AUTHENTIC8 ROI FOR GOVERNMENT ORGANIZATIONS

INTRACTABLE PROBLEMS REQUIRE PROFOUND CHANGE

FREE COMES AT A PRICE

What is the cost of running a “free” local web browser in your organization?

That’s a provocative question because running a “free” browser comes at a price when the browser remains the same off-the-shelf non-secure app that came with the federal worker’s computer.[1] Many believe your browser may betray you, but most are not aware of a more secure, anonymous, disposable, productive and compliant option. The Security and Software Engineering Research Center at Georgetown University (S^2ERC), a National Science Foundation (NSF) sponsored research center working on the safety, security, and stability of today’s communications networks has confirmed Silo, Authentic8’s cloud browser, as such an option.[2] The browser doesn’t have to be one of the most insecure elements of your IT network.

FIRST ORDER EFFECT

What is the return on investment (ROI) for deploying a cloud browser instead of a free local browser?

While there are many cost savings from a cloud browser, three dwarf the others: remediation, ticket response, and network bandwidth usage.

COST OF LOSS

Remediation Costs

Silo reduces a significant attack vector for endpoint compromise, so it’s no surprise that Authentic8 customers report spending less time remediating because they have fewer incidents. It’s difficult to put a cap on the cost of an infection from one malicious file download by a free browser. Once a single endpoint is infected, every other endpoint is at risk, and the rest of the organization is at risk of productivity or data loss. Cost savings vary based on organization, but key costs are consistent:

1. The productivity loss for every hour a key organization process is down because of malware disabling the PC or server
2. The hourly rate for help desk personnel to diagnose malware infections and for the support group to re-image infected PCs

	“FREE” CHROME BROWSER	SILO CLOUD BROWSER
Test browser ability to block downloading 54 infected files	~7 infected PCs (1 in 7 malicious files downloaded)3	Zero infected PCs
Productivity Loss per incident	$300 = $100 downtime (1hr) $100 transition back to permanent PC (1hr) $100 cost of loaner PC (depends on user impacted)	$0
PC Reimage per incident	$300 = 4 hours x $75/hr 1 hr take PC off network, transition user to loaner 2 hr reimage 1 hr to transition user back to permanent PC Some organizations dispose of infected PC rather than reimage	$0

A conservative estimate for a government agency with 10,000 workers is Silo saves $150,000 per year (1 remediation per weekday at $600 per incident).

REDUCTION IN ALERTS

Ticket Response

When running Silo, the SOC, NOC and IT teams benefit from reduction in alerts from infections and fewer incident responses. Still these same teams are often overwhelmed with tickets due to web content proxies blocking access to sites users need to do their jobs. The use of Silo allows users to navigate to sites/services without admin intervention. Users get the unfiltered access they need. IT maintains policies as all user actions are auditable in secure, single use virtual containers.

	"FREE" CHROME BROWSER	SILO CLOUD BROWSER
Web Proxy blocks uncategorized URLs or URLs that users need to research	Ticket to provide temporary access to URL	No ticket
Ticket Response	$30/ticket = $15 (assumes level 1 help desk is authorized to open access to URL without any research)[4] $15 to close URL after work is completed	$0
Risk of self-infection from accessing uncategorized or unacceptable URL	Unknown	$0

A conservative estimate for a government agency with 10,000 workers is Silo saves $75,000 per year (10 analysts opening 1 ticket per weekday at $30 per ticket).

HARD COST SAVINGS

Bandwidth Reduction

Moving to a cloud browser changes the network load on PCs. The only thing delivered to the user client device is pixels. Only getting an encrypted display uses less bandwidth.

	"FREE" CHROME BROWSER	SILO CLOUD BROWSER
Bandwidth Usage	Web usage is increasing 10% a year	Silo reduces bandwidth by 30%[5]
Ticket Response	$50,000/mo/1GPS current cost	$180,00/year Savings ($15,000/mo/1Gbps)

A conservative estimate for a government agency with 10,000 workers is internet bandwidth savings of $180,000 per year.

Cost Savings Summary

Three areas (remediation, ticket response, and bandwidth usage) generate over $405,000 in savings for an example organization when switching from a free browser to a cloud browser. Above and beyond these hard cost savings are the potential savings through the cloud browser avoiding cybersecurity incidents.

Other Cost Savings

Deploying Silo into an organization's existing security technology stack can have cascading positive effects on security posture and cost savings. Many enterprise security investments are focused on securing an enterprise network from the risk inherent in web browsing. Silo's core value to any organization is isolation of web browsing and policy controls around features and functions in the browser. The powerful capabilities in Silo support the replacement, reduction, or enhancement of your existing security solutions.

CAPABILITY	DESCRIPTION	COST SAVINGS
Virtual Machines/Micro Containers/Virtual Containers	Silo provides cloud based single use and hardened virtual containers	Reduce VM licenses needed to support secure browsing
Patching/Vulnerability Management	Silo takes the burden of vulnerability and patch management for the browser from the IT team	Reduce browser patching
Web Content Proxy	Silo allows administrators to whitelist/ blacklist domains and disable access to sites through category content filtering (eg: pornography, social media, shopping)	Eliminate or reduce existing web content proxies, if Silo is the primary means of accessing the open internet
Proxy/VPN	Silo encrypts all traffic in motion and at rest. In addition, the IP addresses that user web traffic originates from is identified as Authentic8. This differs from your organization's external IP	Reduce the use of proxies and VPNs
User Behavioral Analytics/ Insider Threat Monitoring	Silo monitors all user activity within the platform - sites and services navigated to, uploads/downloads and more	Reduce the cost of UBA/InT software, Windows Event loggers, storage and related software
DLP	Silo has policy controls over upload/download as well as directional copy paste	Reduce existing DLP investments around data transfer policies
Cloud Storage	Silo has encrypted cloud storage at the per-user level, temporary storage for a session a user is in, and shared storage amongst a user group	Reduce existing levels of cloud, network, and hardware based storage.

CAPABILITY	DESCRIPTION	COST SAVINGS
Remote Account Management/Cloud Access Security Broker (CASB)	Silo enables admins to provision login credentials to cloud service providers. This capability combined with our control policies allow for total control of data flow, access and authentication, and security	Reduce investments in account management and CASB solutions
Password Management	Silo enables users and admins to save login credentials for any site/service they access through the browser. These credentials are encrypted	Reduce investments in password management software
Antivirus	Silo scans files before download to the user's endpoint. The inline antivirus solution is built on Clam AV	Reduce investments on browser based AV scanning
Hardware End of Life Extension	Silo runs in Authentic8 data centers removing the free local browser requirement for CPU, RAM, Disk I/O and network bandwidth from the endpoint. Only a local display agent runs on the PC	Organizations can extend the life of their existing hardware

IMPROVING SECURITY POSTURE

Conclusion

Silo complements an organization's existing security stack by improving security posture and providing cost savings. Silo addresses the risk inherent in web browsing, an intractable problem for most organizations, by giving government personnel full access to the public web without risk or attribution. Use of Silo reduces or eliminates many security workflows while reducing use of network bandwidth. Silo allows users to navigate to sites/services without admin intervention. Benefits of Silo cascade from fewer incidents to less time spent remediating to security teams spending more time on their core mission. Silo isn't just another security product to add to your ever growing technology stack. The powerful capabilities in Silo support the replacement, reduction, or enhancement of your existing security solutions.

Learn more about how Silo addresses the risk inherent in web browsing while reducing costs for government organizations:

www.authentic8.com

[1] Traditional Browsers Put Federal (and regular) Workers at Risk, https://www.linkedin.com/pulse/traditional-browsers-put-federal-regular-workers-risk-scott-petry/

[2] S^{2}ERC's Productive Browser Project reveals Authentic8 Silo virtual browser delivers greater malware protection than Google Chrome desktop model https://www.businesswire.com/news/home/20180307005169/en/Georgetown-Security-Software-Engineering-Research-Center-Tests

[3] Ibid.

[4] Metric of the Month: Service Desk Cost per Ticket, https://www.thinkhdi.com/library/supportworld/2017/metric-of-month-service-desk-cost-per-ticket.aspx

[5] DISA