Rethinking security efficacy:

How to reduce and manage your business risk

Content

Introduction

Every day, employees and customers deploy more apps, on more devices, and connect to corporate networks from a nearly infinite number of locations.

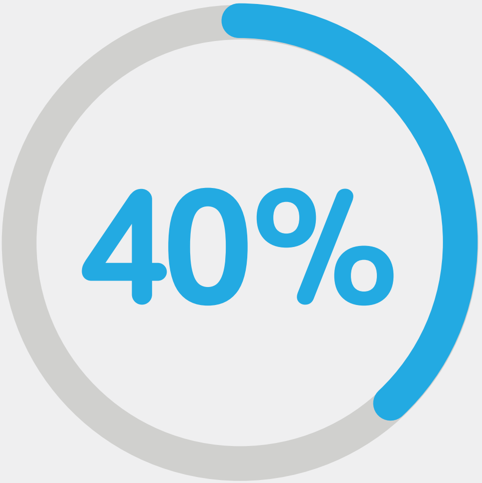
In this new world of apps everywhere and users anywhere, IT and security leaders encounter ever-increasing levels of risk.

They face greater exposure to security breaches, caused in part by the daunting challenge of supporting disparate security solutions, with multiple management consoles and inconsistent policies. They must cope with expanded attack surfaces that give attackers more places to find data and steal user credentials. They lack the tools to correlate and interpret ever-increasing volumes of threat data. And they must overcome the increased complexity of managing infrastructures that span data centers and diverse cloud platforms across the globe.

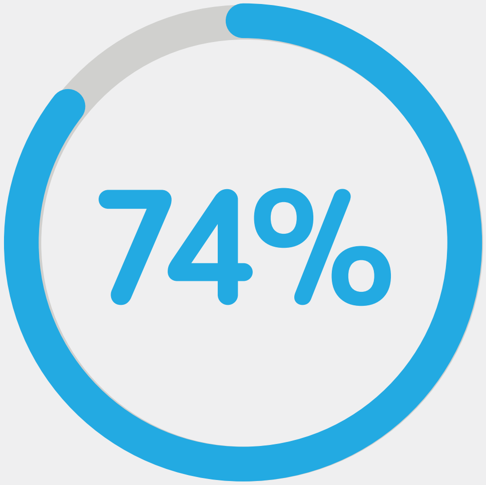
← Pg. 2 | Pg. 4 →

Back to contents

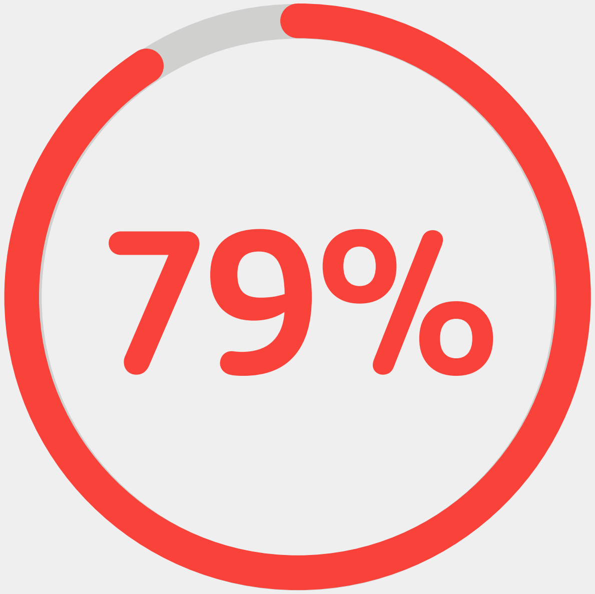
Data tells the story: data breaches are increasing, no network is safe from attack by sophisticated adversaries, and IT organizations lack confidence in their ability to defend their users, applications, and data.



Increase in data breaches in 2016 (reaching an all-time high)



IT professionals who agree with the statement "A new IT security framework is needed to improve our security posture and reduce risk



Global networks **compromised at least once** by a successful cyberattack

← Pg. 2 | Pg. 4 →

Back to contents

Rethinking Security Efficacy

How can you reduce and manage risk in an apps everywhere and users anywhere world? By increasing your “security efficacy.”

Increasing security efficacy means strengthening your capabilities to...

↓

Defend against as many attacks as possible, including:

- Web Application Attacks
- Malware
- Data leaks
- DoS and DDoS attacks
- Ransomware

↓

Identify those attacks that get through as quickly as possible, using:

- Rich, real-time security information from a wide range of security and network devices
- Context-sensitive data about user, network, and system behaviors
- Machine learning
- Advanced threat analytics

↓

Respond effectively, through:

- Identification and remediation of vulnerabilities and security anomalies
- Automated patching
- Dynamic policy updates

← Pg. 4 | Pg. 6 →

Back to contents

A recent report from Verizon found that attacks on web applications represented

over 40%

of incidents resulting in a data breach, and caused more data loss than any other type of cyberattack.*

← Pg. 2 | Pg. 4 →

Back to contents

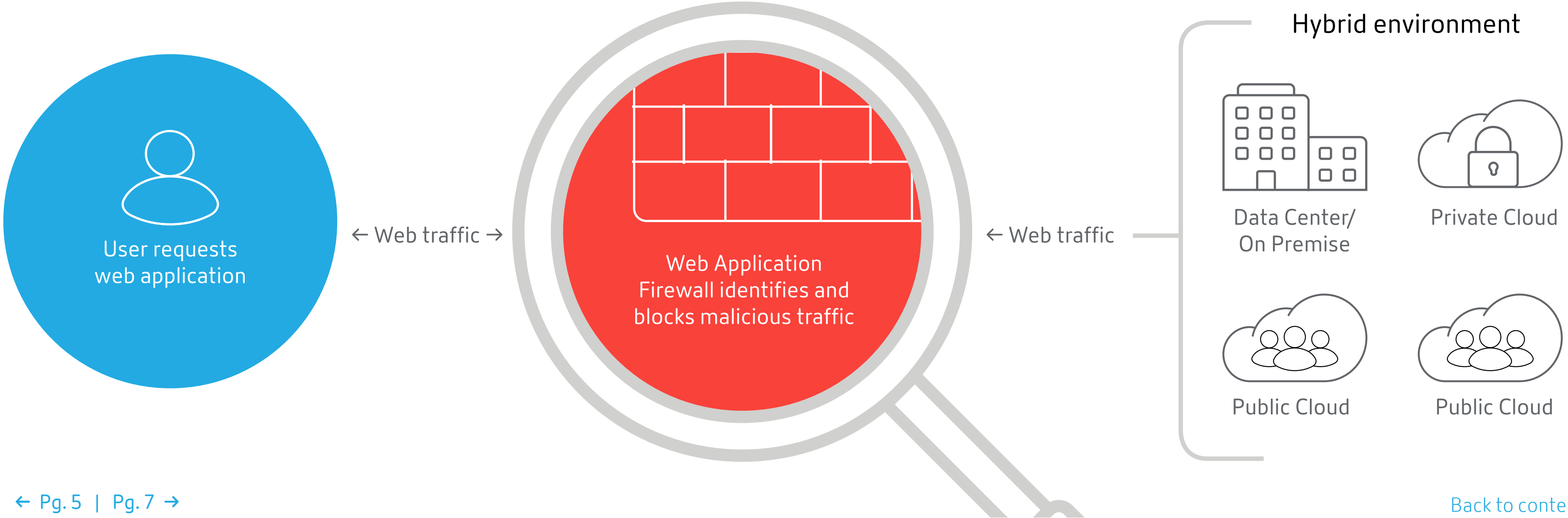
Defend Against Web Application Attacks

Many web application attacks employ well known techniques such as SQL injection and cross-site scripting. Others exploit misconfigured servers and badly designed authentication and session management software. Still others launch zero-day attacks against newly discovered vulnerabilities in popular web software packages.

The key defense against web application attacks is the Web Application Firewall (WAF). A WAF provides centralized application-layer security for web apps and services. It sits between web clients and servers and analyzes application traffic, using signatures and patterns to detect security policy violations and a wide range of web application attacks. That includes recognizing and blocking most of the “OWASP Top 10” most critical web application security risks, compiled by the Open Web Application Security Project.

A web application firewall can also protect against application anomalies and zero-day attacks by dynamically profiling the behavior of web applications and flagging unusual activities.

In addition, a WAF can help security and network administrators segment networks, so only authorized users can access key applications. Improved network segmentation helps enterprises comply with regulations like PCI DSS, HIPAA, and the EU GDPR.



← Pg. 5 | Pg. 7 →

Back to contents

Defend Against DDoS Attacks

Distributed Denial of Service (DDoS) attacks can cripple web sites and disrupt business processes. They are becoming more frequent every year. One analysis found that almost half of enterprise, government and educational organizations experience more than 10 DDoS attacks per month.*

Fortunately, web application firewalls offer a variety of DDoS protection features such as:

- **Protocol validation**
- **Rate limiting**
- **Load balancing**

These and other capabilities help WAFs detect and mitigate conventional network level and infrastructure level DDoS attacks, which flood web servers with useless network packets. Some can also blunt sophisticated "low and slow" application-level DDoS attacks, which take advantage of weaknesses in web applications to overwhelm web and database servers.

DNS protection can blunt attacks that attempt to swamp DNS servers and prevent users from reaching external websites.

An IP threat reputation service is another powerful tool against DDoS attacks. This service gathers and shares information from a large community of enterprises about web sites and botnets that are controlled by hackers and cybercriminals. Armed with this information, a WAF can terminate all sessions from these malicious IP addresses before they interfere with business operations.

Types of DDoS Attacks

Application

GET and malicious POST floods; slowloris, slow POST, and other low-bandwidth variants

Infrastructure

Connection floods, SSL floods, DNS floods (udp, query, nxdomain)

Network

Syn, UDP, ICMP, PUSH and ACK floods; LAND, smurf, and teardrop attacks

← Pg. 6 | Pg. 8 →

Back to contents

Defend Against Malware and Malicious Web Traffic

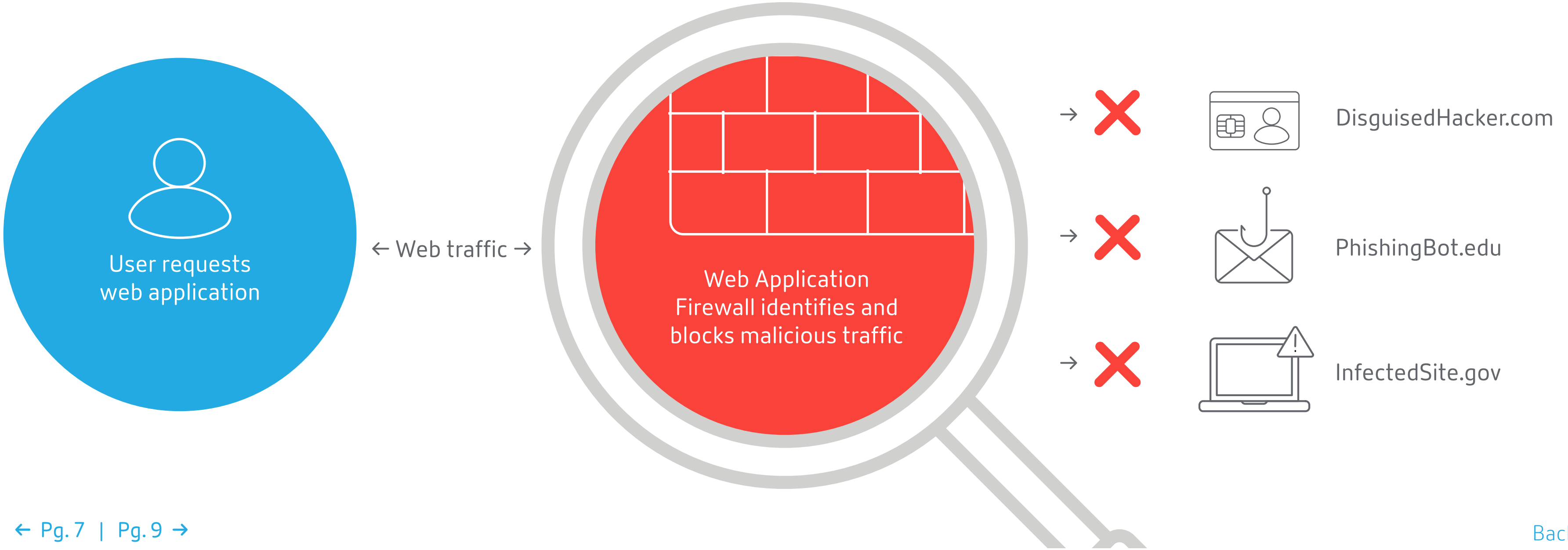
Many of today's most damaging advanced attacks start with malware that reaches users' devices either as attachments to emails, or as downloads from a website under the control of the attacker.

A Secure Web Gateway can help protect against many of these web attacks.

URL Filtering prevents users from surfing to web sites that are known to be under the control of hackers and cybercriminals and inadvertently acquiring malware there. It also stops employees from being lured by phishing emails to compromised web sites where they give away login credentials and personal information.

URL filtering also helps organizations comply with the requirements of CIPA (Children's Internet Protection Act) and similar regulations. CIPA requires schools, libraries and others to prevent minors from accessing web sites with materials that are inappropriate for their age group.

High-Speed Decryption of SSL Traffic allow organizations to handle safely large volumes of encrypted web traffic. That is critical, because over half of today's web traffic is encrypted.* A Secure Web Gateway can decrypt SSL traffic and scan it for malware and attack signatures. It can also protect data by ensure that outgoing traffic is encrypted, even if SSL encryption was not built into the original applications.


User requests web application
← Web traffic →
Web Application Firewall identifies and blocks malicious traffic
DisguisedHacker.com
PhishingBot.edu
InfectedSite.gov

← Pg. 7 | Pg. 9 →

Back to contents

Defend Against Unauthorized Access

Hackers and cybercriminals have found that the easiest way to break into a network is usually to capture login credentials and impersonate legitimate users. In fact, Verizon reports that 81% of hacking-related breaches leveraged stolen or weak passwords.*

To manage risk without disrupting business processes, IT and security leaders need to ensure that:

- **Applications can be accessed only by authorized users**
- **Authorized users can always access the applications they need, no matter where they are and what devices they are using**

Succeeding in this balancing act requires a significant investment in Identity and Access Management (IAM) technologies.

For example, web gateways can:

- Support multi-factor authentication and single sign-on (SSO) for users across all their devices, and all their apps, anywhere in the world they may be working.
- Employ centralized access control and network segmentation to protect critical applications and data from unauthorized access.
- Support auditing and security analytics by capturing and analyzing detailed information on application traffic, and on events like failed access requests.

← Pg. 8 | Pg. 10 →

Back to contents

Identify the Attacks That Get Through as Quickly as Possible

IT and security leaders no longer can hope to block all attacks from reaching their network. In order to increase their Security Efficacy, they need to be able to identify those attacks that get through by quickly recognizing indicators of compromise and anomalous behaviors.

Security analytics tools can help organizations:

↓ Pinpoint and monitor the users and applications most often attacked.

↓ Identify indicators of compromise and evidence of malicious activity, including network traffic to web sites and botnets controlled by hackers, failed access requests, and attempted web application attacks.

↓ Flag risky and anomalous behaviors of employees, contractors, and other insiders (and of attackers using their credentials), such as inappropriate web surfing, excessive access to sensitive files, and attempts to transfer data to insecure storage devices.

↓ Recognize anomalous network traffic, including unusual volumes of data being uploaded and downloaded and spikes in traffic that indicate incipient DDoS attacks.

← Pg. 9 | Pg. 11 →

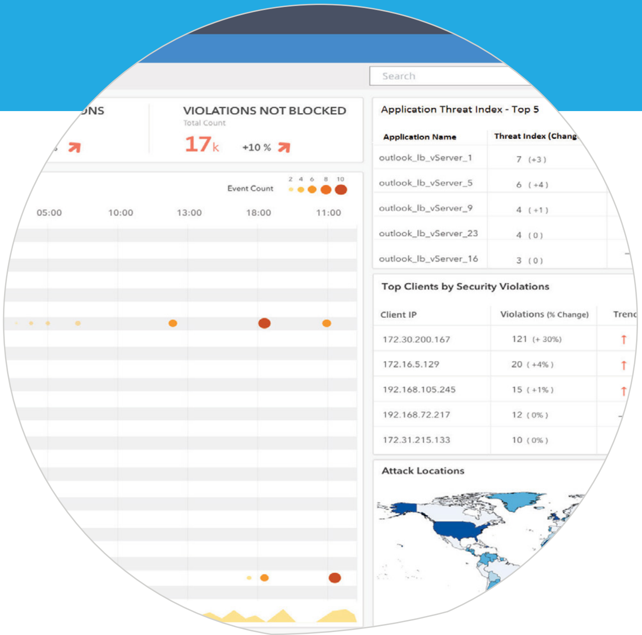
Back to contents

Advanced Security Analytics Solutions Go Far Beyond Just Generating Alerts

↓
They collect and correlate data from a wide range of sources, including desktop and mobile apps and devices, web apps and microservices, and network and security devices and middleware.

↓
They enable analysts to quickly grasp patterns and trends about users, applications, devices, and networks with the aid of dashboards and visualization tools.

↓
They employ machine learning and artificial intelligence to identify subtle anomalous behaviors and find suspicious patterns in seemingly unrelated indicators of compromise.



Application Threat Index - Top 5

Application Name	Threat Index (Chang
outlook_lb_vServer_1	7 (+3)
outlook_lb_vServer_5	6 (+4)
outlook_lb_vServer_9	4 (+1)
outlook_lb_vServer_23	4 (0)
outlook_lb_vServer_16	3 (0)

Top Clients by Security Violations

Client IP	Violations (% Change)	Trenc
172.30.200.167	121 (+ 30%)	↑
172.16.5.129	20 (+4%)	↑
192.168.105.245	15 (+1%)	↑
192.168.72.217	12 (0%)	–
172.31.215.133	10 (0%)	

These capabilities help security and network analysts eliminate blind spots and detect ongoing attacks sooner, before they compromise data and business processes.

- Applications under attack
- Clients with most security violations
- Top attack locations
- Attack trends

← Pg. 9 | Pg. 11 →

Back to contents

Respond Effectively to Threats

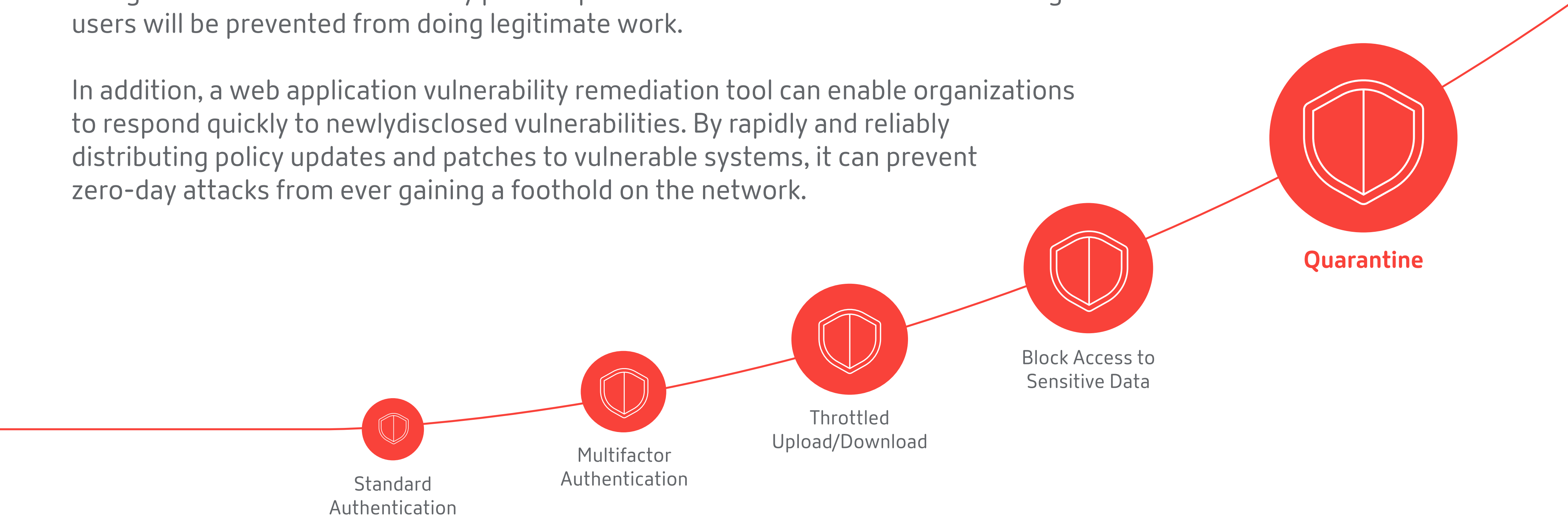
Identifying attacks is not enough. Organizations must be able to stop ongoing attacks in their tracks, then remediate vulnerabilities so attacks cannot recur in the future.

After recognizing attacks, some advanced security analytics tools can close the loop by taking automatic steps to progressively increase defenses. For example, as evidence becomes stronger that a user account may have been compromised, a tool could:

- First, require multi-factor authentication for application access
- Then reduce the volume of data that user can download and upload
- Then block that user's access to applications containing sensitive data
- Finally, quarantine the user, preventing any data from being accessed or sent outside the network

This granular control over security policies prevents data breaches while minimizing the chance that users will be prevented from doing legitimate work.

In addition, a web application vulnerability remediation tool can enable organizations to respond quickly to newlydisclosed vulnerabilities. By rapidly and reliably distributing policy updates and patches to vulnerable systems, it can prevent zero-day attacks from ever gaining a foothold on the network.


Standard Authentication
Multifactor Authentication
Throttled Upload/Download
Block Access to Sensitive Data
Quarantine

← Pg. 8 | Pg. 10 →

Back to contents

General Requirements: End-to-End Visibility and Protection

To protect themselves in an era of ever-more complex computing infrastructures, organizations need solutions that allow them to manage more security technologies, across a wider range of on-premises and cloud platforms, with fewer administrators and technical support staff.

Today, security efficacy demands:

Data center-to-cloud visibility and control, so organizations can protect hybrid environments that span on-premise, public and private cloud data centers.

Integrated security solutions, so organizations can defend themselves against a wide range of threats without having to create and maintain custom interfaces and connectors.

Centralized management, so a lean staff can deploy and maintain a consistent set of security policies across multiple security technologies, computing environments, and global regions.

Comprehensive security analytics, so organizations can detect advanced, subtle, multi-vector security threats.

This combination not only simplifies management and reduces costs, it also dramatically increases an organization's ability to deploy and modify applications with confidence.

← Pg. 8 | Pg. 10 →

Back to contents

How Citrix Networking Solutions Keep Your Business Safer Than Ever Before

Defend Against Web Application Attacks

Citrix Web App Firewall, formerly NetScaler AppFirewall™, uses signatures and pattern matching to defend against known web application attacks. They also employ dynamic profiling of web application behavior to recognize and protect against application anomalies and zero-day attacks.

It also provides network segmentation features that keep intruders away from key applications. This strengthens regulatory compliance as well as security.

Defend Against Network Attacks

Citrix ADC, formerly NetScaler ADC, includes built-in DDoS and DNS protection that defend you from network attacks. Techniques such as rate limiting, load balancing, and analysis of web application traffic can mitigate DDoS attacks at all levels – application, infrastructure, and network – and keep DNS services functioning. Another built-in feature, IP reputation service, terminates connections from IP addresses with bad reputations.

← Pg. 8 | Pg. 10 →

Back to contents

Defend Against Malware and Malicious Web Traffic

Citrix Secure Web Gateway, formerly NetScaler Secure Web Gateway™, helps you defend against malware and malicious web traffic. URL Threat Intelligence blocks access to web sites used for phishing attacks and drive-by downloads or malware. High-speed decryption of SSL traffic makes it possible to spot malware and malicious traffic concealed by SSL encryption.

Defend Against Unauthorized Access

Citrix Gateway, formerly NetScaler Unified Gateway™, helps organizations defend against unauthorized access to key applications and data. It supports key Identity and Access Management technologies such as multi-factor authentication and single sign-on. It also provides centralized access control, network segmentation, and auditing.

Identify Attacks as Quickly as Possible

Citrix Analytics, together with Citrix Application Delivery Management, formerly NetScaler Management and Analytics System (MAS), and insights from our networking technologies, enable security and network analysts to identify ongoing attacks. They capture data from a wide array of devices and networks, provide dashboards and data visualization tools, and use machine learning and artificial intelligence to find patterns and highlight deviations from those patterns. By identifying indicators of compromise and flagging risky and anomalous behaviors, these advanced security analytics tools enable you to determine faster and with higher confidence whether a real attack is taking place.

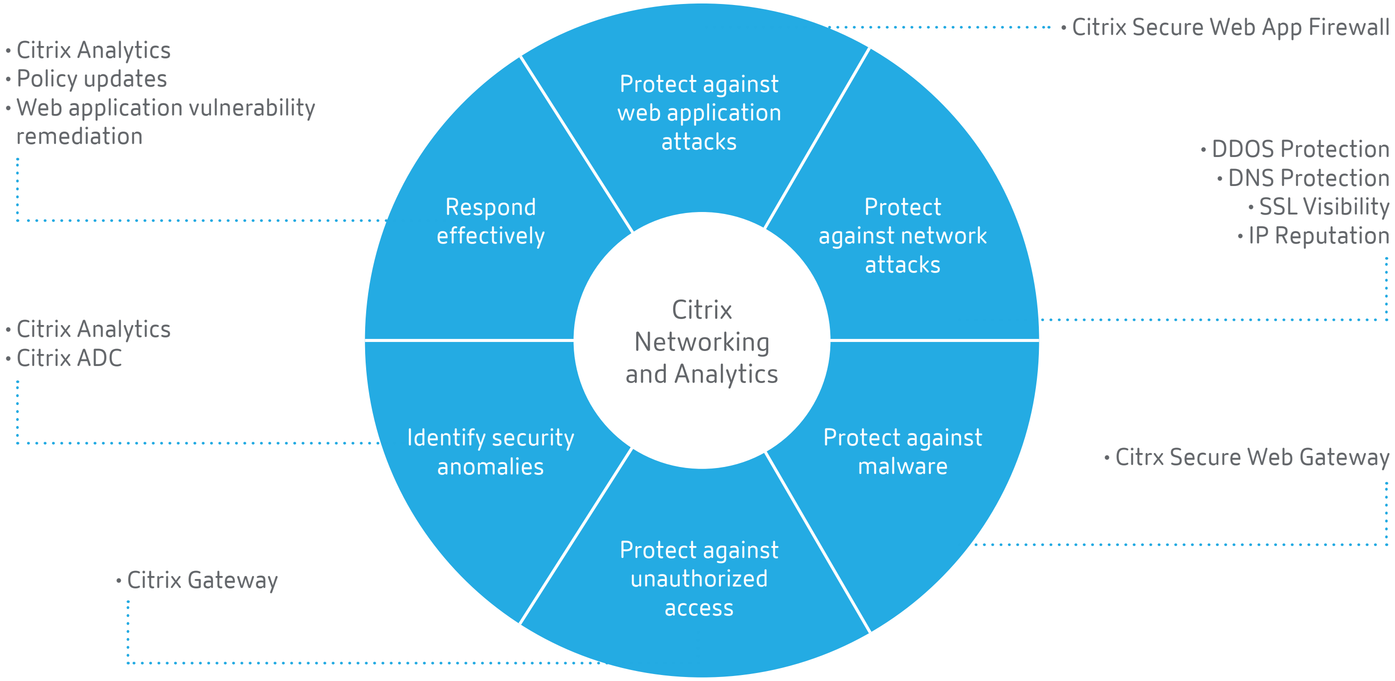
← Pg. 8 | Pg. 10 →

Back to contents

Respond Effectively to Threats

Citrix Analytics not only helps identify and analyze threats, it also gives you a tool to close the loop by progressively increasing defenses at levels commensurate with risk. For example, as additional indicators of compromise are discovered and associated with a user, you can automatically apply more rigorous authentication methods, reduce the user's access to information, or even quarantine the user.

Citrix Networking solutions also include web application vulnerability remediation tools that allow you to respond to newly-discovered vulnerabilities by rapidly distributing and applying policy updates and patches.



Citrix Networking and Analytics

Protect against web application attacks
- Citrix Secure Web App Firewall

Protect against network attacks
- DDOS Protection
- DNS Protection
- SSL Visibility
- IP Reputation

Protect against malware
- Citrx Secure Web Gateway

Protect against unauthorized access
- Citrix Gateway

Identify security anomalies
- Citrix Analytics
- Citrix ADC

Respond effectively
- Citrix Analytics
- Policy updates
- Web application vulnerability remediation

← Pg. 8 | Pg. 10 →

Back to contents

CITRIX®

Enjoy End-to-End Visibility and Protection

Finally, Citrix helps you increase security efficacy in the face of expanding attack surfaces, increased complexity, and tight budgets.
Citrix Networking portfolio offers you:

- Data center-to-cloud visibility and control
- A portfolio of integrated security solutions
- Centralized management, and finally,
- Comprehensive security analytics

Learn more at **now.citrix.com/security-efficacy.**

Back to contents