customers who have visited the Center. We've included information in this report that provides insight into some of the challenges the industry is facing and our strategies to address them.

Cyber Defense Operations Center

The vanishing security boundary

There was a time when protecting your environment simply meant setting up a strong perimeter to keep adversaries out. But with the significant growth of connected devices and services, including bring-your-own-device and cloud-based applications, that perimeter now extends across a much more diverse set of technologies. This increased connectedness can be seen in automobiles, energy management controls, health monitors, security systems, smart phones, televisions, refrigerators and tablets that are now a part of the "Internet of Things."

Today with the explosion of data from both inside and outside of an organization, it's clear that attack vectors are everywhere. Furthermore, the "bad actors" (cyber terrorists and hackers) are becoming more sophisticated and organized to take advantage of the ever evolving and connected world.

Through the course of this brief, we will share insights into how we protect Microsoft's hyper-scale cloud infrastructure and cloud services, products and devices our customers use, and the company's internal resources beyond a traditional security perimeter, how we detect intrusions and how we respond to compromises and attacks.

The Microsoft Cyber Defense Operations Center

Microsoft has invested more than $15 billion on our cloud infrastructure and invests more than $1 billion each year on security. The company delivers more than 200 cloud services, including Bing, Outlook.com, Office 365, OneDrive, Skype, Xbox Live, and the Microsoft Azure platform. These services are hosted in Microsoft's globally-distributed cloud infrastructure – exceeding 100 datacenters with more than a million physical servers – and connected through one of the world's three largest networks.

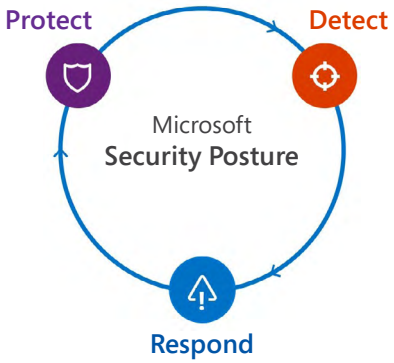
The Microsoft Cyber Defense Operations Center (CDOC) brings together security response experts from across the company to help protect, detect and respond 24x7 to security threats against our infrastructure and services in real-time. Informed by trillions of data points across an extensive network of sensors, devices, authentication events and communications, the CDOC teams employ automated software, machine learning, behavioral analysis and forensic techniques to create an intelligent security graph of our environment. The intelligent security graph helps us protect all endpoints, better detect attacks and accelerate our response.

$1 billion

is invested annually by Microsoft to advance our efforts on security, data protection and risk management.

Operational data from within Microsoft's ecosystem is analyzed by more than 50 security experts and data scientists who are connected to over 3,500 security professionals across the company. In a unified and holistic approach, they can detect attacks as they happen and before they can impact our services and customers. Our extensive investments in security analytics build rich behavioral profiles and predictive models that allow us to connect the dots and identify advanced threats that might otherwise have gone undetected, then counter with strong containment and coordinated remediation activities.

Microsoft is also deeply committed to sharing security knowledge and best practices we have learned from operating at hyper-scale with our customers, partners and the industry, so we can make the online world safer for everyone.



The Microsoft cybersecurity posture

While security has always been a focus for Microsoft, we recognize that the digital world requires continuous evolution in our commitment to how we protect, detect, and respond to cybersecurity threats. These three commitments define our approach to cyberdefense and are a useful framework for our discussion of the CDOC strategies and capabilities.

Protect

Microsoft's first commitment is to protect the computing environment used by our customers and employees to ensure the resiliency of our cloud infrastructure and services, products, devices and the company's internal corporate resources.

Access to these resources is tightly controlled and managed to help prevent unauthorized intrusion. An extensive risk-based Information Security Management System guides our operations, which includes over 800 controls that align to industry standards such as ISO/IEC 27001:2013 and NIST 800-SP61 Rev2.

We also ensure that configuration change management policies are established and closely monitored. The proactive maintenance of controls and components is employed across the environment and updates are swiftly deployed.

Additionally, risk-based information security and privacy controls, and an extensive compliance framework ensures that our infrastructure meets our commitments while helping customers simplify their otherwise complex compliance requirements. For our cloud service customers, these measures and regular third-party audits result in numerous security certifications and attestations that ensure we meet the security, privacy and compliance regulations of the industries and regions that we serve, such as FISMA, FEDRAMP, DISA, PCI, and SOX.

With these extensive security and data protection measures in place, we can achieve a broad range of international, industry and regional certifications and attestations from recognized third-party authorities. In fact, the Microsoft cloud today has more compliance certifications than any other cloud provider.

3,500+

security-focused professionals are employed by Microsoft. The Center brings together over 50 cybersecurity experts and data scientists in a centralized hub that is tightly connected to these globally-distributed security professionals.

Microsoft has decades of experience in supporting businesses and enterprise and government customers of all sizes. This means we understand the critical requirements for running software for businesses, including certifications, data sovereignty, security and privacy. Microsoft is the only global cloud vendor licensed to operate in China and the only one to offer data sovereignty in Germany. By adopting Microsoft cloud services to host your workloads, you are several steps closer to meeting your own compliance requirements.

Defense-in-depth is a best practice across the industry and it's the approach we take to protect our valuable customer and corporate assets. Applying controls at multiple layers involves employing overlapping safeguards and risk mitigation strategies, which helps to ensure more resilient protection across our platforms.

Microsoft's protection tactics include:

- **Extensive monitoring and controls** over the physical environment of our global datacenters, including cameras, personnel screening, fences and barriers, and multi-factor authentication for physical access.
- **Software-defined networks** that protect our cloud infrastructure from intrusions and distributed denial of service attacks. These include advanced firewalls and network intrusion detection systems.

- **Multifactor authentication** is employed across our infrastructure to control identity and access management. It ensures that critical resources and data are protected by at least two of something you know (password or PIN), something you are (biometrics) and/or something you have (smartphone).
- **Non-persistent administration** employs just-in-time (JIT) and just-enough administrator (JEA) privileges to engineering staff managing our infrastructure and services. This provides a unique set of credentials for elevated access that automatically expires after a pre-designated duration. In addition, secrets management practices and password vault usage eliminates the need to keep passwords in shared lists and reduces the effectiveness of lateral movement techniques such as "pass-the-hash."
- **Proper hygiene** is rigorously maintained through up-to-date, anti-malware software and adherence to strict patching and configuration management. Microsoft is uniquely positioned in the battle against malware due to the trillions of data points across an extensive network of sensors, devices, authentication events and communications that we receive from hundreds of millions of servers and devices around the globe.
- **Microsoft Malware Protection Center's** team of researchers identify, reverse engineer and develop malware signatures and then deploy them across our infrastructure for advanced detection and defense. These signatures are distributed to our responders, customers and the industry through Windows Updates and notifications to protect their devices as well.
- **Microsoft Security Development Lifecycle** is used to harden all applications, online services and products, and to routinely validate its effectiveness through penetration testing and vulnerability scanning.
- **Threat modeling and attack surface analysis** ensures that potential threats are assessed, exposed aspects of the service are evaluated, and the attack surface is minimized by restricting services or eliminating unnecessary functions.
- **Classifying data** according to its sensitivity—high, medium or low business impact—and taking the appropriate measures to protect it, including encryption in transit and at rest, and enforcing the principle of least-privilege access provides additional protection.
- **Awareness training** that fosters a trust relationship between the user and the security team to develop an environment where users will report incidents and anomalies without fear of repercussion

$3 trillion

is the estimated economic value destroyed by cybercrime attacks, according to the World Economic Forum.

Having a rich set of controls and a defense-in-depth strategy helps ensure that should any one area fail, there are compensating controls in other areas to help maintain the security and privacy of our customers, cloud services and our own infrastructure environment.

However, no environment is truly impenetrable, as people will make errors and determined adversaries continuously look for ways to trigger and/or exploit them. The significant investments we continue to make in these protection layers and baseline analysis enables us to rapidly detect when abnormal activity is present.

Detect

Microsoft operates under an "Assume Breach" posture. This means that despite all the protections in place, we assume systems will fail or people will make errors, and an adversary may penetrate our infrastructure and services. This posture places us in an "always ready" position to rapidly detect a compromise and take appropriate actions.

Our unique, hyper-scaled network of sensors, devices, authentication events and communications provide deep insights into the threat landscape that leverages the scale and intelligence of our cloud, with machine learning and behavioral monitoring, to quickly detect abnormal activity. This signal is enriched with contextual metadata and behavioral models generated from sources such as Active Directory, asset and configuration management systems and event logs.

Microsoft also employs its own custom-developed security software, along with industry-leading tools, and machine learning. Our threat intelligence is continually evolving, with automated data enrichment, to better detect malicious activity rapidly.

Vulnerability scans are performed regularly to test and refine the effectiveness of protective measures. The breadth of Microsoft's investment in its security ecosystem and the variety of signals monitored by the CDOC teams provide a more comprehensive threat view than can be achieved by most service providers.

140+ days

is the industry median that an attacker is on a victim's network before they are detected. Microsoft's cloud and security software tools reduce this median time down from a couple days to minutes, depending on the type of attack.

Microsoft's detection tactics include:

- **Monitoring network and physical environments** 24x7x365 for potential cybersecurity events. Behavior profiling is based on usage patterns and an understanding of unique threats to our services.
- **Identity and behavioral analytics** are developed to highlight abnormal activity.
- **Machine learning** software tools and techniques are routinely used to discover and flag irregularities.
- **Advanced analytical tools and processes** are deployed to further identify anomalous activity and innovative correlation capabilities. This enables highly-contextualized detections to be created from the enormous volumes of data in near real-time.
- **Automated software-based processes** that are continuously audited and evolved for increased effectiveness.
- **Data scientists and security experts** routinely work side-by-side to address escalated events that exhibit unusual characteristics requiring further analysis of targets. They can then determine potential response and remediation efforts.

When we detect something abnormal in our systems, it triggers our response teams to engage.

Respond

Our third commitment is to respond swiftly and with precise force. Notifications from our software-based detection systems flow through our automated response systems. These systems use risk-based algorithms to flag events requiring intervention from our response team. Mean-Time-to-Mitigate is paramount and our automation system provides responders with relevant, actionable information that accelerates triage, mitigation and recovery.

To manage security incidents at hyper-scale, we deploy a tiered system to efficiently assign response tasks to the right resource and facilitate a rational escalation path. Our cybersecurity personnel have advanced certifications in many areas, including incident response, forensics and intrusion analysis, and possess a deep understanding of the platforms and applications operating in our production datacenters globally.

$15 million

is the average cost companies paid for cybercrime in 2015 for remediation and related expenses.

Microsoft's cyberthreat intelligence and security analysts enable the CDOC to reduce vulnerabilities, mitigate attacks and rapidly respond to cybersecurity events, while minimizing service disruptions.

Microsoft's response tactics include:

- **Automated response systems** use risk-based algorithms to flag events requiring human intervention.
- **Well-defined, documented and scalable incident response processes** within a continuous improvement model helps to keep us ahead of adversaries by making these available to all responders.
- **Subject matter expertise** across our teams, in multiple security areas, including incident response, forensics, and intrusion analysis, and deep understanding of the platforms, services and applications operating in our cloud datacenters provides a diverse skill set for addressing incidents.
- **Wide enterprise searching** across both cloud, hybrid and on-premises data and systems to determine the scope of the incident.
- **Deep forensic analysis** for major attacks are performed by specialists to understand incidents and to aid in their containment and eradication.
- **Microsoft's security software tools, automation and hyper-scale cloud infrastructure** enable our security experts to reduce the time to detect, investigate, analyze and rapidly respond and recover from cyberattacks.

Evolution of cyberthreats—Same tactics. New sophistication.

$1.8 million

was the average cost of a spear-phishing attack for U.S. businesses in 2016.

Compromised credentials

- *Credentials remain stubbornly easy to access, as social engineering efforts collide with well-intended employees, often creating a weak link in cybersecurity. More than 90 percent of advanced persistent threat attacks start with a phishing email. Adversaries prey upon human emotion— helpfulness, fear, confusion and preoccupation —to trick users into unwittingly sharing their log-in information. Phishing emails are the weapon of choice for the initial intrusion into a targeted organization. While it used to be fairly easy to recognize a phishing email—poor language, ragged logos—adversaries have become quite skilled in tricking even the most experienced users. Once in, moving laterally across the network is successful or not depending upon the additional protections the victim has in place.*

Distributed Denial of Service (DDoS)attacks)

- *While DDoS attacks have been around for years, it is the scale of attacks that continues to make this threat difficult to defend against. Attacks of more than 100 gigabits per second were rare just a year ago, but attacks of this magnitude are becoming common and we are now seeing attacks of more than 600 gigabits per second.*
- *Both the growth of the Internet and the growth of the Internet of Things is creating more connected devices; many of which are unsecure and render them available to carry out these larger DDoS attacks. Microsoft Azure provides an automated DDoS detection and response capability that can detect and respond to an attack within 90 seconds without human intervention. The high rate of detection and mitigation is due to a change in the way we distribute traffic around the world.*

Malware/Ransomware

- *Malware has been with us since nearly the birth of the Internet and continues to expand. In 2015, more than 300 million unique variants were created. Ransomware attacks cost their victims a total of $209 million in the first three months of 2016, a surge upward from $24 million in all of 2015 based on reports received by the FBI.*
- *Ransomware was traditionally targeted at individual users, but enterprises are now in the crosshairs of attackers. Organizations in the healthcare field are now a common target. When dealing with life-or-death situations, hospitals need access to patient information and today the adversaries are sophisticated enough to pre-determine a level of ransom that the targeted company can pay—and in many cases, will. Effectively protecting from malware requires an active effort based on the part of all involved. For in-depth guidance, see the Microsoft Malware Protection Center.*

82%

of all companies globally expect to face a cyberattack in 2017.

Assume breach posture

Cyber attackers always push boundaries, so everyone with an online presence needs to push themselves to keep pace. Recent studies showed that more than 82 percent of companies expect to experience a cybersecurity event in the coming year.

It's estimated that up to ten percent of Microsoft's daily network traffic is a result of attempted DDoS attacks and/or other adversarial activity.

A key security principle we follow is an assume breach model. This simply means that despite the confidence we have in the defensive protections in place, we assume adversaries can and will find a way to penetrate security perimeters. This posture allows defenses to be seen from an attacker's point of view and includes tests to discover and fix vulnerabilities.

To ensure that we stay ahead of the recent threats displayed by adversaries, we regularly conduct "red team" and "blue team" exercises. The red team acts as an opposition group of adversaries who attempt to breach our live production services by defeating mitigative controls, using the same tactics, techniques and procedures (TTPs) that advanced adversaries use. The blue team, in parallel, uses our advanced software tools and cybersecurity techniques—leveraging the significant investments made in data visualization and machine learning—to detect and thwart the red team's efforts.

Prevent Breach: Protect perimeter

- Defense-in-depth
- Threat modeling
- Security scanning
- Security development lifecycle

Critical, but not enough to eliminate all security risks

Assume Breach: War Game/Penetration test

Red team: covert attempts at penetration and exploitation

Blue team: centralized detection and response; not solely dependent on protected perimeter

Proactively tests all aspects of security and uncovers unforeseen vulnerabilities

Trillions

of signals from billions of sources provide unique insights into Microsoft's threat landscape. The hyper-scale intelligence of our cloud powers machine learning and behavioral monitoring to quickly detect malicious activity.

In many cases, these tests will intentionally allow the red team to penetrate past the initial barrier, so interior infrastructure defenses can also be thoroughly tested. These simulations are targeted only at our own infrastructure, services and platforms. Every red team engagement is then followed-up with a full disclosure between the red team and blue team members to identify gaps, address findings, build new processes and tools, and collaboratively seek innovative ways to improve our cybersecurity and breach response tactics. Red teams actively contribute to our automation and innovative detection techniques.

The assume breach approach limits the trust placed in applications, services, identities and networks by treating them all—both internal and external—as presumed to be potentially compromised. Deep investments in training cybersecurity experts and software tools, and these ongoing exercises help Microsoft to uncover potential vulnerabilities and drive continuous improvements across our people, processes and technologies.

Cyber defense for our customers

We are often asked what tools and processes our customers can adopt for their own environment, and how Microsoft might help in their implementation. Microsoft has consolidated many of the cyber defense products and services we use in the CDOC into a range of products and services, and the Enterprise Cybersecurity Group and Microsoft Consulting Services' teams engage with our customers to deliver the solutions most appropriate for their specific needs.

300+ million

new pieces of malware were created in 2015.

One of the first steps that Microsoft highly recommends is to establish a security foundation. Our foundation services provide critical attack defenses and core identity-enablement services that help you to ensure your assets are protected. The foundation helps you to accelerate your digital transformation journey to move towards a more secure modern enterprise.

Building on this foundation, customers can then leverage solutions proven successful with other Microsoft customers and deployed in Microsoft's own IT and cloud services environments. For more information on our Enterprise cybersecurity tools, capabilities and service offerings, please visit Microsoft.com/security and contact our teams at cyberservices@microsoft.com.

Best practices to protect your environment

Invest in your platform	Invest in your instrumentation	Invest in your people
Agility and scalability require planning and building enabling platforms	*Ensure you are exhaustively measuring the elements in your platform*	*Skilled analysts and data scientists are the foundation of defense, while users are the new security perimeter*
Maintain a well-documented inventory of your assets	Acquire and/or build the tools needed to fully monitor your network, hosts and logs	Establish relationships and lines of communication between the incident response team and other groups
Have a well-defined security policy with clear standards and guidance for your organization	Proactively maintain controls and measures, and regularly test them for accuracy and effectiveness	Adopt least privilege administrator principles; eliminate persistent administrator rights
Maintain proper hygiene—most attacks could be prevented with timely patches and anti-virus	Maintain tight control over change management policies	Use the lessons learned process to gain value from every major incident
Employ multi-factor authentication to strengthen protection of accounts and devices	Monitor for abnormal account and credential activity to prevent abuse	Educate, empower and enlist users to recognize likely threats and their role in protecting business data

The following individuals contributed to this strategy brief: Andre Alfred, Hannah Bostwick, Bryan Casper, John Dellinger, Monica Drake, Alex Harmon, Brian Hooper, Marek Jedrzejewicz, Jessen Kurien, Kristina Laidler, Cory Marchand, Biju Matthew, Tom Snead and Darrell West.